

P-GW Administration Guide, StarOS Release 21.27

First Published: 2022-04-14

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



About this Guide

Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with CUPS products. References to any CUPS products or features are for informational purposes only. Please contact your Cisco Account or Support representative for any questions about parity between this product and any CUPS products.

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

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

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

Packet Data Network Gateway (P-GW) is a StarOS application that runs on Cisco® ASR 5500 and virtualized platforms.

- Conventions Used, on page iv
- Supported Documents and Resources, on page v
- Contacting Customer Support, on page vi

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

The following common documents are available:

- *AAA Interface Administration Guide and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration Guide and Reference*
- *Installation Guide* (platform dependent)
- *Release Change Reference*

- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependent)
- *Thresholding Configuration Guide*

Related Product Documentation

The following product documents are also available and work in conjunction with the P-GW:

- *ADC Administration Guide*
- *ECS Administration Guide*
- *GGSN Administration Guide*
- *IPSec Reference*
- *MME Administration Guide*
- *NAT Administration Guide*
- *PSF Administration Guide*
- *SAEGW 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

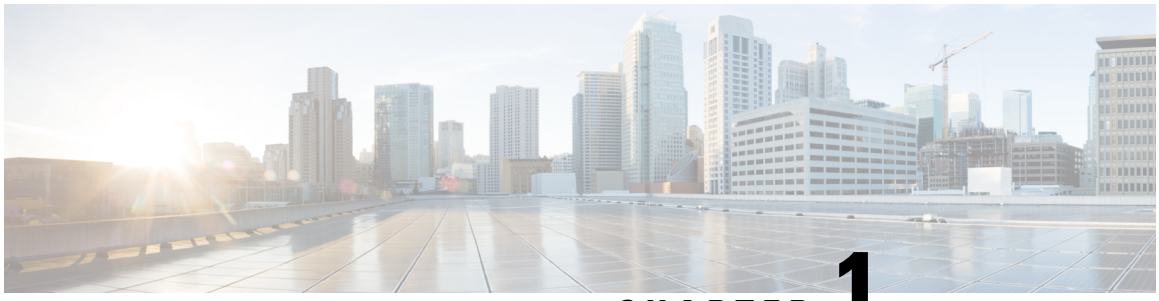
Use the following path selections to access the P-GW documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco PGW Packet Data Network Gateway

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

PDN Gateway Overview

The Cisco® Packet Data Network (PDN) Gateway (P-GW) is a critical network function for the 4G mobile core network, known as the evolved packet core (EPC). The P-GW acts as the interface between the 3GPP2 Long Term Evolution-System Architecture Evolution (LTE-SAE) network and other packet data networks, such as the Internet, SIP-based IP Multimedia Subsystem (IMS) networks, and evolved High Rate Packet Data (eHRPD) wireless data networks.

This overview provides general information about the P-GW including:

- Product Description, on page 1
- Network Deployment(s), on page 4
- Features and Functionality - Base Software, on page 17
- Features and Functionality - Inline Service Support, on page 66
- Features and Functionality - Optional Enhanced Feature Software, on page 71
- How the PDN Gateway Works, on page 94
- Supported Standards, on page 103

Product Description

The P-GW is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening.

Figure 1: P-GW in the Basic E-UTRAN/EPC Network

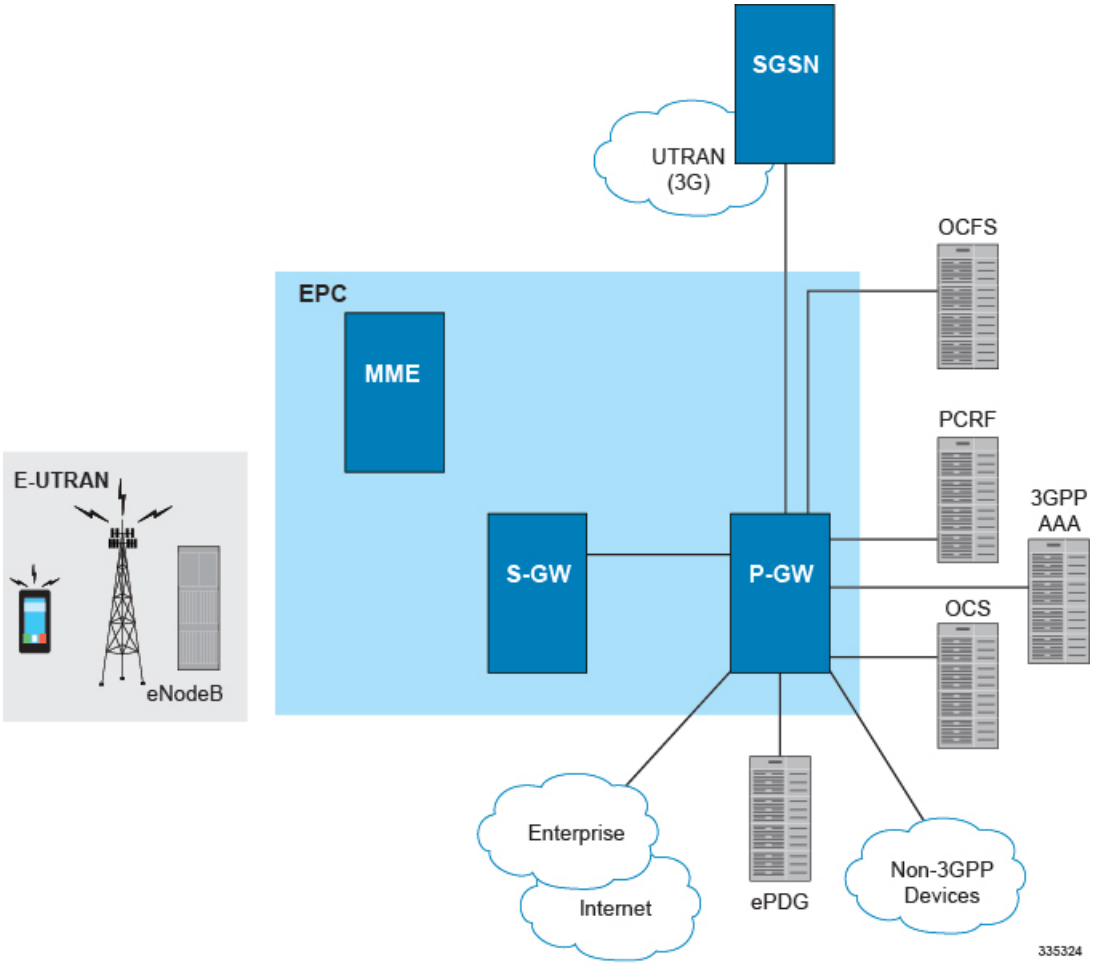
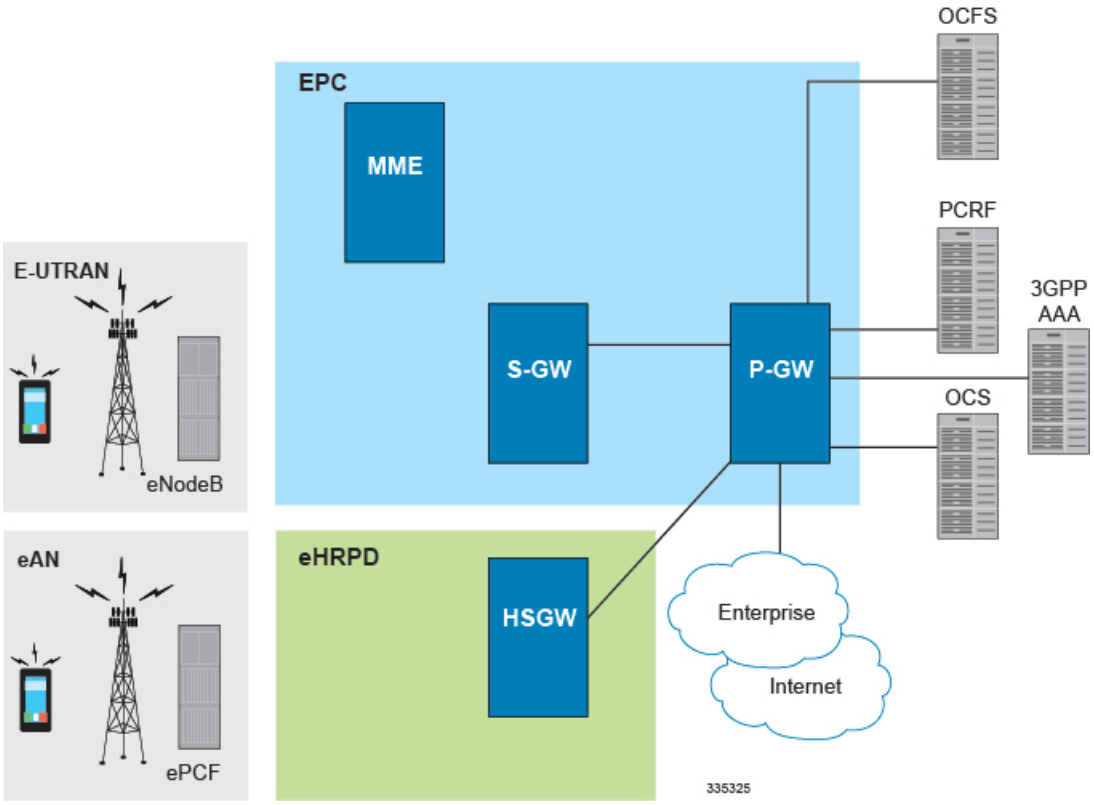


Figure 2: P-GW in the Basic E-UTRAN/EPC and eHRPD Network



Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

P-GW functions include:

- Mobility anchor for mobility between 3GPP access systems and non-3GPP access systems. This is sometimes referred to as the SAE Anchor function.
- Policy enforcement (gating and rate enforcement)
- Per-user based packet filtering (deep packet inspection)
- Charging support
- Lawful Interception
- UE IP address allocation
- Packet screening
- Transport level packet marking in the downlink;
- Down link rate enforcement based on Aggregate Maximum Bit Rate (AMBR)

The following are additional P-GW functions when supporting non-3GPP access (eHRPD):

- P-GW includes the function of a Local Mobility Anchor (LMA) according to draft-ietf-netlmm-proxymip6, if PMIP-based S5 or S8 is used.

- The P-GW includes the function of a DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal, if S2c is used.

Qualified Platforms

P-GW 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.

Licenses

The P-GW 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*.

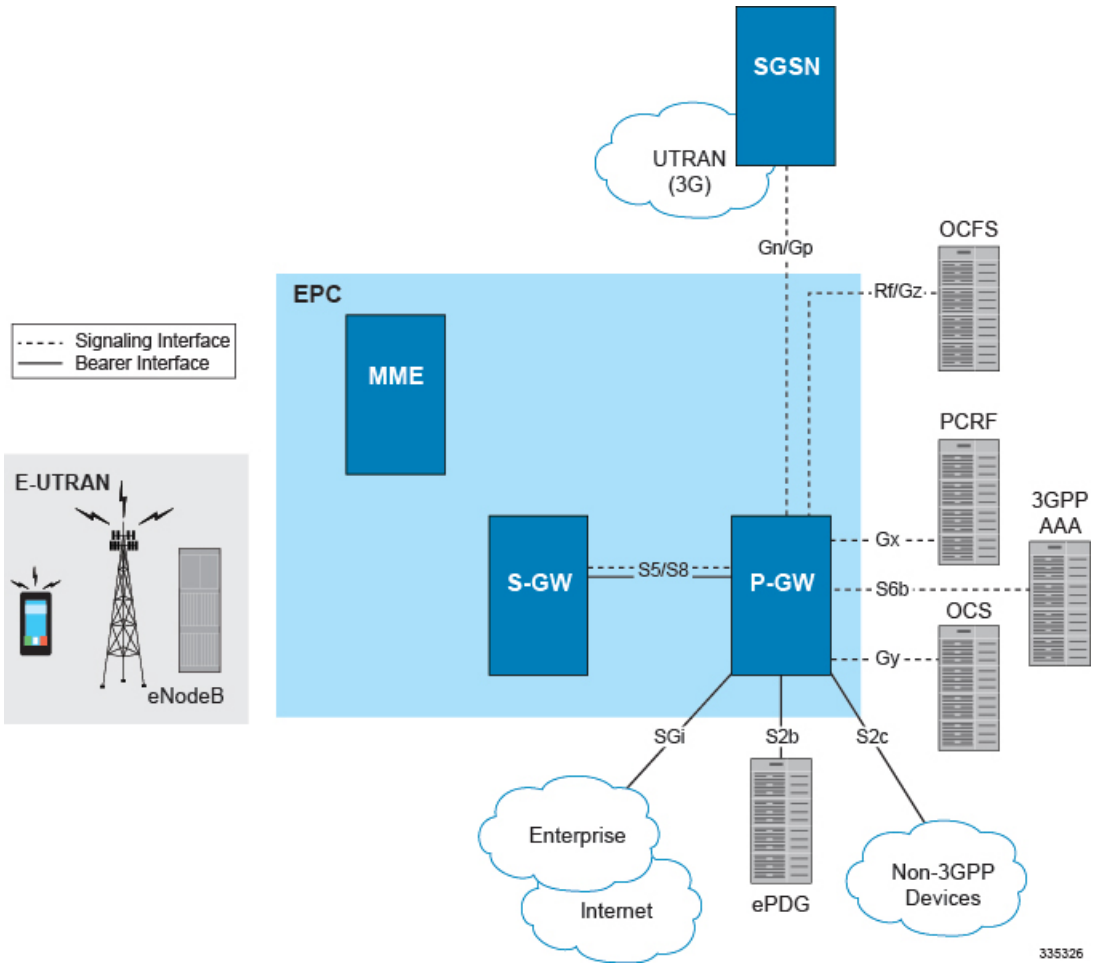
Network Deployment(s)

This section describes the supported interfaces and the deployment scenarios of a PDN Gateway.

PDN Gateway in the E-UTRAN/EPC Network

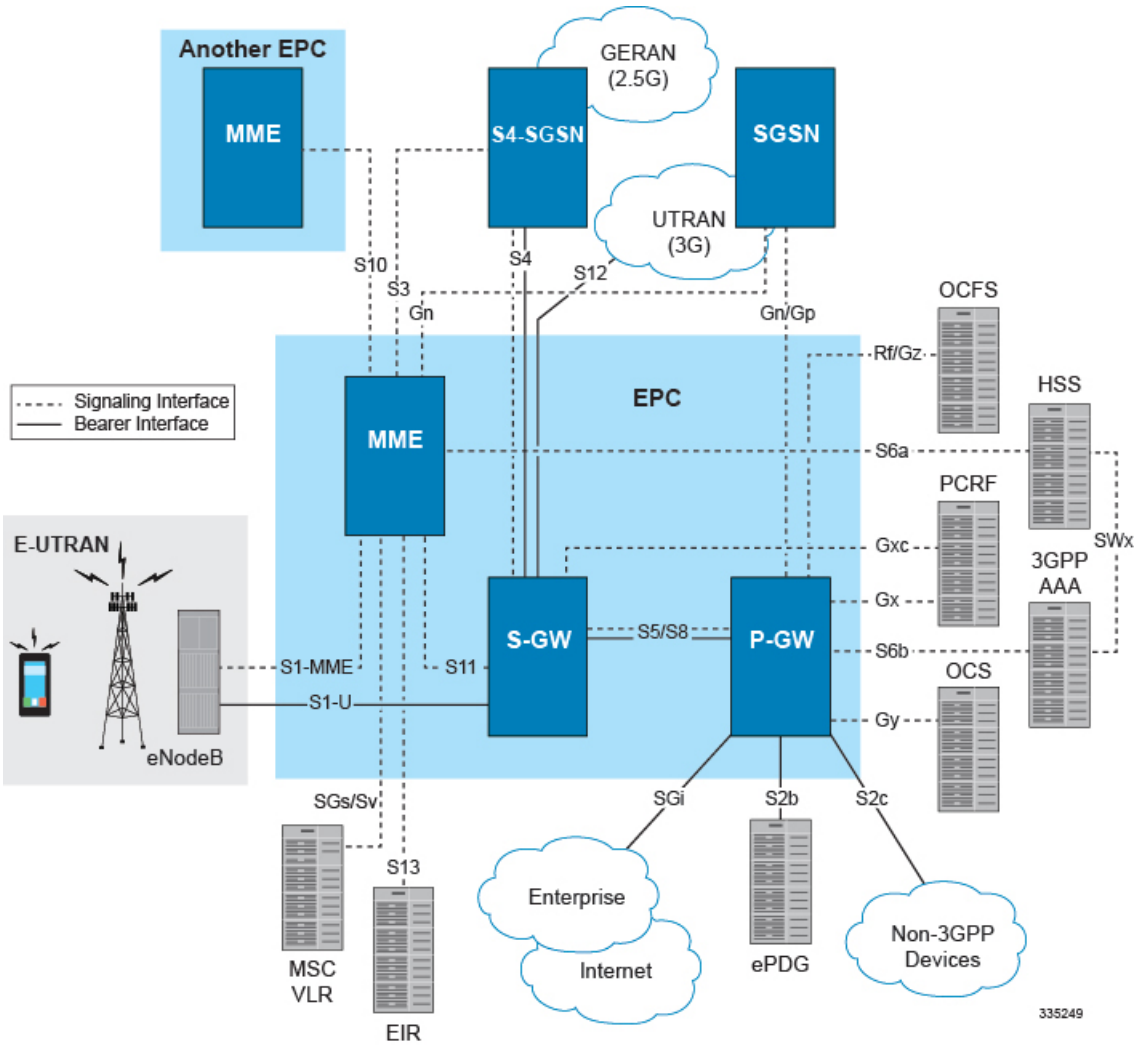
The following figure displays the specific network interfaces supported by the P-GW. Refer to Supported Logical Network Interfaces (Reference Points), on page 13 for detailed information about each interface.

Figure 3: Supported P-GW Interfaces in the E-UTRAN/EPC Network



The following figure displays a sample network deployment of a P-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

Figure 4: P-GW in the E-UTRAN/EPC Network



Supported Logical Network Interfaces (Reference Points)

The P-GW provides the following logical network interfaces in support of E-UTRAN/EPC network:

S2b Interface

The S2b interface reference point defined between the non-trusted non-3GPP ePDG (Evolved Packet Data Gateway) and the P-GW uses PMIPv6 (Proxy Mobile IP version 6) for providing access to the EPC. GTPv2-C is the signaling protocol used on the S2b. The S2b interface is based on 3GPP TS 29.274.

The S2b interface runs PMIPv6 protocol to establish WLAN UE sessions with the P-GW. It also supports the transport of P-CSCF attributes and DNS attributes in PBU (Proxy-MIP Binding Update) and PBA (Proxy-MIP Binding Acknowledgement) messages as part of the P-CSCF discovery performed by the WLAN UEs.

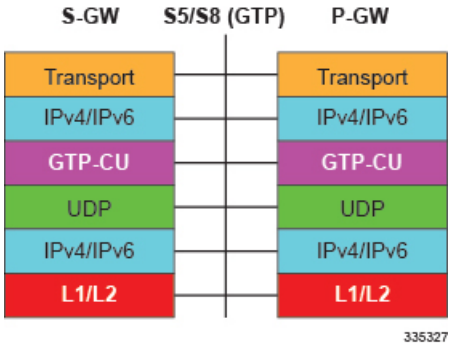
When the P-CSCF Address information is missing, P-CSCF Discovery is initiated upon S4-SGSN to LTE (and vice versa) handoff.If the P-CSCF Address information is already available, there is no need to explicitly trigger another P-CSCF Discovery upon S4-SGSN to LTE (and vice versa) handoff.

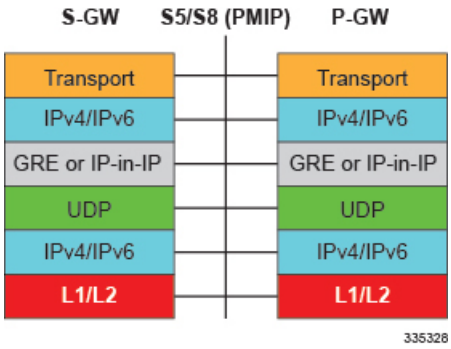
S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401 and TS 23.402. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

Supported protocols

- Transport Layer: UDP, TCP
- Tunneling:
  - GTP: GTPv2-C (signaling channel), GTPv1-U (bearer channel)
  - PMIPv6: GRE or IP-in-IP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet





S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool,

Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

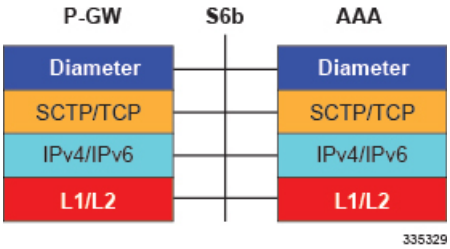
Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

StarOS Release 17 and onwards, P-GW supports receiving AVP "Restoration-Priority-Indicator" from AAA server over the S6b interface to distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections. KPIs are also provided based on the AVP value.

Important The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



SGi Interface

This reference point provides connectivity between the P-GW and a packet data network (3GPP TS 23.401). This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

Supported protocols:

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

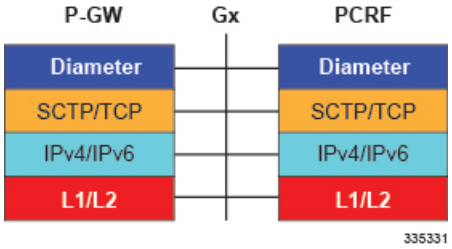


Gx Interface

This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



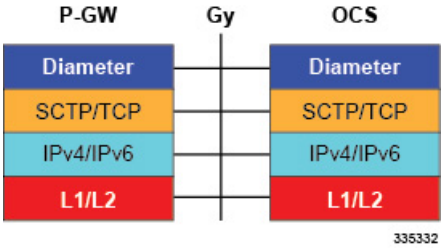
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface), on page 30.

Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



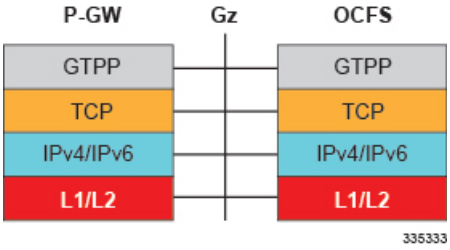
For more information on the Gy interface and online accounting, refer to Gy Interface Support, on page 36.

Gz Interface

The Gz reference interface enables offline accounting functions on the P-GW. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

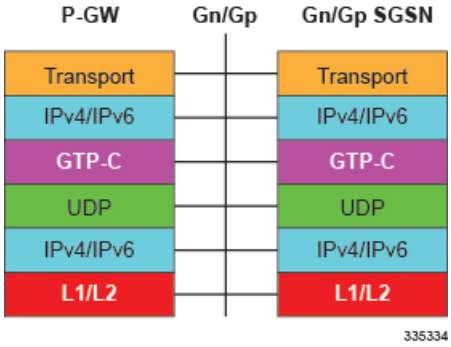


Gn/Gp Interface

This reference point provides tunneling and management between the P-GW and the SGSN during handovers between the EPS and 3GPP 2G and/or 3G networks (3GPP TS 29.060). For more information on the Gn/Gp interface, refer to Gn/Gp Handoff Support, on page 37.

Supported protocols

- Transport Layer: UDP, TCP
- Tunneling: GTP: GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

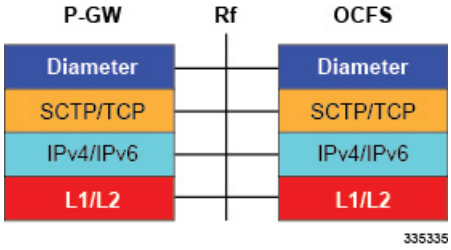


Rf Interface

The Rf interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

Supported protocols:

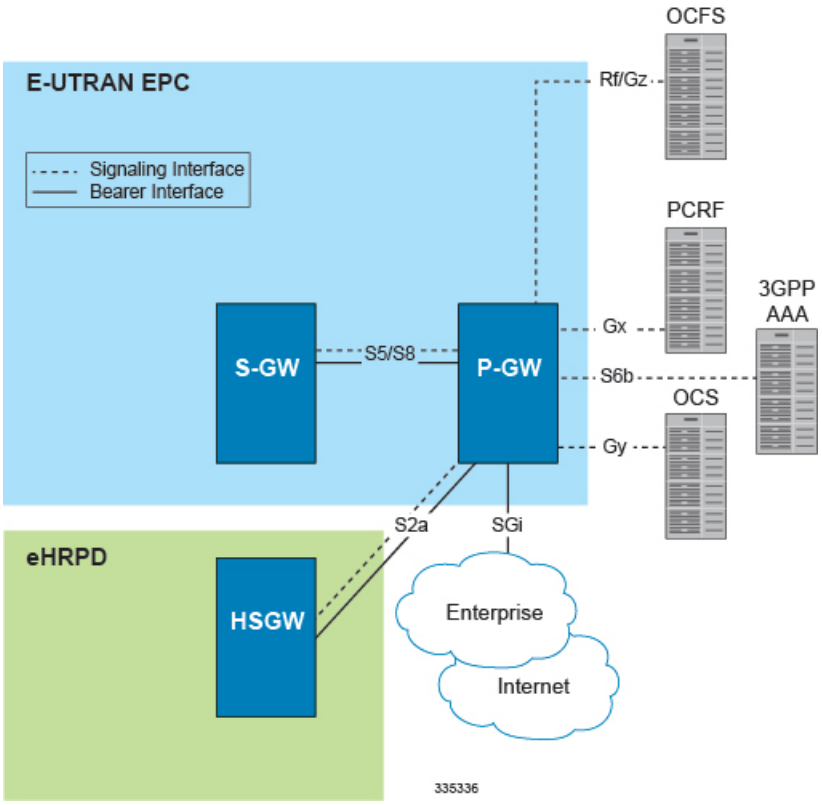
- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity

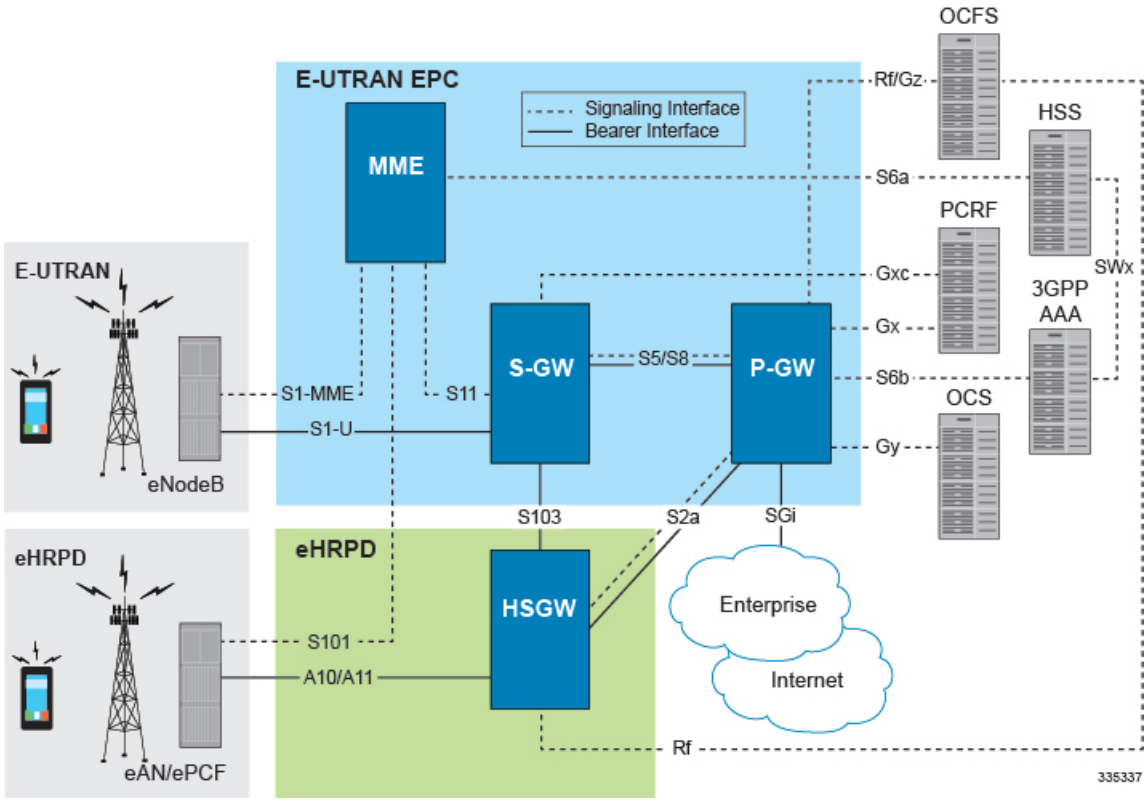
The following figure displays the specific network interfaces supported by the P-GW in an eHRPD network. Refer to Supported Logical Network Interfaces (Reference Points), on page 6 for detailed information about each interface.

Figure 5: P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity



The following figure displays a sample network deployment of a P-GW in an eHRPD Network, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

Figure 6: P-GW in the E-UTRAN/EPC Network Supporting the eHRPD Network



Supported Logical Network Interfaces (Reference Points)

The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

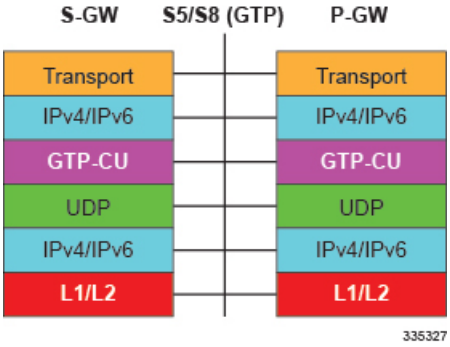
S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling:
  - GTP: IPv4 or IPv6 GTP-C (signaling channel) and GTP-U (bearer channel)
  - PMIPv6: IPv6 GRE or IP-in-IP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP

- Physical Layer: Ethernet

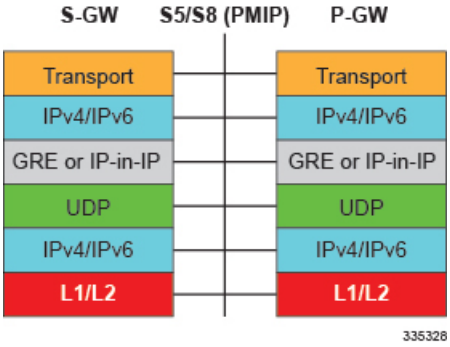


S2a Interface

This reference point supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the PDN Gateway. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling: GRE IPv6
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool

name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers

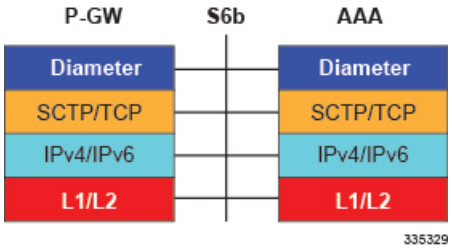
Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

Important The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



SGi Interface

This reference point provides connectivity between the P-GW and a packet data network. This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

Supported protocols:

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP

- Physical Layer: Ethernet

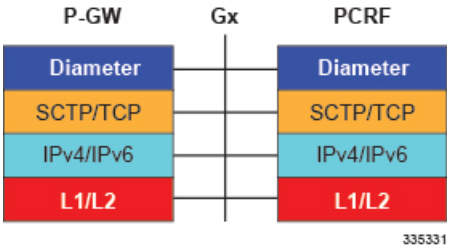


Gx Interface

This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



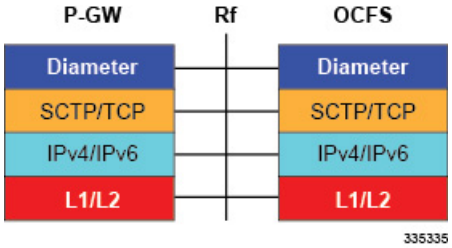
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface), on page 30.

Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



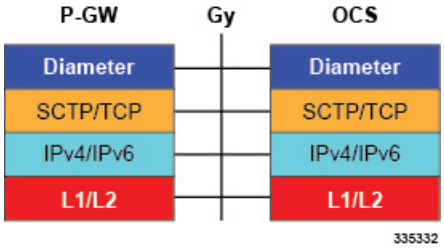
For more information on Rf accounting, refer to Features and Functionality - Base Software, on page 17.

Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



For more information on the Gy interface and online accounting, refer to Gy Interface Support, on page 36.

Features and Functionality - Base Software

This section describes the features and functions supported by default in the base software for the P-GW service and do not require any additional licenses to implement the functionality.

Important To configure the basic service and functionality on the system for the P-GW service, refer to the configuration examples provided in this guide.

3GPP R9 Volume Charging Over Gx

Also known as accumulated usage tracking over Gx, this 3GPP R9 enhancement provides a subset of the volume and charging control functions defined in TS 29.212 based on usage quotas between a P-GW and PCRF. The quotas can be assigned to the default bearer or any of the dedicated bearers for the PDN connection.

This feature enables volume reporting over Gx, which entails usage monitoring and reporting of the accumulated usage of network resources on an IP-CAN session or service data flow basis. PCRF subscribes to the usage monitoring at session level or at flow level by providing the necessary information to PCEF. PCEF in turn reports the usage to the PCRF when the conditions are met. Based on the total network usage in real-time, the PCRF will have the information to enforce dynamic policy decisions.

When usage monitoring is enabled, the PCEF can monitor the usage volume for the IP-CAN session, or applicable service data flows, and report accumulated usage to the PCRF based on any of the following conditions:

- When a usage threshold is reached,
- When all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated,
- When usage monitoring is explicitly disabled by the PCRF,
- When an IP CAN session is terminated or,
- When requested by the PCRF.

Accumulated volume reporting can be measured by total volume, the uplink volume, or the downlink volume as requested by the PCRF. When receiving the reported usage from the PCEF, the PCRF deducts the value of the usage report from the total allowed usage for that IP-CAN session, usage monitoring key, or both as applicable.

3GPP Release 12 Cause Code IE Support

When an E-RAB or a data session is dropped, an operator may need to get detailed RAN and/or NAS release cause code information as well as ULI information from the access network to be included in P-GW and S-GW CDRs for call performance analysis, user QoE analysis and proper billing reconciliation. The operator may also need to retrieve the above information at the P-CSCF for IMS sessions.

"Per E-RAB Cause" was received in a E-RAB Release command and a E-RAB Release Indication messages over S1. However RAN and NAS causes were not forwarded to the P-GW and the S-GW and they were not provided by the P-GW to the PCRF.

A "RAN/NAS Release Cause" information element (IE), which indicates AS and/or NAS causes, has been added to the Session Deletion Request and Delete Bearer Command. The "RAN/NAS Release Cause" provided by the MME is transmitted transparently by the S-GW to the P-GW (if there is signaling towards the P-GW) for further propagation towards the PCRF.

For backward compatibility, the S-GW can still receive the cause code from the CC IE in the S4/S11 messages and/or receive the cause code from some customers' private extension.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis.

Important As AAA applications do not support the indirectly connected hosts, configure only the directly connected host.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5500 and an element management system since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

APN Support

The P-GW's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW. In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting**: RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication**: Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging**: Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP**: Method for IP address allocation (e.g., local allocation by P-GW, Mobile IP, DHCP, etc.). IP address ranges, with or without overlapping ranges across APNs.

- **Tunneling**: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the P-GW independently from the APN.
- **QoS**: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the P-GW, the subscriber may be authenticated/authorized with an AAA server. The P-GW allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the P-GW during subscriber authentication/authorization.



Important For more information on APN configuration, refer to the *PDN Gateway Configuration* chapter this guide.

Assume Positive for Gy-based Quota Tracking

In the current implementation, the PCEF uses a Diameter based Gy interface to interact with the OCS and obtain quota for each subscriber's data session. Now, the PCEF can retry the OCS after a configured amount of quota has been utilized or after a configured amount of time. The quota value would be part of the dcca-service configuration, and would apply to all subscribers using this dcca-service. The temporary quota will be specified in volume (MB) and/or time (minutes) to allow for 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 PCEF shall retry 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 PCEF should reallocate with the configured amount of quota and time assigned to the user. The PCEF should report all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the PCEF shall report quota used during all allocation intervals.

When the Gy interface is unavailable, the P-GW shall enter "assume positive" mode. Unique treatment is provided to each subscriber type. Each functional application shall be assigned unique temporary quota volume amounts and time periods based on a command-level AVP from the PCRF on the Gx interface. In addition, a configurable option has been added to disable assume positive functionality for a subscriber group identified by a command-level AVP sent on the Gx interface by the PCRF.

Asynchronous Core Transfer Support for egtpinmgr

Asynchronous core transfer support for egtpinmgr has been added to optimize outage time during an egtpinmgr restart.

Previously, when the egtpinmgr restarted, the recovery process began only after a core dump file was created and transferred. However, the time taken to transfer the core file was significant. The outage time during an egtpinmgr restart was equal to the egtpinmgr recovery time plus the core file transfer time.

Support for Asynchronous Core Transfer has been added to include the egtpinmgr during the recovery process. Now, recovery begins when the egtpinmgr process crashes without waiting for the kernel to complete a core

dump file transfer and release its resources. As a result, the outage time during an egtpinmgr restart is equal to the egtpinmgr recovery time only.

With this enhancement, outage time during an egtpinmgr restart is reduced. The outage time consists only of the time required to recover the egtpinmgr. The time taken to create and transfer the core file no longer contributes to the outage time.

Availability of SSID Information in Gx, Gy, Gz, and LI Interface

On the S2a interface P-GW receives the identity of the Wifi access point in the TWAN-IDENTIFIER attribute in the CREATE SESSION REQUEST message. This information consists of AP MAC address, SSID, and CIVIC Address (which may contain information like AP Group name).

For location tracking and location based policy purpose, the above information needs to be propagated to the Policy Server (Gx), Quota Server(Gy), Charging Gateway(Gz) and LI Server. This new feature enhances the P-GW to propagate the AP SSID, BSSID and Civic Address on all these interfaces whenever received on the S2a interface.

Gx Interface

On the Gx interface this information is sent to PCRF in CCR-I/CCR-U and CCR-T messages in TWAN IDENTIFIER attribute. The standard Gx dictionary configuration is sufficient for this.

Gy Interface

On the Gy interface this information is sent to quota server in CCR-I/CCR-U and CCR-T messages in a Cisco Vendor specific attribute named "Civic-Addr" whenever dcca_custom33 dictionary is configured for this interface.

Gz Interface

On the Gz interface this information is sent to charging gateway in the CDR (Charging Data Records) in TWANUserLocationInformation attribute whenever custom53 dictionary is configured on this interface.

LI Interface

On the LI interface the information is sent to the LI server in the IRI events in "twan_identifier" field. No specific dictionary change is needed for this.



Important The PGW receives this SSID/BSSID/Civic Address information on s2a interface from a Trusted WLAN network (via SaMOG). If Cisco SaMOG is used then the functionality of sending this information from SaMOG to PGW can be controlled via a configuration (refer the SaMOG functionality for this). This feature will lead to 3-4% increase in baseline AAAmgr memory usage.

Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

Important For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

Bit Rate Mapping Across Gx and GTP-based Interfaces

This feature provides for more consistent behavior and ensures correct bandwidth is allocated for bearers.

Bit rate granularity provided by different interfaces was not aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

With this feature, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up.

This feature (rounding up the bitrate in kpbs) will be enabled by default. However, a CLI command under P-GW service, **[no] egtp bitrates-rounded-down-kbps**, controls the behavior of rounding-up. The CLI command enables/disables the old behavior of rounding down. By default, this CLI command is configured to use rounded-up bitrate values. Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value will be sent on GTP interface towards the Access side. If the CLI command is enabled, then it will result in the old behavior. In addition, **show subscribers pgw-only full all** shows the APN-AMBR in terms of bps. Previously, **show subscribers pgw-only full all** used to show in terms of kpbs.

CR - C4-132189 - is defined for TS 29.274 for GTP conversion by P-GW.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with an element management system (EMS), the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a list of supported schemas for P-GW:

- **APN**: Provides Access Point Name statistics
- **APN Expansion**: Provides more granular GTP-C statistics on a per-APN and per-QCI level

- **Card**: Provides card-level statistics
- **Context**: Provides context service statistics
- **Diameter-acct**: Provides Diameter Accounting statistics
- **Diameter-auth**: Provides Diameter Authentication statistics
- **ECS**: Provides Enhanced Charging Service statistics
- **eGTP-C**: Provides Evolved GPRS Tunneling Protocol - Control message statistics
- **FA**: Provides FA service statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP**: Provides GPRS Tunneling Protocol - Prime message statistics
- **GTPU**: Provides GPRS Tunneling Protocol - User message statistics
- **HA**: Provides HA service statistics
- **IMSA**: Provides IMS Authorization service statistics
- **IP Pool**: Provides IP pool statistics
- **LMA**: Provides Local Mobility Anchor service statistics
- **P-GW**: Provides P-GW node-level service statistics
- **P-GW eGTP-C S2a**: Provides eGTP-C S2a interface statistics.
- **P-GW eGTP-C S2b**: Provides eGTP-C S2b interface statistics.
- **P-GW eGTP-C S5/S8**: Provides eGTP-C S5/S8 interface statistics.
- **Port**: Provides port-level statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **System**: Provides system-level statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When an EMS is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of an EMS parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on an EMS server.



Important For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
    - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
  - **Service Congestion Policies**: Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.



Important For more information on congestion control, refer to the *Congestion Control* chapter in the *System Administration Guide*.

Default and Dedicated EPC Bearers

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications

pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

In the StarOS 9.0 release and later, the Cisco EPC core platforms support one or more EPS bearers (default plus dedicated). An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in the case of a GTP-based S5/S8 interface, and between a UE and HSGW (HRPD Serving Gateway) in case of a PMIP-based S2a interface. In networks where GTP is used as the S5/S8 protocol, the EPS bearer constitutes a concatenation of a radio bearer, S1-U bearer and an S5/S8 bearer anchored on the P-GW. In cases where PMIPv6 is used the EPS bearer is concatenated between the UE and HSGW with IP connectivity between the HSGW and P-GW.



Important The P-GW supports GTP-based S5/S8 and PMIPv6 S2a capabilities, with no commercial support for PMIPv6 S5/S8.

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and P-GW in the GTP-based S5/S8 design, and between a UE and HSGW in the PMIPv6 S2a approach. If different QoS scheduling priorities are required between Service Data Flows, they should be assigned to separate EPS bearers. Packet filters are signalled in the NAS procedures and associated with a unique packet filter identifier on a per-PDN connection basis.

One EPS bearer is established when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. A PDN connection represents a traffic flow aggregate between a mobile access terminal and an external Packet Data Network (PDN) such as an IMS network, a walled garden application cloud or a back-end enterprise network. Any additional EPS bearer that is established to the same PDN is referred to as a dedicated bearer. The EPS bearer Traffic Flow Template (TFT) is the set of all 5-tuple packet filters associated with a given EPS bearer. The EPC core elements assign a separate bearer ID for each established EPS bearer. At a given time a UE may have multiple PDN connections on one or more P-GWs.

DHCP Support

The P-GW supports dynamic IP address assignment to subscriber IP PDN contexts using the Dynamic Host Control Protocol (DHCP), as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

The method by which IP addresses are assigned to a PDN context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. Dynamically assigned IP addresses for subscriber PDN contexts can be assigned through the use of DHCP.

The P-GW acts as a DHCP server toward the UE and a DHCP client toward the external DHCP server. The DHCP server function and DHCP client function on the P-GW are completely independent of each other; one can exist without the other.

DHCP supports both IPv4 and IPv6 addresses.

The P-GW does not support DHCP-relay.

Deferred IPv4 Address Allocation

Apart from obtaining IP addresses during initial access signalling, a UE can indicate via PCO options that it prefers to obtain IP address and related configuration via DHCP after default bearer has been established. This is also know as Deferred Address Allocation.

IPv4 addresses are becoming an increasingly scarce resource. Since 4G networks like LTE are always on, scarce resources such as IPv4 addresses cannot/should not be monopolized by UEs when they are in an ECM-IDLE state.

PDN-type IPv4v6 allows a dual stack implementing. The P-GW allocates an IPv6 address only by default for an IPv4v6 PDN type. The UE defers the allocation of IPv4 addresses based upon its needs, and relinquishes any IPv4 addresses to the global pool once it is done. The P-GW may employ any IPv4 address scheme (local pool or external DHCP server) when providing an IPv4 address on demand.

Support for Option 26 in DHCP

While fetching IPv4 address for the UE, P-GW acts as an independent DHCP server and client at the same time. It acts as a DHCP server towards the UE and as DHCP client towards the external DHCP server. In earlier release, support for exchange of certain DHCP options between the UE and the external DHCP server through the P-GW was added. This included support for relaying certain external DHCP server provided options (1, 3, 6, 28, and 43) to the UE along with the IPv4 address when deferred address allocation was configured with IP-Addralloc Proxy mode.

This feature adds support for Option 26 received in DHCP OFFER message from the DHCP server.

P-GW preserved the exchanged DHCP option 26 between the UE and the external DHCP server. P-GW relays this option for any future message exchanges between the UE and the external DHCP server. The external DHCP server component of the P-GW reserves and maintains the external DHCP server provided DHCP option so that when the UE renews or rebinds the DHCP lease, P-GW responds with the preserved value.

This feature introduces a behavior change with respect to renewal request. Earlier, when the ASR5500 was configured in DHCP proxy mode and when the DHCP server did not respond to a renewal request, a retransmission at time T2 (.85 * lease time) did not include both of the configured DHCP servers. DHCP lease got expired after retries exhaustion in the RENEW state.

With this feature, suppose the number of retransmission is configured as 2, then in RENEW state maximum 2 retries are done for the DHCP request messages. If no response is received from the DHCP server and state is changed to REBIND then also DHCP request messages is retried 2 times.

Old Behavior: Earlier, for lower values of "number of retransmission" (example >= 2), DHCP request message was not retried in the REBIND state.

New Behavior: Now, DHCP request message is retried for the number of times it is configured in both RENEW and REBIND state.

DHCPv6 Support

The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables the DHCP servers to pass the configuration parameters, such as IPv6 network addresses to IPv6 nodes. It offers the capability of allocating the reusable network addresses and additional configuration functionality automatically.

The DHCPv6 support does not just feature the address allocation, but also fulfills the requirements of Network Layer IP parameters. Apart from these canonical usage modes, DHCPv6's Prefix-Delegation (DHCP-PD) has also been standardized by 3GPP (Rel 10) for "network-behind-ue" scenarios.

P-GW manages IPv6 prefix life-cycle just like it manages IPv4 addresses, thus it is responsible for allocation, renew, and release of these prefixes during the lifetime of a session. IPv6 Prefix is mainly for the UE's session attached to P-GW, where as delegated prefix is for network/devices behind UE. For IPv6 prefixes. P-GW may be obtained from either local-pool, AAA (RADIUS/DIAMETER) or external DHCPv6 servers based on respective configuration. For Delegated IPv6 Prefix allocation, P-GW obtained it from external DHCPv6 servers based on configuration.

Unicast Address Support Feature: The IPv6 prefix delegation for the requested UE is either allocated locally or from an external DHCPv6 server by P-GW, GGSN, SAEGW based on configuration at these nodes. These DHCP messages are sent to the external DHCPv6 server using multicast address as destination address. In networks where there are large number of P-GW servers, but less number of DHCP servers, the DHCPv6 messages with multicast address have to travel through the entire network, increasing load on the network. The Unicast address support feature enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCP service. This feature is CLI controlled and the operator needs to configure a CLI to support for client unicast operation to the DHCP Server.

DHCPv6 support for P-GW covers the following requirements:

- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (Basic DHCPv6)
- RFC 3633, prefix delegation mechanism



Important For more information on DHCPv6 service configuration, refer to the *DHCPv6 Configuration* section of the *PDN Gateway Configuration* chapter.

Direct Tunnel Support

When Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality.

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel "switching" latency from the user plane. An additional advantage of direct tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The direct tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typically makes the decision to establish direct tunnel at PDP Context Activation. A direct tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request toward the GGSN).

A major consequence of deploying direct tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced of part of direct tunnel deployment. The Cisco GGSN and SGSN offer massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once direct tunnel is deployed.



Important For more information on direct tunnel support, refer to the *Direct Tunnel for 4G (LTE) Networks* chapter in this guide.

DNS Support for IPv4/IPv6 PDP Contexts

This feature adds functionality in P-GW for PDN type IPv4v6. in StarOS Release 15.0. Previously, if an MS requested an IPv4 DNS address, P-GW did not send the IPv4 DNS address.

MS may request for DNS server IPv4 or IPv6 addresses using the Protocol Configurations Options IE (as a container or as part of IPCP protocol configuration request) in PDP Context Activation procedure for PDP Type IPv4, IPv6, or IPv4v6. In that case, the P-GW may return the IP address of one or more DNS servers in the PCO IE in the PDP Context Activation Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008.

For PDP Type IPv4v6, if MS requested DNS server IPv4 address, it did not return anIPv4 address. Support is now added to respond with address requested by MS.

AAA server may also provide DNS Server IP Address in Access-Accept Auth Response. In such cases, AAA provided DNS server IPs takes priority over the one configured under APN.

When DNS server address is requested in PCO configuration, the following preference would be followed:

1. DNS values received from RADIUS Server.
2. DNS values locally configured with APN.
3. DNS values configured at context level with **ip name-servers** CLI.

Domain Based Flow Definitions

This solution provides improved flexibility and granularity in obtaining geographically correct exact IP entries of the servers by snooping DNS responses.

Currently, it is possible to configure L7 rules to filter based on domain (m.google.com). Sometimes multiple servers may serve a domain, each with its own IP address. Using an IP-rule instead of an http rule will result in multiple IP-rules; one IP-rule for each server "behind" the domain, and it might get cumbersome to maintain a list of IP addresses for domain-based filters.

In this solution, you can create ruledefs specifying hostnames (domain names) and parts of hostnames (domain names). Upon the definition of the hostnames/domain names or parts of them, the P-GW will monitor all the DNS responses sent towards the UE and will snoop only the DNS response, which has q-name or a-name as specified in the rules, and identify all the IP addresses resulted from the DNS responses. DNS snooping will be done on live traffic for every subscriber.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For Interactive Traffic class, the P-GW supports per-gateway service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The following matrix may be used to determine the Diffserv markings used based on the configured traffic class and Allocation/Retention Priority:

Table 1: Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

In addition, the P-GW allows configuration of diameter packets and GTP-C/GTP-U echo with DSCP values.

RAT-Type based DSCP Marking

Operators can perform DSCP marking on gateways such as P-GW, SAE-GW and GGSN, based on RAT-Type. It allows the operator to configure different QoS services and to optimize traffic based on the RAT-type: EUTRAN, GERAN and UTRAN.

RAT-Type based DSCP marking includes the following:

- Support for all QCI and ARP values.
- Support for Standard and non-Standard QCIs.
- If a particular RAT-Type is not configured, the DSCP marking functionality is applied to all RAT-Type.
- Applicable for Virtual APNs.
- During Inter-RAT hand-offs, DSCP marking is based on the RAT-Type of the current hand-off.
- DSCP marking per RAT-Type is only applicable for user data traffic and not for control traffic (GTP-C packets).



Important Backward compatibility is maintained for existing DSCP marking and IP-ToS functionalities.

GTP-U on per APN Basis

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.

The S-GW/P-GW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

Previously, DSCP marking table was configured on P-GW service level. As part of this requirement, CLI was added to associate the qos-qci-mapping table in APN.

Important The P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 84.

In order to be backward compatible with older configurations, if a DSCP marking table is associated with P-GW service and not with the APN, then the one in P-GW service will be used. If table is associated in both P-GW service and APN, then the one on APN will take precedence.

Dynamic GTP Echo Timer

The Dynamic GTP Echo Timer enables the eGTP and GTP-U services to better manage GTP paths during network congestion. As opposed to the default echo timer, which uses fixed intervals and retransmission timers, the dynamic echo timer adds a calculated round trip timer (RTT) that is generated once a full request/response procedure has completed. A multiplier can be added to the calculation for additional support during congestion periods.

Important For more information, refer to the *Configuring the GTP Echo Timer* section located in the *Configuring Optional Features on the P-GW* section of the *PDN Gateway Configuration* chapter.

Dynamic Policy Charging Control (Gx Reference Interface)

Dynamic policy and charging control provides a primary building block toward the realization of IMS multimedia applications. In contrast to statically provisioned architectures, the dynamic policy framework provides a centralized service control layer with global awareness of all access-side network elements. The centralized policy decision elements simplify the process of provisioning global policies to multiple access gateways. Dynamic policy is especially useful in an Always-On deployment model as the usage paradigm transitions from a short lived to a lengthier online session in which the volume of data consumed can be extensive. Under these conditions dynamic policy management enables dynamic just in-time resource allocation to more efficiently protect the capacity and resources of the network.

Dynamic Policy Control represents the ability to dynamically authorize and control services and application flows between a Policy Charging Enforcement Function (PCEF) on the P-GW and the PCRF. Policy control enables a centralized and decoupled service control architecture to regulate the way in which services are provisioned and allocated at the bearer resource layer.

The StarOS 9.0 release included enhancements to conform with 3GPP TS 29.212 and 29.230 functions. The Gx reference interface uses Diameter transport and IPv6 addressing. The subscriber is identified to the PCRF at session establishment using IMSI based NAIs within the Subscription-ID AVP. Additionally the IMEI within the Equipment-Info AVP is used to identify the subscriber access terminal to the policy server. The Gx reference interface supports the following capabilities:

- Authorize the bearer establishment for a packet flow
- Dynamic L3/L4 transfer of service data flow filters within PCC rules for selection and policy enforcement of downlink/uplink IP CAN bearers

- Support static pre-provisioned L7 rulebase name attribute as trigger for activating Inline Services such as Peer-to-Peer Detection
- Authorize the modification of a service data flow
- Revoke the authorization of a packet flow
- Provision PCC rules for service data flows mapped to default or dedicated EPS bearers
- Support P-GW initiated event triggers based on change of access network gateway or IP CAN
- Provide the ability to set or modify APN-AMBR for a default EPS bearer
- Create or modify QoS service priority by including QCI values in PCC rules transmitted from PCRF to PCEF functions

Enhanced Charging Service (ECS)

The Enhanced Charging Service provides an integrated in-line service for inspecting subscriber data packets and generating detail records to enable billing based on usage and traffic patterns. Other features include:

- Content Analysis Support, on page 33
- Content Service Steering, on page 34
- Support for Multiple Detail Record Types, on page 34
- Diameter Credit Control Application, on page 35
- Accept TCP Connections from DCCA Server, on page 35
- Gy Interface Support, on page 36

The Enhanced Charging Service (ECS) is an in-line service feature that is integrated within the system. ECS enhances the mobile carrier's ability to provide flexible, differentiated, and detailed billing to subscribers by using Layer 3 through Layer 7 deep packet inspection with the ability to integrate with back-end billing mediation systems.

ECS interacts with active mediation systems to provide full real-time prepaid and active charging capabilities. Here the active mediation system provides the rating and charging function for different applications.

In addition, ECS also includes extensive record generation capabilities for post-paid charging with in-depth understanding of the user session. Refer to Support for Multiple Detail Record Types, on page 34 for more information.

The major components include:

- **Service Steering**: Directs subscriber traffic into the ECS subsystem. Service Steering is used to direct selective subscriber traffic flows via an Access Control List (ACL). It is used for other redirection applications as well for both internal and external services and servers.
- **Protocol Analyzer**: The software stack responsible for analyzing the individual protocol fields and states during packet inspection. It performs two types of packet inspection:
  - **Shallow Packet Inspection**: inspection of the layer 3 (IP header) and layer 4 (e.g. UDP or TCP header) information.
  - **Deep Packet Inspection**: inspection of layer 7 and 7+ information. Deep packet inspection functionality includes:
    - Detection of URI (Uniform Resource Identifier) information at level 7 (e.g., HTTP, WTP, RTSP Uniform Resource Locators (URLs)).

- Identification of true destination in the case of terminating proxies, where shallow packet inspection would only reveal the destination IP address / port number of a terminating proxy.
- De-encapsulation of upper layer protocol headers, such as MMS-over-WTP, WSP-over-UDP, and IP-over GPRS.
- Verification that traffic actually conforms to the protocol the layer 4 port number suggests.

- **Rule Definitions**: User-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true. Expressions may contain a number of operator types (string, =, >, etc.) based on the data type of the operand. Each Ruledef configuration is consisting of multiple expressions applicable to any of the fields or states supported by the respective analyzers.
- **Rule Bases**: a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. It is possible to define a rule definition with different actions.

Mediation and Charging Methods

To provide maximum flexibility when integrating with billing mediation systems, ECS supports a full range of charging and authorization interfaces.

- **Pre-paid**: In a pre-paid environment, the subscribers pay for service prior to use. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or call ends. The pre-paid accounting server is responsible for authorizing network nodes (GGSNs) to grant access to the user, as well as grant quotas for either time connected or volume used. It is up to the network node to track the quota use, and when these use quotas run low, the network node sends a request to the pre-paid server for more quota.

  If the user has not used up the purchased credit, the server grants quota and if no credit is available to the subscriber the call will be disconnected. ECS and DCCA manage this functionality by providing the ability to setup quotas for different services.

  Pre-paid quota in ECS is implemented using DIAMETER Credit Control Application (DCCA). DCCA supports the implementation of real-time credit control for a variety of services, such as networks access, messaging services, and download services.

  In addition to being a general solution for real-time cost and credit control, DCCA includes these features:

  - **Real-time Rate Service Information** - DCCA can verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
  - **Support for Multiple Services** - DCCA supports the usage of multiple services within one subscriber session. Multiple Service support includes; 1) ability to identify and process the service or group of services that are subject to different cost structures 2) independent credit control of multiple services in a single credit control sub-session.

    Refer to Diameter Credit Control Application, on page 35*Diameter Credit Control Application* for more information.

- **Post-paid**: In a post-paid environment, the subscribers pay after use of the service. A AAA server is responsible for authorizing network nodes (GGSNs) to grant access to the user and a CDR system generates G-CDRs/eG-CDRs/EDRs/UDRs or Comma Separated Values (CSVs) for billing information on pre-defined intervals of volume or per time.



Important Support for the Enhanced Charging Service requires a service license; the ECS license is included in the P-GW session use license. For more information on ECS, refer to the *ECS Administration Guide*.

Content Analysis Support

The Enhanced Charging Service is capable of performing content analysis on packets of many different protocols at different layers of the OSI model.

The ECS content analyzers are able to inspect and maintain state across various protocols at all layers of the OSI stack. ECS system supports, inspects, and analyzes the following protocols:

- IP
- TCP
- UDP
- DNS
- FTP
- TFTP
- SMTP
- POP3
- HTTP
- ICMP
- WAP: WTP and WSP
- Real-Time Streaming: RTP and RTSP
- MMS
- SIP and SDP
- File analysis: examination of downloaded file characteristics (e.g. file size, chunks transferred, etc.) from file transfer protocols such as HTTP and FTP.

Traffic analyzers in enhanced charging subsystem are based on configured rules. Rules used for Traffic analysis analyze packet flows and form usage records. Usage records are created per content type and forwarded to a pre-paid server or to a mediation/billing system. A traffic analyzer performs shallow (Layer 3 and Layer 4) and deep (above Layer 4) packet inspection of the IP packet flows.

The Traffic Analyzer function is able to do a shallow (layer 3 and layer 4) and deep (above layer 4) packet inspection of IP Packet Flows.

It is able to correlate all layer 3 packets (and bytes) with higher layer trigger criteria (e.g. URL detected in a HTTP header) and it is also perform stateful packet inspection to complex protocols like FTP, RTSP, SIP that dynamically open ports for the data path and by this way, user plane payload is differentiated into "categories".

The Traffic Analyzer works on the application level as well and performs event based charging without the interference of the service platforms.

Important This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *ECS Administration Guide*.

Content Service Steering

Content Service Steering (CSS) directs selective subscriber traffic into the ECS subsystem (In-line services internal to the system) based on the content of the data presented by mobile subscribers.

CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of "rules" (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and applies to a subscriber through either a subscriber profile or an APN profile in the destination context.

Important For more information on CSS, refer to the *Content Service Steering* chapter of the *System Administration Guide*.

Important For more information on ACLs, refer to the *IP Access Control Lists* chapter of the *System Administration Guide*.

Support for Multiple Detail Record Types

To meet the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the Enhanced Charging Service (ECS) provides the following type of usage records:

- Event Detail Records (EDRs)
- Usage Detail Records (UDRs)

ECS provides for the generation of charging data files, which can be periodically retrieved from the system and used as input to a billing mediation system for post-processing. These files are provided in a standard format, so that the impact on the existing billing/mediation system is minimal and at the same time, these records contain all the information required for billing based on the content.

GTPP accounting in ECS allows the collection of counters for different types of data traffic into detail records. The following types of detail records are supported:

- **Event Detail Records (EDRs)**: An alternative to standard G-CDRs when the information provided by the G-CDRs is not sufficient to do the content billing. EDRs are generated according to explicit action statements in rule commands that are user-configurable. The EDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.
- **User Detail Records (UDRs)**: Contain accounting information related to a specific mobile subscriber. The fields to be reported in them are user-configurable and are generated on any trigger of time threshold, volume threshold, handoffs, and call termination. The UDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.

Important This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *ECS Administration Guide*.

Diameter Credit Control Application

Provides a pre-paid billing mechanism for real-time cost and credit control based on the following **standards**:

- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005

The Diameter Credit Control Application (DCCA) is used to implement real-time credit-control for a variety of end user services such as network access, Session Initiation Protocol (SIP) services, messaging services, download services etc.

Used in conjunction with ECS, the DCCA interface uses a mechanism to allow the user to be informed of the charges to be levied for a requested service. In addition, there are services such as gaming and advertising that may credit as well as debit from a user account.

DCCA also supports the following:

- **Real-time Rate Service Information:** The ability to verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services**: The usage of multiple services within one subscriber session is supported. Multiple Service support includes:
  - The ability to identify and process the service or group of services that are subject to different cost structures.
  - Independent credit control of multiple services in a single credit control sub-session.



Important This functionality is available for use with the Enhanced Charging Service, which requires a session-use license. For more information on ECS, refer to the *ECS Administration Guide*.

Accept TCP Connections from DCCA Server

This feature allows for peer Diameter Credit Control Application servers to initiate a connection the NGME.

This feature allows peer diameter nodes to connect to the NGME on TCP port 3868 when the diameter server is incapable of receiving diameter incoming diameter requests.



Important For more information on Diameter support, 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*.

Gy Interface Support

The Gy interface enables the wireless operator to implement a standardized interface for real time content based charging with differentiated rates for time based and volume based charging.

As it is based on a quota mechanism, the Gy interface enables the wireless operator to spare expensive Prepaid System resources.

As it enables time-, volume-, and event-based charging models, the Gy interface flexibly enables the operator to implement charging models tailored to their service strategies.

The Gy interface provides a standardized Diameter interface for real time content based charging of data services. It is based on the 3GPP standards and relies on quota allocation.

It provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an "online" or "prepaid" style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

Gy is a Diameter interface. As such, it is implemented atop, and inherits features from, the Diameter Base Protocol. The system supports the applicable Base network and application features, including directly connected, relayed or proxied DCCA servers using TLS or plaintext TCP.

In the simplest possible installation, the system exchanges 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 Cisco implementation is based on the following standards:

- RFC 4006 generic DCCA, including:
  - CCR Initial, Update, and Final signaling
  - ASR and RAR asynchronous DCCA server messages
  - Time, Total-Octets, and Service-Specific-Units quota management
  - Multiple independent quotas using Multiple-Services-Credit-Control
  - Rating-Group for quota-to-traffic association
  - CC-Failure-Handling and CC-Session-Failover features
  - Final-Unit-Action TERMINATE behavior
  - Tariff-Time-Change feature.
- 3GPP TS 32.299 online mode "Gy" DCCA, including:
  - Final-Unit-Action REDIRECT behavior
  - Quota-Holding-Time: This defines a user traffic idle time, on a per category basis, after which the usage is returned and no new quota is explicitly requested
  - Quota-Thresholds: These AVPs define a low value watermark at which new quota will be sought before the quota is entirely gone; the intent is to limit interruption of user traffic.

    These AVPs exist for all quota flavors, for example "Time-Quota-Threshold".

- Trigger-Type: This AVP defines a set of events which will induce a re-authentication of the current session and its quota categories.

Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the P-GW authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the P-GW for the "mobile router." If the P-GW receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session. For more information, see *Routing Behind the Mobile Station on an APN* chapter.

Gn/Gp Handoff Support

Integrated support of this feature requires that a valid session use license key be installed for both P-GW **and** GGSN. Contact your local Sales or Support representative for information on how to obtain a license.

In LTE deployments, smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. P-GW supports handovers as user equipment (UE) moves across different access technologies.

Cisco's P-GW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs, which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. These Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and P-GW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the P-GW works as an IP anchor for the EPC.

Important To support the seamless handover of a session between GGSN and P-GW, the two independent services must be co-located on the same node and configured within the same context for optimum interoperation.

Important For more information on Gn/GP handoffs, refer to Gn/Gp Interface, on page 10.

GTP-C Path Failure Enhancements and Improved Debugging Tools

In StarOS release 20.0, enhancements have been added to optimize GTP-C path failure functionality, and to improve the debug capability of the system for GTP-C path failure problems. These features will help Operators and Engineers to debug different aspects of the system that will help in identifying the root cause of GTP-C path failures in the network. These enhancements affect path failure detection via the s5, s8, s2b, and s2a interfaces.

The following enhancements are added as part of this feature:

- The node can be configured so that it does not detect a path failure if a low restart counter is received due to incorrect or spurious messages. This prevents call loss. The option to disable path failure due to Echo Request/Response and Control Message Request/Response messages is also available so that call loss is prevented in the event of a false path failure detection.
- More granularity has been added to GTP-C path failure statistics so that the root cause of issues in the network can be diagnosed more quickly.
- A path failure history for the last five path failures per peer is available to assist in debugging path failures in the network.
- Seamless path failure handling is implemented so that call loss is avoided during redundancy events.

Support to Avoid False Path Failure Detection

Several enhancements have been made to facilitate the node's ability to avoid false path failure detection:

- The software has been enhanced to avoid path failure detection due to spurious/incorrect messages from a peer. These messages can cause a large burst in network traffic due to the number of service deactivations and activations, resulting in network congestion. The **gtpc** command in *eGTP-C Service Configuration Mode* has been enhanced to resolve this issue. The **max-remote-restart-counter-change** keyword has been added to ensure false path failure detections are not detected as GTP-C path failures. For example, if the **max-remote-restart-counter-change** is set to 10 and the current peer restart counter is 251, eGTP will detect a peer restart only if the new restart counter is 252 through 255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP will detect a peer restart only if the new restart counter is 2 through 11.
- Also as part of this enhancement, new keywords have been added to the **path-failure detection-policy** command in *eGTP-C Service Configuration Mode* to enable or disable path failure detection.
- The **show egtp-service all** command in Exec Mode has been enhanced to indicate whether Echo Request/Echo Response Restart Counter Change and Control Message Restart Counter Change are enabled/disabled on the node.

Improved GTP-C Path Failure Statistics

Several improvements have been made to improve the quality of the GTP-C path failures so that operators/engineers can more quickly identify the cause of the failure.

- The output of the **show egtpc statistics path-failure-reasons** has been enhanced to show the number and type of control message restart counter changes at the demuxmgr and sessmgr. This command output has also been enhanced to track the number of path failures detected that were ignored at the eGTP-C layer.
- The **show egtpc peers path-failure-history** command output has been added to provide detailed information on the last five path failures per peer.
- The output of the **show egtp-service all name** and **show configuration** commands has been enhanced to show the current configuration settings specific to path GTP-C path failure detection policy.

IMS Emergency Bearer Handling

With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Signaling either happens on the default emergency bearer, or signaling and RTP media flow over separate dedicated emergency bearers. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions). Receiving emergency services in limited service state does not require a subscription.

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only
- MSI required, authentication optional
- All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.
- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

IP access lists, or access control lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber

- All subscriber sessions facilitated by a specific context

Important For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

IP Address Hold Timers

Also known as address quarantining, this subscriber-level CLI introduces an address hold timer to temporarily buffer a previously assigned IP address from an IP address pool to prevent it from being recycled and reassigned to a new subscriber session. It is especially useful during inter-RAT handovers that sometimes lead to temporary loss of the mobile data session.

This feature provides a higher quality user experience for location-based services where the remote host server needs to reach the mobile device.

Important Currently, the P-GW only supports an address hold timer with IPv4 addresses.

IPv6 and IPv4 Capabilities

Enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The P-GW offers the following IPv6 capabilities:

Native IPv6 and IPv6/IPv4 transport

- Support for any combination of IPv4, IPv6 or dual stack IPv4/v6 address assignment from dynamic or static address pools on the P-GW.
- Support for mobility packets wrapped with UDP and IPv4 headers.
- Support for native IPv6/IPv4 transport and service addresses on PMIPv6 S2a interface. Note that transport on GTP S5/S8 connections in this release is IPv4 based.
- Support for IPv6 transport for outbound traffic over the SGi reference interface to external Packet Data Networks.
- Support for downlink IPv4 data packets received from the SGi forwarded/redirected to a configured next-hop address if the subscriber session does not exist in the P-GW. If the next-hop is not ARP resolvable, then the packet will be dropped. The appropriate interface stats will be updated with the packets forward/dropped counts.

Important The **unconnected-address next-system** *ip address* keyword must be enabled to support the downlink IPv4 data packets forwarding/redirection.

IPv6 Connections to Attached Elements

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gx policy signaling interface
- Diameter Gy online charging reference interface
- S6b authentication interface to external 3GPP AAA server
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

Routing and Miscellaneous Features

- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (e.g. ECS)

IPv6 MTU Option Support in RA Message

In RFC-4861, there is a provision to send the Maximum Transmission Unit (MTU) in Router Advertisement (RA) messages. The P-GW now supports the sending of the IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types towards the UE. As a result, the UE can now send uplink data packets based on the configured MTU and perform data fragmentation at the source, if required. This feature also reduces the number of ICMPv6 *Packet Too Big Error* messages in the customer's network.

The MTU size is configurable via the Command Line Interface (CLI) on the GGSN and P-GW.

Supported Functionality

To support the IPv6 MTU Option in RA Message feature, the P-GW/GGSN supports the following functionality and behavior:

- The **ipv6 initial-router-advt option mtu value** command in *APN Configuration Mode* is available to enable/disable this feature per APN. By default, this feature is enabled for all APNs.
  - For the P-GW and SAEGW, IPv6 initial router advertisement option MTU value must be configured in *octets -integer 1280-2000*. The configured value is sent in the RA packet rather than the data tunnel MTU.



Important This value is used only for advertisement in RA packet and the gateway need not enforce this value. The behaviour of 'default' and 'no' options of this CLI remains the same.

  - For the P-GW and SAEGW, the session manager sends the MTU value that is configured via the CLI command **data-tunnel mtu** *1280-2000* in *APN Configuration Mode*.
  - For the GGSN, the RADIUS-returned value in the Framed-MTU Attribute Value Pair (AVP) takes precedence over the value configured via the **ppp mtu** *100-2000* CLI command in *APN Configuration Mode*.

- For the GGSN, if the RADIUS-returned MTU value is less than the minimum IPv6 MTU, then the minimum IPv6 MTU value of 1280 is sent in the IPv6 MTU option field in RA messages.
- For the GGSN, if the **ppp mtu***100-2000* CLI command is configured with an MTU value of less than 1280, then the minimum IPv6 MTU value is sent in the IPv6 MTU option field in RA messages.
- When no MTU value comes from the RADIUS server and both the above mentioned CLI commands are not configured, the default value of 1500 is used for the MTU.
- Support for the MTU option in RA messages is available in the GGSN/P-GW/SAEGW.
- This feature is supported on the P-GW independent of interfaces such as s2a/s2b/s5/s8.
- The MTU option in RA messages is supported for both IPv6 and IPv4v6 PDN types.
- The MTU option in RA messages is available in the output of the **monitor protocol** command.
- The same MTU value is sent by the gateway in initial and periodic RA messages for a calling.
- The behavior of sending the IPv6 MTU option in RA for a PDN call is persistent across session recovery and ICSR switchover.
- Existing MTU-related data path behavior for the GGSN/P-GW/SAEGW is not changed.

Restrictions/Limitations

Note the following restrictions/limitations for this feature:

- The GGSN/P-GW/SAEGW does not consider the GTP-U tunnel overhead while calculating the MTU value to be sent in the IPv6 MTU option in RAs. Therefore, the operator has to configure the **data-tunnel mtu** by considering the tunnel overhead. Refer to the *Link MTU Considerations* section in *Annex-C* of *3GPP TS 23.060*.
- Existing MTU-related data path behavior for the GGSN/P-GW/SAEGW is unchanged.
- If there is a Gn/Gp Handover followed by session recovery, operators will see the following behavior: The stateless IPv6 session is recovered with the MTU value configured for the current GGSN/P-GW service after the handover. This is existing behavior if the feature is not configured. With this feature enabled, the same recovered MTU value will be sent in periodic RA messages after such a handover occurs when followed by session recovery.
- This feature is not supported for eHRPD. As a result, in scenarios where an LTE-to-eHRPD to LTE-Handover or eHRPD-to-LTE Handover occurs, a new stateless IPv6 session is re-created using the latest APN configuration.
- With this feature enabled, there is no support for an MTU value received by the gateway via the S6b interface.

IPv6 Prefix-Based Search Support for LTE-WiFi Handoff

LTE-to-WiFi handoffs were failing for some UE devices for a specific customer during Inter-RAT testing for WiFi. The UE devices were using Stateless Address Auto Configuration. This issue was only seen from specific UE devices when the UE is sending the changed IPv6 address on Create Session Response (CSResp) messages during handoffs. Another vendor device had no issues for the LTE-to-WiFI handoff since it was sending the IPv6 address assigned initially during the Create Session Response (CSResp) from P-GW.

When the P-GW performed an IPv6 lookup of the existing LTE session based on the complete IPv6 128-bit address (Prefix + Intf ID), the handover would fail with the error EGTP_CONTEXT_NOT_FOUND.

Now, the P-GW performs the IPv6 lookup of the existing LTE session during an LTE-WiFi handoff using only the IPv6 prefix (64-bit). Operators now will see seamless handovers on these calls for UE devices with Stateless Address Auto Configuration. The P-GW will not reject the handoff request if the UE uses a different interface-ID from the one provided during call creation during handoffs for PDN types IPv6 and IPv4v6.



Important There are no changes on external interfaces. The only change as part of this feature is that the internal search to find the existing session is performed using the 64-bit IPv6 prefix during handoff.

Restrictions/Limitations

With Stateless Auto Configuration, when the UE uses a different interface-ID from the one provided by P-GW. The UE then later moves to another location that results in an S1/X2 handover with an S-GW change. As result, the S-GW may have a different IPv6 address for a PDN from the one maintained by the P-GW (that is, the IP Address provided during initial attach) for the same UE. This can result in a difference in the servedPDPPDNAddress element in the CDR from the P-GW and S-GW.

This restriction is due to an existing limitation in the 3GPP Modify procedure, such as Modify Bearer Request/Modify Bearer Response, where an exchange of the changed UE IPv6 address is not supported between the P-GW and S-GW during the S1/X2 handover.

It is assumed that the mediation devices will look into the 64-bit prefix of the IPv6 address in CDRs for Stateless Auto Configuration devices.

Local Break-Out

Provides a standards-based procedure to enable LTE operators to generate additional revenues by accepting traffic from visited subscribers based on roaming agreements with other mobile operators.

Local Breakout is a policy-based forwarding function that plays an important role in inter-provider roaming between LTE service provider networks. Local Breakout is determined by the SLAs for handling roaming calls between visited and home networks. In some cases, it is more beneficial to locally breakout a roaming call on a foreign network to the visited P-W rather than incur the additional transport costs to backhaul the traffic to the Home network.

If two mobile operators have a roaming agreement in place, Local Break-Out enables the visited user to attach to the V-PLMN network and be anchored by the local P-GW in the visited network. The roaming architecture relies on the HSS in the home network and also introduces the concept of the S9 policy signaling interface between the H-PCRF in the H-PLMN and the V-PCRF in the V-PLMN. When the user attaches to the EUTRAN cell and MME (Mobility Management Entity) in the visited network, the requested APN name in the S6a NAS signaling is used by the HSS in the H-PLMN to select the local S-GW (Serving Gateway) and P-GWs in the visited EPC network.

LTE Video Calling

In a Voice over LTE (VoLTE) scenario, the P-GW provides support for LTE Video Calling (LVC). No additional configuration is required to support this functionality.

The P-GW checks the data usage quota for a subscriber at video call setup and periodically during an active video call. The following functionality applies to post paid subscribers with data usage control:

Quota Check - Call Setup

If the P-GW determines that the subscriber has reached their data usage quota during the call setup:

- The audio bearer portion of the call is activated.The video bearer portion of the call is NOT activated.The P-GW sends the PCRF a Credit Control Request update (CCR-U) with "OUT_OF_CREDIT" event trigger and the Final-Unit-Action (FUA) received from the OCS.The PCRF removes the Service Data Flow (SDF) from the P-GW, and sends the P-CSCF indication of the failure of the video bearer channel setup.

Quota Check - During Active Video Call

If the subscriber exhausts their data usage during a video call:

- The audio bearer portion of the call is preserved.The video bearer portion of the call is terminated.The P-GW sends the PCRF CCR-U with "OUT_OF_CREDIT" event trigger and the Final-Unit-Action (FUA) received from the OCS.The PCRF removes the SDF from the P-GW, and sends the P-CSCF indication of the failure of the video bearer channel setup.

Mapping High Throughput Sessions on Session Managers

Session managers are upgraded to manage several high throughput sessions without sharing the core and without creating a bottleneck on the CPU load.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is checkpointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.



Note

- The selection of session managers for non-high throughput sessions remains the same in the existing setup.
- Non-high throughput sessions are placed along with the high throughput sessions on the same session manager.

Limitations

Managing high throughput sessions on a session manager has the following limitations:

- The following scenarios may result in placing two high throughput sessions on a session manager:
  - Initial attach from eHRPD/2G/3G sessions.
  - IP addresses – both IPv4 and IPv6, are placed on the same session manager.
  - For an S-GW, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.

- For a collapsed call, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
- In a Multi-PDN call from a UE that is capable of DCNR. For example: VoLTE and Internet capable of DCN will be placed on the same session manager.

- The DCNR flag is not defined by 3GPP for Wi-Fi. Therefore, a session cannot be assigned to a session manager during a Wi-Fi to LTE handover with the DCNR flag set.
- This feature manages and supports distribution of high throughput sessions on a session manager but does not guarantee high throughput for a subscriber.
- In some cases, the round robin mechanism could place a high throughput session on a session manager that was already loaded with other high throughput sessions.

MPLS EXP Marking of User Plane Traffic

Similar to 802.1p marking, MPLS EXP bit marking is supported for Enterprise APNs that use MPLS tunneling on the SGi interface on the P-GW. The QoS marking used in the LTE/EPC network (QCI per EPS bearer) is mapped to the 802.1p and MPLS EXP bit marking between the P-GW and L2/EPC switch and MPLS/PE routers (this is applicable to the upstream direction, from the P-GW to the Network).MPLS EXP marking related configuration is available as part of the QCI-QOS configuration table. MPLS EXP marking is selected based on QCI of the bearer to which that packet belongs.



Important The P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 84.

Mobile IP Registration Revocation

Mobile IP registration revocation functionality provides the following benefits:

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

Registration Revocation is a general mechanism whereby either the P-GW or the HSGW providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HSGW 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 HSGW sessions (sessions that could not be recovered)

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

Important For more information on MIP registration revocation support, refer to the *Mobile IP Registration Revocation* chapter in this guide.

MTU Size PCO

UEs usually use a hardcoded MTU size for IP communication. If this hardcoded value is not in sync with the network supported value, it can lead to unnecessary fragmentation of packets sent by the UE. Thus, in order to avoid unnecessary fragmentation, this feature helps in using the network-provided MTU size instead of the hardcoded MTU in UE.

3GPP defined a new PCO option in Release 10 specifications for the network to be able to provide an IPv4 MTU size to the UE. P-GW supports an option to configure a IPv4 Link MTU size in the APN profile.

If the UE requests IPv4 Link MTU size in the PCO options during Initial Attach or PDN connectivity request, the P-GW will provide the preconfigured value based on the APN.

If the MTU size configuration on APN is changed, the new MTU size will take effect only for new PDN connections and initial attaches. P-GW will not update for the existing PDN connections.

If UE does not request IPv4 Link MTU size, P-GW will not include the IPv4 Link MTU size.

Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or off-deck content services.

The MAG function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 tunnel for all user sessions toward the LMA function of the P-GW. When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMAs. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default & dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.

Important Up to 11 multiple PDN connections are supported.

Node Functionality GTP Echo

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new "node features" IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node's supported features. S-GW's supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover

This feature enables a seamless inter-technology roaming capability in support of dual mode e-HRPD/e-UTRAN access terminals.

The non-optimized inter-technology mobility procedure is rooted at the P-GW as the mobility anchor point for supporting handovers for dual radio technology e-HRPD/E-UTRAN access terminals. To support this type of call handover, the P-GW supports handoffs between the GTP-based S5/S8 (GTPv2-C / GTPv1-U) and PMIPv6 S2a tunneled connections. It also provisions IPv4, IPv6, or dual stack IPv4/IPv6 PDN connections from a common address pool and preserves IP addresses assigned to the UE during inter-technology handover. In the current release, the native LTE (GTP-based) P-GW service address is IPv4-based, while the e-HRPD (PMIP) address is an IPv6 service address.

During the initial network attachment for each APN that the UE connects to, the HSS returns the FQDN of the P-GW for the APN. The MME uses DNS to resolve the P-GW address. When the PDN connection is established in the P-GW, the P-GW updates the HSS with the IP address of the P-GW on PDN establishment through the S6b authentication process. When the mobile user roams to the e-HRPD network, the HSS returns the IP address of the P-GW in the P-GW Identifier through the STa interface and the call ends up in the same P-GW. The P-GW is also responsible for initiating the session termination on the serving access connection after the call handover to the target network.

During the handover procedure, all dedicated EPS bearers must be re-established. On LTE- handovers to a target e-HRPD access network, the dedicated bearers are initiated by the mobile access terminal. In contrast, on handovers in the opposite direction from e-HRPD to LTE access networks, the dedicated bearers are network initiated through Gx policy interactions with the PCRF server.

Finally, in order to support the inter-technology handovers, the P-GW uses common interfaces and Diameter endpoint addresses for the various reference points:

- S6b: Non-3GPP authentication
- Gx: QoS Policy and Charging
- Rf: Offline Charging

All three types of sessions are maintained during call handovers. The bearer binding will be performed by the HSGW during e-HRPD access and by the P-GW during LTE access. Thus, the Bearer Binding Event Reporting (BBERF) function needs to migrate between the P-GW and the HSGW during the handover. The HSGW establishes a Gxa session during e-HRPD access for bearer binding and releases the session during LTE access. The HSGW also maintains a limited context during the e-HRPD <-> LTE handover to reduce latency in the event of a quick handover from the LTE RAN back to the e-HRPD network.



Important For more information on handoff interfaces, refer to Supported Logical Network Interfaces (Reference Points), on page 6.

Online/Offline Charging

The Cisco EPC platform offers support for online and offline charging interactions with external OCS and CGF/CDF servers.

Online Charging

Gy/Ro Reference Interfaces

The StarOS 9.0 online prepaid reference interface provides compatibility with the 3GPP TS 23.203, TS 32.240, TS 32.251 and TS 32.299 specifications. The Gy/Ro reference interface uses Diameter transport and IPv6 addressing. Online charging is a process whereby charging information for network resource usage must be obtained by the network in order for resource usage to occur. This authorization is granted by the Online Charging System (OCS) upon request from the network. The P-GW uses a charging characteristics profile to determine whether to activate or deactivate online charging. Establishment, modification or termination of EPS bearers is generally used as the event trigger on the PCRF to activate online charging PCC rules on the P-GW.

When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource usage authorization that may be limited in its scope (e.g. volume of data or duration based). The OCS assigns quotas for rating groups and instructs the P-GW whether to continue or terminate service data flows or IP CAN bearers.

The following Online Charging models and functions are supported:

- Time based charging
- Volume based charging
- Volume and time based charging
- Final Unit Indication and termination or redirection of service data flows when quota is consumed
- Reauthorization triggers to rearm quotas for one or more rating groups using multi-service credit control (MSCC) instances
- Event based charging
- Billing cycle bandwidth rate limiting: Charging policy is enforced through interactions between the PDN GW and Online Charging Server. The charging enforcement point periodically conveys accounting information for subscriber sessions to the OCS and it is debited against the threshold that is established for the charging policy. Subscribers can be assigned a max usage for their tier (gold, silver, bronze for

example), the usage can be tracked over a month, week, day, or peak time within a day. When the subscriber exceeds the usage limit, bandwidth is either restricted for a specific time period, or dropped depending on their tier of service.

- Fair usage controls

Offline Charging

Ga/Gz Reference Interfaces

The Cisco P-GW supports 3GPP-compliant offline charging as defined in TS 32.251,TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally, when Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW and P-GWs support integrated Charging Transfer Functions (CTF) and Charging Data Functions (CDF). Each gateway uses Charging-ID's to distinguish between default and dedicated bearers within subscriber sessions. The Ga/Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP/S-FTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to FTP/S-FTP charging records between the CDF and CGF server. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc. The ASR 5500 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it also possible to enable file compression using protocols such as GZIP. The Offline Charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighbor CGF within the configurable polling interval, they will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct OCS servers (See Online Charging description above).

Rf Reference Interface

The Cisco EPC platforms also support the Rf reference interface to enable direct transfer of charging files from the CTF function of the P-GW to external CDF/CGF servers. This interface uses Diameter Accounting Requests (Start, Stop, Interim, and Event) to transfer charging records to the CDF/CGF. Each gateway relies on triggering conditions for reporting chargeable events to the CDF/CGF. Typically as EPS bearers are activated, modified or deleted, charging records are generated. The EPC platforms include information such as Subscription-ID (IMSI), Charging-ID (EPS bearer identifier) and separate volume counts for the uplink and downlink traffic.

Optimization for egtpinmgr Recovery

The software has been enhanced to optimize the recovery outage window in the event of an egtpinmgr task restart. The optimization has been achieved by optimizing the internal algorithms of egtpinmgr recovery as well as optimizing the data structures required. In addition, recovery time now is dependent only on the number of unique IMSIs and not on the number of sessions for an IMSI.

P-CSCF Recovery

Supports spec-based mechanism to support P-CSCF discovery for GTP-based S2b interface for WiFi integration. This is needed for Voice over WiFi service.

The P-GW can store the P-CSCF FQDN received during the initial registration with the AAA. Upon receiving the P-CSCF restoration flag from the MME/S-GW, the P-GW performs a new DNS query using the existing P-CSCF FQDN to provide the updated list of three P-CSCF IP addresses using PCO.

Peer GTP Node Profile Configuration Support

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of P-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with P-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

PMIPv6 Heartbeat

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The core functional entities Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) set up tunnels dynamically to manage mobility for a mobile node.

Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

PMIP heartbeats from the HSGW to the P-GW are supported per RFC 5847. Refer to the **heartbeat** command in the LMA Service mode or MAG Service mode respectively to enable this heartbeat and configure the heartbeat variables.



Important For more information on PMIPv6 Heartbeat support, refer to the *PMIPv6 Heartbeat* chapter in this guide.

Proxy Mobile IPv6 (S2a)

Provides a mobility management protocol to enable a single LTE-EPC core network to provide the call anchor point for user sessions as the subscriber roams between native EUTRAN and non-native e-HRPD access networks

S2a represents the trusted non-3GPP interface between the LTE-EPC core network and the evolved HRPD network anchored on the HSGW. In the e-HRPD network, network-based mobility provides mobility for IPv6 nodes without host involvement. Proxy Mobile IPv6 extends Mobile IPv6 signaling messages and reuses the HA function (now known as LMA) on the P-GW. This approach does not require the mobile node to be involved in the exchange of signaling messages between itself and the Home Agent. A proxy mobility agent (e.g. MAG function on HSGW) in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network.

The S2a interface uses IPv6 for both control and data. During the PDN connection establishment procedures the P-GW allocates the IPv6 Home Network Prefix (HNP) via Proxy Mobile IPv6 signaling to the HSGW. The HSGW returns the HNP in router advertisement or based on a router solicitation request from the UE. PDN connection release events can be triggered by either the UE, the HSGW or the P-GW.

In Proxy Mobile IPv6 applications the HSGW (MAG function) and P-GW (LMA function) maintain a single shared tunnel and separate GRE keys are allocated in the PMIP Binding Update and Acknowledgement messages to distinguish between individual subscriber sessions. If the Proxy Mobile IP signaling contains Protocol Configuration Options (PCOs) it can also be used to transfer P-CSCF or DNS server addresses

QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFT's) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco PDN GW offers all of the following bearer-level aggregate constructs:

QoS Class Identifier (QCI): An operator provisioned value that controls bearer level packet forwarding treatments (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). The Cisco EPC gateways also support the ability to map the QCI values to DiffServ code points in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.

To support 802.1p network traffic prioritization for use in grouping packets into various traffic classes, the P-GW enables operators to map QCI values to 802.1p priorities for uplink and downlink packets.

Important The P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 84.

Guaranteed Bit Rate (GBR): A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

Maximum Bit Rate (MBR): The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given Dedicated EPS bearer.

Aggregate Maximum Bit Rate (AMBR): AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

Policing: The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority.

RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- 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

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority**: Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm**: Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create "user defined" RADIUS server groups, as many as 399 (excluding "default" server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the P-GW supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.



Important For more information on RADIUS AAA configuration, 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*.

Removal of Private Extension-based Overcharging Feature

Prior to StarOS release 21.0, the Cisco P-GW and S-GW supported the sending and receiving of overcharging protection data via both a non-3GPP Private Extension Information Element (IE), and a 3GPP Indication IE.

However, since 3GPP support to exchange overcharging protection data exists, no operators were using the Overcharging Private Extension (OCP) based solution. It was also reported by some operators that the Private Extension IE carrying overcharging protection data sent by the P-GW was leading to issues at S-GWs of other vendors.

As a result, support for Private Extension-based Overcharging Support is being removed from the Cisco P-GW and S-GW. This has the benefit of preventing unexpected scenarios occurring due to the decoding of a Private Extension ID carrying overcharging protection data at the P-GW/S-GW of other vendors.

Previous and New Behavior for the P-GW

The following table describes the previous and new behavior at the P-GW for Create Session Request (CSReq) and Create Session Response (CSRsp) messages due to the removal of Private Extension Overcharging Support.

Table 2: Previous and New Behavior: CSReq and CSRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support

Scenario No.	IE Carrying OCP Capability Received from S-GW in CSReq	Old Behavior: IE carrying OCP Capability Sent to S-GW in CSRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in CSRsp
1	Indication IE	Indication IE	No change. Indication IE will be sent in CSRsp.
2	Private Extension IE	Both Private Extension and Indication IEs.	Private Extension IE received from S-GW is ignored. Indication IE is sent in CSRsp.
3	None	Both Private Extension and Indication IEs.	Only Indication IE is sent in CSRsp.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from S-GW is ignored. Only Indication IE is sent in CSRsp.

The following table describes the previous and new behavior in Modify Bearer Request (MBReq) and Modify Bearer Response (MBRsp) messages due to the removal of Private Extension Overcharging Support.

Table 3: Previous and New Behavior: MBRreq and MBRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support

Scenario No.	IE carrying OCP Capability Received from S-GW in MBReq	Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp
1	Indication IE	Indication IE	No Change. Indication IE is sent in MBRsp messages.
2	Private Extension IE	Private Extension IE	Private Extension IE received from S-GW is ignored. Indication IE is sent in MBRsp message.
3	None	Both Private Extension and Indication IEs.	Only the Indication IE is sent in MBRsp message.

Scenario No.	IE carrying OCP Capability Received from S-GW in MBReq	Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from the S-GW is ignored. Only the Indication IE is sent in the MBRsp message.

Previous and New Behavior for the S-GW

The following table describes the previous and new behavior in Create Session Response (CSRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

Table 4: Previous and New Behavior: CSRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
12	Indication IE	No change. OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in CSRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **Private Extension IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
3	Both Private Extension IE and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only OCP capability received as a part of the Indication IE is accepted.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **Private Extension IE and Indication IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
4	None	No change.	None	No change.

The following table describes the previous and new behavior in Modify Bearer Response (MBRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

Table 5: Previous Behavior and New Behavior: MBRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
1	Indication IE	No change. OCP capability received as part of Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **None**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, neither one of the two IEs is sent in the MBRsp to the MME for the OCP capability.
3	Both Private Extension ID and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only the OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.
4	None	None	None	No change.

Important In the current release, the S-GW will send a MBReq message with only the indication IE for the Pause/Start Charging procedure. The private extension IE is not sent.

Important If the S-GW receives only the private extension IE from the P-GW in the CSRsp/MBRsp message, then the S-GW ignores the private extension IE. As a result, the S-GW assumes that Overcharging Protection is NOT enabled for the P-GW. So, in this scenario, even if the overcharging condition is met at the S-GW, the S-GW will not send a MBReq message for Charging pause to the P-GW.

S-GW Restoration Support

S-GW Restoration helps in handling the S-GW failure in the EPC network. It allows affected PDNs that fail due to S-GW to be restored by selecting another S-GW to serve the affected PDNs. This avoids unnecessary flooding of signaling for PDN cleanup.

The P-GW maintains the sessions in case path failure is detected or if S-GW restart is detected during recovery IE on GTP-C signaling. The P-GW will ensure that any dropped packets in this scenario are not charged. The P-GW also rejects any bearer additions or modification requests received for the PDN connection maintained after the S-GW failure detection. This occurs until the PDN is restored.

Once the session has been restored by the MME and the P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW, then the P-GW continues forwarding any received downlink data and start charging them.

When a subscriber is in S-GW restoration phase, all RARs (expect for Session Termination) reject the PCEF. The P-GW rejects all internal updates which can trigger CCR-U towards the PCRF. The P-GW triggers a CCR-U with AN-GW changes for the PDNs that are restored if the S-GW has changed on restoration.

The MME/S4-SGSN is locally configured to know that the P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at the P-GW, it supports it for all S-GWs/MMEs.



Important Only MME/S4-SGSN triggered S-GW restoration procedure will be supported.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

The P-GW Restart Notification may also be used to signal that the peer P-GW has failed and not restarted. In this case, the P-GW Restart Notification contains a cause value: P-GW not responding. While sending the PRN, the S-GW includes the cause with this new cause value depending on the echo response.



Important For more details on this feature, refer to the *S-GW Restoration Support* chapter in this guide.

Source IP Address Validation

Insures integrity between the attached subscriber terminal and the PDN GW by mitigating the potential for unwanted spoofing or man-in-the-middle attacks.

The P-GW includes local IPv4/IPv6 address pools for assigning IP addresses to UEs on a per-PDN basis. The P-GW defends its provisioned address bindings by insuring that traffic is received from the host address that it has awareness of. In the event that traffic is received from a non-authorized host, the P- GW includes the ability to block the non-authorized traffic. The P-GW uses the IPv4 source address to verify the sender and the IPv6 source prefix in the case of IPv6.

SRVCC PS-to-CS Handover Indication Support

This feature helps in notifying the PCRF about the exact reason for PCC rule deactivation on Voice bearer deletion. This exact cause will help PCRF to then take further action appropriately.

This feature ensures complete compliance for SRVCC, including support for PS-to-CS handover indication when voice bearers are released. The support for SRVCC feature was first added in StarOS Release 12.2.

SRVCC service for LTE comes into the picture when a single radio User Equipment (UE) accessing IMS-anchored voice call services switches from the LTE network to the Circuit Switched domain while it is able to transmit or receive on only one of these access networks at a given time. This removes the need for a UE to have multiple Radio Access Technology (RAT) capability.

After handing over the PS sessions to the target, the source MME shall remove the voice bearers by deactivating the voice bearer(s) towards S-GW/P-GW and setting the VB (Voice Bearer) flag of Bearer Flags IE in the Delete Bearer Command message (TS 29.274 v9.5.0).

If the IP-CAN bearer termination is caused by the PS to CS handover, the PCEF may report related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER (TS 29.212 v10.2.0 and TS 23.203 v10.3.0).

Support for new AVP PS-to-CS-Session-Continuity (added in 3GPP Release 11) inside Charging Rule Install, which indicates if the bearer is selected for PS to CS continuity is not added.

Subscriber Level Trace

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the P-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S5/S8, S2a, SGi, and Gx. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal



Important Once the trace is provisioned, it can be provisioned through the access cloud via various signalling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5500 platform. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

In the current release, the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI. Once a subscriber level trace request is activated it can be propagated via the S5/S8

signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S5/S8: Create Session Request
- S5/S8: Modify Bearer Request
- S5/S8: Trace Session Activation (New message defined in TS 32.422)

Performance Goals: As subscriber level trace is a CPU intensive activity the max number of concurrently monitored trace sessions per Cisco P-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

3GPP tracing was enhanced in StarOS Release 15.0 to increase the number of simultaneous traces to 1000. The generated trace files are forwarded to external trace collection entity at regular intervals through (S)FTP if "push" mode is enabled. If the push mode is not used, the files are stored on the local hard drive and must be pulled off by the TCE using FTP or SFTP.



Important The number of session trace files generated would be limited by the total available hard disk capacity.

3GPP Tracing to Intercept Random Subscriber

Previously, a subscriber identifier like IMSI was required in order to enable trace. Sometimes operators want to enable a trace without knowing the subscriber ID. For example, an operator may want to monitor the next "n" number of calls, or monitor subscribers in a particular IMSI range.

3GPP tracing was enhanced in StarOS Release 15.0 to intercept random subscribers with this feature. The current session trace feature is either signaling or management based, which is very specific to a particular subscriber. The requirement is to trace random subscribers which are not explicitly linked or identified by IMSI in GTP messages or configured through CLI.

The random subscribers could be in an IMSI range, context activation in particular time intervals, etc.

The session trace is activated on demand for a limited period of time for specific analysis purposes. The maximum limit would restrict the number of random subscriber tracing. Random session trace will be given priority over signalling and management-based session trace.

Support for One Million S1-U Peers on the S-GW

Due to customer business requirements and production forecasts, support has been added to the StarOS for one million S1-U connections on a single S-GW.

The S1-U interface is the user plane interface carrying user data between an eNodeB and an S-GW received from the terminal. The StarOS now has the capability to scale the number of S1-U peers to one million per VPN context.

A new CLI command has been added to enable operators to set the number of S1-U peers for which statistics should be collected. The limit is restricted to less than one million peers (128k) due to StarOS memory limitations.

How it Works

The gtpumgr uses the following guidelines while allocating peers:

- When a session installation comes from the Session Manager, a peer is created. If statistics are maintained at the Session Manager, the gtpumgr also creates the peer record with the statistics.
- Peer records are maintained per service.
- The number of peers is maintained at the gtpumgr instance level. The limit is one million S1-U peers per gtpumgr instance.
- If the limit of one million peers is exceeded, then peer creation fails. It causes a call installation failure in the gtpumgr, which leads to an audit failure if an audit is triggered.

The feature changes impact all the interfaces/services using the gtpu-service including GGSN/S4-SGSN/SGW/PGW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW for:

- The Gn and Gp interfaces of the General Packet Radio Service (GPRS)
- The Iu, Gn, and Gp interfaces of the UMTS system
- The S1-U, S2a, S2b, S4, S5, S8, and S12 interfaces of the Evolved Packet System (EPS)

Recovery/ICSR Considerations

- After a session manager/gtpumgr recovery or after an ICSR switchover, the same set of peers configured for statistics collection is recovered.
  - Peers with 0 sessions and without statistics are not recovered.
  - Peers with 0 sessions and with statistics are recovered.
  - Peers with Extension Header Support disabled are recovered.
- While upgrading from a previous release, ensure the newer release chassis **gtpu peer statistics threshold** is equal to or greater than the previous release. This ensures that the GTPU peer statistics are preserved during the upgrade. For example, if you are upgrading from release 19.0 to 20.2, and the 19.0 system has 17,000 GTPU sessions, then configure the threshold on the 20.2 chassis to 17,000 as well.

Configuration/Restrictions

- Due to the large number of GTP-U entities connecting to the StarOS, Cisco recommends disabling the GTP-U Path Management feature.
- The configured threshold is not the hard upper limit for statistics allocation because of the distributed nature of system. It is possible that total GTP-U peers with statistics exceeds the configured threshold value to some extent.
- It is assumed that all 1,000,000 peers are not connected to the node in a point-to-point manner. They are connected through routers.
- There will not be any ARP table size change for the StarOS to support this feature.

TCP Window Size

Important This feature is not fully qualified in this release. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

The operator can restrict the effective window size of all downlink TCP packets. A new CLI command **window-size** is added in the Rulebase Configuration mode to enable this feature.

The P-GW updates the TCP packets with the configured value if the effective window size is greater than the configured window size. Otherwise, the P-GW does not modify the window size of the packet.

The newly updated window size might not be the same as the configured window size because the P-GW does not have control over the Window Scale option (sent with SYN flag). Therefore, the updated window size is rounded off to the nearest value calculated by the Window Scale option.

This feature is not applicable on non-SYN flows as they do not have the Window Scale option is not available.

When TCP Window Size is enabled, Rulebase changes and configuration changes are applicable to both newly created flows and existing flows. The changes will not be applicable if TCP Window Size feature is not enabled for these flows.

Note There will be a performance impact as PGW updates every downlink packet for a specified Rulebase where the configured window size is lesser than the effective windows size in the packet.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

  Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

  Logs are supported in both the Alert and the Alarm models.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through an element management system.

  The Alarm System is used only in conjunction with the Alarm model.



Important For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

Transaction Rate KPIs - Session Events Per Second

Key Performance Indicators (KPIs) did not differentiate between successful or unsuccessful PDN session activations and deactivations. In addition, the KPIs did not provide any information related to the Voice-over-LTE (VoLTE) service.

Session Events Per Second (SEPS) KPIs have been implemented to address the above issues. These KPIs measure the signaling load on the P-GW/ePDG. Further, network initiated setup/tear down KPIs have been added to measure the event rate for VoLTE call setup and tear down. Together, these measurements assist operators in performing network dimensioning/planning for the P-GW/ePDG node.

For the P-GW, both types of KPIs are supported on the S5, S8, S2a, and S2b Interfaces. Also for the P-GW, SEPS KPIs are supported for any associated eHRPD/PMIP service.

Specifically, the following KPIs have been implemented:

Session Events Per Second (SEPS)

Session Events per Second KPIs have been implemented to assist operators in measuring the signaling load on the P-GW/ePDG. These SEPS KPIs include the following:

- Total session events (session setup and tear down) per second.
- Successful Session Events (session setup and tear down) per second.
- Unsuccessful Session Events (session setup and tear down) per second.

N/w Initiated Setup/Tear down Events Per Second

Network initiated setup/tear down event KPIs have been implemented to assist operators in measuring Voice-over-LTE (VoLTE) call setup and tear down events rate at the P-GW/ePDG. Both Create Bearer Requests (CBReqs) and Delete Bearer Requests (DBReqs) originally initiated by the P-GW and CBReqs and

DBReqs initiated by the P-GW as a result of Home Subscriber Server (HSS)- and User Equipment (UE)-initiated events will be accounted for in these KPIs. The N/w Initiated Setup/Tear down Events Per Second KPIs include the following:

- Total N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second.
- Successful N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second.
- Unsuccessful N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second

Operation

The P-GW/ePDG contains 8 buckets for transaction rate statistics collection for both session events per second KPIs and N/w Initiated Setup/Tear down Events per Second KPIs. The buckets are based on a configurable bucket interval that is from 1 to 20 minutes in length. During the configured time interval, an average is computed and stored for the entire bucket interval.

After the first 8 bucket intervals have elapsed and statistics collected, the P-GW continues sequentially through the 8 bucket intervals and eventually overwrites the original 8 bucket-intervals with more recent data. In short, the 8 bucket intervals provide a running value for the last eight bucket-intervals for which the KPIs have been computed. While the statistics are eventually overwritten with new values, all statistic totals are added to the historical statistics, which are not overwritten.

UE Time Zone Reporting

This feature enables time-based charging for specialized service tariffs, such as super off-peak billing plans

Time Zone of the UE is associated with UE location (Tracking Area/Routing Area). The UE Time Zone Information Element is an attribute the MME tracks on a Tracking Area List basis and propagates over S11 and S5/S8 signalling to the P-GW.

Time zone reporting can be included in billing records or conveyed in Gx/Gy signaling to external PCRF and OCS servers.

User Location Change Reporting Support

The user information change reporting is enabled on GGSN via PCRF using GPRS specific event triggers and GPRS specific credit re-authorization triggers. The user information to be reported include Location Change Reporting (ULI) and Closed Subscriber Group Information Change reporting (UCI)

For Location change reporting for a subscriber session requested by GGSN, the SGSN includes the User Location Information (ULI) if the MS is located in a RAT Type of GERAN, UTRAN or GAN. It also includes the CGI, SAI or RAI depending on whether the MS is in a cell, a service or a routing area respectively. The SGSN may optionally include the User Location Information for other RAT Types.

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG info change reporting for a subscriber session requested by GGSN, the SGSN includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

Release 20.0 and later, support has been added to process and handle a MS Info Change notification received with valid information to identify a PDN (non-zero TEID and/or IMSI+NSAPI) and with appropriate ULI and/or UCI information. In case of collision between MS-Info-change message and NRUPC, GGSN will

process MS-info-change request first and send out its MS-info-change response. Then the NRUPC will be retried again.

Important CSG reporting is not yet supported on GGSN, P-GW, or SAEGW.

Limitations

Following are the limitations of this feature:

- UCI trigger from PCRF is not supported.
- The MS Info Change reporting action trigger will not be recovered if trigger if:
  - trigger is changed
  - MS reporting action has not gone in CPC/UPC/NRUPC
  - session manager (SM) recovery happens
- The MS Change info message is not supported if it comes on UE level.

3GPP ULI Reporting Support Enhanced

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

Feature Change

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Actiontowards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

Behavior Change

Previous of Change Reporting Action: Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

Behavior of MS Info Change Reporting Action: Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

Limitations

1. In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
2. In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.

Virtual APN Support

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address



Important For more information, refer to the **virtual-apn preference** command in *APN Configuration Mode Commands* in the *Command Line Interface Reference*.

Features and Functionality - Inline Service Support

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

Content Filtering

The Cisco P-GW 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 P-GW. 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 URLs or URIs 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 P-GW services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active P-GW 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) for the P-GW 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 P-GW either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

Header Enrichment: Header Insertion and Encryption

Header enrichment provides a value-added capability for mobile operators to monetize subscriber intelligence to include subscriber-specific information in the HTTP requests to application servers.

Extension header fields (x-header) are the fields that can be added to headers of a protocol for a specific purpose. The enriched header allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. Unrecognized fields should be ignored by the recipient and must be forwarded by transparent proxies.

Extension headers can be supported in HTTP/WSP GET and POST request packets. The Enhanced Charging Service (ECS) for the P-GW offers APN-based configuration and rules to insert x-headers in HTTP/WSP GET and POST request packets. The charging action associated with the rules will contain the list of x-headers to be inserted in the packets. Protocols supported are HTTP, WAP 1.0 and WAP 2.0 GET, and POST messages.

Important For more information on ECS, see the *ECS Administration Guide*.

The data passed in the inserted HTTP header attributes is used by end application servers (also known as Upsell Servers) to identify subscribers and session information. These servers provide information customized to that specific subscriber.

The Cisco P-GW can include the following information in the http header:

- User-customizable, arbitrary text string
- Subscriber's MSISDN (the RADIUS calling-station-id, in clear text)
- Subscriber's IMSI
- Subscriber's IP address
- S-GW IP address (in clear text)

X-Header encryption enhances the header enrichment feature by increasing the number of fields that can be supported and through encryption of the fields before inserting them.

The following limitations to insertion of x-header fields in WSP headers apply:

- x-header fields are not inserted in IP fragmented packets before StarOS v14.0.
- In case of concatenated request, x-header fields are only inserted in first GET or POST request (if rule matches for the same). X-header fields are not inserted in the second or later GET/POST requests in the concatenated requests. For example, if there is ACK+GET in packet, x-header is inserted in the GET packet. However, if GET1+GET2 is present in the packet and rule matches for GET2 and not GET1 x-header is still inserted in GET2. In case of GET+POST also, x-header is not inserted in POST.
- In case of CO, x-header fields are not inserted if the WTP packets are received out of order (even after proper reordering).
- If route to MMS is present, x-headers are not inserted.
- x-headers are not inserted in WSP POST packet when header is segmented. This is because POST contains header length field which needs to be modified after addition of x-headers. In segmented WSP headers, header length field may be present in one packet and header may complete in another packet.

Hash-Value Support for Header Enrichment

Hash-Value strings are implemented as a part of the Header Enrichment feature. P-GW is enhanced to receive and store hash values that are received from the PCRF for each subscriber. The stored hash value is inserted in the HTTP/WSP header making it available for operators to handle subscriber profiles.

Some Mobile Advertisement platforms generate a hashed string based on a subscriber's MSISDN value. When a hashed string is sent to Content Providers, they identify the subscriber's profile information and in turn insert advertisements on the subscriber's browser based on the user's profile.

To receive Hash-values from the PCRF, a new AVP: **Hash-Value**; with an octet-string data-type is implemented on the Gx interface. The AVP supports a maximum length of 80 characters. The P-GW ignores the hashed string if it exceeds the maximum length. The hash-value received from the PCRF is inserted in the HTTP/WSP header only if HTTP Header Enrichment is enabled for a subscriber.

The X-Header field is used to insert a Hash-Value in the HTTP/WSP headers. The Hash-Value can be encrypted based on the existing encryption mechanism of X-Header fields. These hash values (encrypted or not encrypted) are inserted in the HTTP/WSP header based on the x-header format configured under Charging Action configuration.

Note A Hash-Value is check-pointed as a part of the subscriber's session information. It is check-pointed immediately, once received from the PCRF.

IPNE Service Support

The P-GW 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 for wireless operators and partners to share and exchange session and network information to realize intelligent services. For detailed information on IPNE, refer to the *IP Network Enabler* chapter 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 characteristics—Source-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 *NAT Administration Guide.*

NAT64 Support

This feature helps facilitate the co-existence and gradual transition to IPv6 addressing scheme in the networks. Use of NAT64 requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises will continue to build and roll out IPv6 networks. However, because of the broad

scale IPv4 deployment, it is not practical that the world changes to IPv6 overnight. There is need to protect the IPv4 investment combined with the need to expand and grow the network will force IPv4 and IPv6 networks to co-exist together for a considerable period of time and keep end-user experience seamless.

The preferred approaches are to run dual stacks (both IPv4 and IPv6) on the end hosts, dual stack routing protocols, and dual stack friendly applications. If all of the above is available, then the end hosts will communicate natively using IPv6 or IPv4 (using NAT). Tunneling through the IPv4 or IPv6 is the next preferred method to achieve communication wherever possible. When all these options fail, translation is recommended.

Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa. The system supports a Stateful NAT64 translator based on IETF Behave WG drafts whose framework is described in draft-ietf-behave-v6v4-framework-10. Stateful NAT64 is available as part of the existing NAT licenses from the current system implementation. The NAT44 and NAT64 will co-exist on the chassis and share the resources needed for NATing.

Peer-to-Peer Detection

Allows operators to identify P2P traffic in the network and applying appropriate controlling functions to ensure fair distribution of bandwidth to all subscribers.

Peer-to-Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node can function as a client, a server, or both—a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.

Detecting peer-to-peer protocols requires recognizing, in real time, some uniquely identifying characteristic of the protocols. Typical packet classification only requires information uniquely typed in the packet header of packets of the stream(s) running the particular protocol to be identified. In fact, many peer-to-peer protocols can be detected by simple packet header inspection. However, some P2P protocols are different, preventing detection in the traditional manner. This is designed into some P2P protocols to purposely avoid detection. The creators of these protocols purposely do not publish specifications. A small class of P2P protocols is stealthier and more challenging to detect. For some protocols no set of fixed markers can be identified with confidence as unique to the protocol.

Operators care about P2P traffic because of the behavior of some P2P applications (for example, Bittorrent, Skype, and eDonkey). Most P2P applications can hog the network bandwidth such that 20% P2P users can generate as much as traffic generated by the rest 80% non-P2P users. This can result into a situation where non-P2P users may not get enough network bandwidth for their legitimate use because of excess usage of bandwidth by the P2P users. Network operators need to have dynamic network bandwidth / traffic management functions in place to ensure fair distributions of the network bandwidth among all the users. And this would include identifying P2P traffic in the network and applying appropriate controlling functions to the same (for example, content-based premium billing, QoS modifications, and other similar treatments).

Cisco's P2P detection technology makes use of innovative and highly accurate protocol behavioral detection techniques.



Important For more information on peer-to-peer detection, refer to the *ADC 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-tuple—source and destination IP addresses and ports, and protocol—information 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 *ECS Administration Guide*.



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

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the P-GW service.

Each of the following features requires the purchase of an additional license to implement the functionality with the P-GW service.



Important 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*.

3GPP R13 Emergency Call Support on the ePDG and P-GW

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support

emergency services. Emergency bearer services are provided to normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction. For more information see *3GPP R13 Emergency Call Support on the ePDG and P-GW* section.

AAA and Prefix Delegation DHCP Correlation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Currently at the DHCP server, DHCPv6 does not provide any mechanism to correlate allocated IPv6 (/64) prefix to a particular subscriber. This feature correlates the default prefix allocated from AAA server with the delegated prefix allocated from external DHCPv6 server during the PDN connection setup.

Options are available in DHCP Client Profile Configuration Mode to enable P-GW to send USER_CLASS_OPTION in DHCPv6 messages to external DHCPv6 server during delegated prefix setup.

APN Backoff Timer Support

Previously, the P-GW did not distinguish signaling traffic from Delay Tolerant or Low Priority devices such as low priority machine-to-machine traffic.

The UE was able to indicate its device profile to the MME via NAS and Attach Request messages. The MME was able to pass this information to the P-GW via the Signaling Priority Indication Information Element (IE) on the S5 interface. Some UEs may not have supported providing the Signaling Priority Indication IE on S5 interface to the P-GW. As a result, the P-GW could not distinguish between the signaling types. the current release, the P-GW can distinguish between these signaling types.

Also, during overload situations, the P-GW previously allowed new sessions from LAPI devices and treated the traffic from Low Access Priority Indicator (LAPI) devices with the same priority as the normal UEs. With the current StarOS release, during overload conditions, the P-GW can be configured to backoff the traffic that is identified as LAPI. The identification is based on either the APN configuration or the signaling priority indicator IE.

The backoff timer algorithm and the R12 GTP-C Load/Overload Control algorithm now work together. This feature provides the benefit of rejecting low priority calls, which, in turn allows for more bandwidth for high priority calls.

For additional information, refer to the *APN Backoff Timer Support* chapter in this guide.

Bulkstats for GTP-C Messages by ARP Value

To comply with the “Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority” to support emergency calls over Voice over LTE (VoLTE), several Key Performance Indicators (KPIs) have been introduced with this feature. This feature is utilized to collect statistics for total number of GTP-C messages received for Enhanced Multimedia Priority Service (eMPS) session for specified interval (in minutes). The list of GTP-C messages are defined in accordance with the GIR document. As part of this feature:

- The S-GW will generate peg counts of the total number of received GTP-C messages containing an Allocation and Retention Priority (ARP), chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW level.
- The P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the specific P-GW level.
- The peg counts for GTP-C messages are broken down by message type similar to existing GTP-C message counters. The bulkstats are broken down by applicable S-GW and P-GW service and S5, S8, S11, and S4 interfaces.

Bulkstats are added for eMPS session/message.

Piggy-back Message

For piggy-back messages, if either of the messages have matching ARP or result into converting non-eMPS session to eMPS session, then both messages are counted as eMPS message and corresponding statistics for both messages are incremented.

If Modify Bearer Request is piggy-backed with Create Bearer Response on S11 interface of S-GW and Create Bearer Response result into converting non-eMPS session into eMPS session, then Modify Bearer Response statistics will not increment for this Modify Bearer Request.

Bulkstats Collection and Reset

Bulkstats are added under eGTP-C Schema and pgw-egtpc-s5s8 Schema. These eMPS bulkstats in eGTP-C Schema and pgw-egtpc-s5s8 Schema holds value only for a bulkstat interval, that is, value of these bulkstats shows number of eMPS messages exchanged during the bulkstat interval.

For more information, see *Bulkstats for GTP-C Messages by ARP Value* section.

Common Gateway Access Support

Common Gateway Access support is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, P-GW, and GGSN to allow users to have the same user experience, independent of the access technology available.

In today's scenario, an operator must have multiple access networks (CDMA, eHRPD, and LTE) plus a GSM/UMTS solution for international roaming. Therefore, operators require a solution to allow customers to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE, or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

Dynamic RADIUS Extensions (Change of Authorization)

Use of Dynamic RADIUS Extensions (CoA and PoD) requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

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

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

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

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

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

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

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



Important For more information on dynamic RADIUS extensions support, refer to the *CoA, RADIUS, And Session Redirection (Hotlining)* chapter in this guide.

Expanded Prioritization for VoLTE/Emergency Calls

The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

For control message belonging to eMPS session or containing Allocation and Retention Priority (ARP) associated with eMPS profile, the DSCP marking is based on eMPS profile configured DSCP value.

As part of this enhancement, support is also added for marking of certain GTP-C message at the P-GW and S-GW for priority treatment as defined in the Government Industry Requirements (GIR) NS/EP NGN. For more information, see *Expanded Prioritization for VoLTE/Emergency Calls* section.

ePDG Selection Using PCO

The purpose of this feature is to enable the PGW to send the ePDG IP addresses in an operator PCO so that when connected to a WiFi network the UE will attach to the closest geographic ePDG. This will aid in setting up the IPSEC tunnel to the closest ePDG and therefore reducing latency for VoWiFi and other features.

A new CLI has been introduced to customize PCO options in the network.

Important This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Important ePDG PCO is supported only for the CS request which are received on the S5-S8 interface. This feature is not applicable for the GGSN calls.

For more information on this feature, see *ePDG Selection Using PCO* chapter of this guide.

GRE Protocol Interface Support

Use of GRE Interface Tunneling requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW supports GRE generic tunnel interfaces in accordance with RFC 2784, Generic Routing Encapsulation (GRE). The GRE protocol allows mobile users to connect to their enterprise networks through GRE tunnels.

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSec offers, for example).

GRE tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

Important For more information on GRE protocol interface support, refer to the *GRE Protocol Interface* chapter in this guide.

GTP-based S2a Interface Support

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD.

GTP-based S2a interface support is available on the P-GW and SAEGW. When the WLAN is considered as trusted by the operator, the Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the S2a interface to the P-GW. Support has been extended for WiFi-to-LTE handovers using Make and Break for the SAEGW service. Multi-PDN handovers are also supported as part of this feature.

Operators deploying on the SAEGW are now able to integrate Trusted WiFi network functionality using this feature.

Supported functionality includes:

- Initial Attach
- WiFi-to-LTE handover
- LTE-to-WiFi handover
- Multi-PDN handovers

GTP-based S2b Interface Support

Use of WiFi Integration functionality requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

This section describes the GTP-based S2b interface implementation on the P-GW. The S2b interface connects the P-GW with the ePDG. The UE tries to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies. So the UE can have independent PDN connections via multiple access types. The access types supported are 4G and Wifi.

The S2b interface implementation supports the following:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff



Important For more information on WiFi Integration functionality, refer to the *GTP-based S2b Interface Support on the P-GW and SAEGW*chapter in this guide.

Voice Over WiFi Support

When the UE moves from WiFI to LTE, the P-GW sends a Delete Bearer Request to the ePDG (WiFi access). Previously, the Delete Bearer Request was sent as soon as a Create Session Request for handoff was received at the P-GW. In some cases (for some specific handsets) this broke the IP sec tunnel between the handset and the WAP. In these instances, the handoff failed. To avoid handoff failure, the P-GW should send a Create Session Response first and delay the Delete Bearer Request until handoff is complete for UE. Next, UE

generates a Modify Bearer Request to indicate handoff completion and the Delete Bearer Request is only generated after the P-GW receives the Modify Bearer Request. This indicates that at the P-GW both access types (WiFi and LTE) will remain active until the Modify Bearer Request is received. When UE moves from LTE to WiFi, handoff completion occurs at the Create Session Response.

GTP Throttling

Use of GTP and Diameter Interface Throttling requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

This feature will help control the rate of incoming/outgoing messages on P-GW/GGSN. This will help in ensuring P-GW/GGSN doesn't get overwhelmed by the GTP control plan messages. In addition, it will help in ensuring the P-GW/GGSN will not overwhelm the peer GTP-C peer with GTP Control plane messages.

This feature requires shaping/policing of GTP (v1 and v2) control messages over Gn/Gp and S5/S8 interfaces. Feature will cover overload protection of P-GW/GGSN nodes and other external nodes with which it communicates. Throttling would be done only for session level control messages. Path management messages would not be rate limited at all.

External node overload can happen in a scenario where P-GW/GGSN generates signaling requests at a higher rate than other nodes can handle. If the incoming message rate is higher than the configured message rate, extra messages will get silently dropped. Also the actual call setup rate can be lower than the msg-rate configured, which could be due to delays in setting up the session due to many reasons like slow peer nodes or overloaded sm. Also the drops done as part of this throttling are silent drops, hence if path failure is configured for non-echo messages, path failure can be observed.

For protecting external nodes from getting overloaded from P-GW/GGSN control signaling, a framework will be used to handle shaping/policing of outbound control messages to external interfaces.

Bypass Rate Limit Function

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature.

This enhancement requires no additional license. Existing licenses for the GTP-Throttling Feature (RLF License) and the VoLTE Prioritized Handling feature have been applied and used as follows:

- **RLF License:** The GTP-Throttling feature license has been enhanced to accommodate the message-types based RLF throttling bypass.
- **VoLTE Prioritized Handling Feature License:** This license has been enhanced to accommodate the emergency call, priority call, and apn-names based RLF throttling bypass.

The GTP Throttling feature helps control the rate of incoming/outgoing messages on P-GW. It prevents the message flood from P-GW towards S-GW and MME. Currently, following outgoing messages are throttled by P-GW using the RLF framework:

- Create Bearer Request (CBR)
- Delete Bearer Request (DBR)
- Update Bearer Request (UBR)
- NRUPC
- IPCA
- NRDPC

Once throttling is enabled for outgoing messages, all outgoing messages are throttled except the Create Bearer Request (CBR) message, which is piggybacked with Create Session Response message.

This feature has been enhanced to control the bypassing of some messages being throttled.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.



Important For more information on these commands, refer to the *CLI Reference Guide.*

Operator can configure Overload Protection/RLF Throttling-override (Bypass RLF) on P-GW along with Overload Control feature at the egress side. In this scenario, the Overload Control based on peer's reduction metrics will take higher precedence and messages will be throttled based on Overload Control feature first.

If the message is passed to RLF throttling after Overload Control feature processing then the Throttling override (Bypass RLF) will be applied after that according to the configuration. If the Overload Control Feature is not configured and RLF throttling and Bypass RLF throttling is configured, then messages would be throttled based on RLF and Throttling Override (Bypass RLF) feature.



Important For more information on these commands, refer to R12 GTP-C Load and Overload Support, on page 87.

HSS and PCRF Based P-CSCF Restoration Support

Use of P-CSCF Restoration requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature enables support for P-CSCF restoration. 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 includes 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 For more information on this feature, refer to the *HSS and PCRF Based P-CSCF Restoration Support* chapter in this guide.

Inter-Chassis Session Recovery

Use of Interchassis Session Recovery requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The ASR 5500 provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 PSC/PSC2 hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total PSC/PSC2 failure will cause a PSC switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the MME Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Interchassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

- **Interchassis Communication**

  Chassis configured to support Interchassis Session Recovery communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

  - router identifier
  - chassis priority
  - SPIO MAC address

- **Checkpoint Messages**

  Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.



Important For more information on interchassis session recovery support, refer to the *Interchassis Session Recovery* chapter in the *System Administration Guide*.

IP Security (IPSec) Encryption

Use of Network Domain Security requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

IPSec encryption enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

The Cisco P-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.



Important For more information on IPSec support, refer to the *IPSec Reference*.

IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
- IPv6 Interface ID from the RADIUS Server



Important For more information on IPv6 Prefix Delegation, refer *IPv6 Prefix Delegation from the RADIUS Server and the Local Pool* chapter.

L2TP LAC Support

Use of L2TP LAC requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the P-GW and the corporation, an L2TP tunnel must be setup in the P-GW running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the P-GW and benefits from dynamic resource allocation and distributed message and data processing.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware or software issues. Tunnel state is preserved by copying the information across processor cards.



Important For more information on this feature support, refer to the *L2TP Access Concentrator* chapter in this guide.

Lawful Intercept

The feature use license for Lawful Intercept on the P-GW is included in the P-GW session use license.

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

Layer 2 Traffic Management (VLANs)

Use of Layer 2 Traffic Management requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as "tags" on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts; therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.



Important For more information on VLAN support, refer to the *VLANs* chapter in the *System Administration Guide*.

Local Policy Decision Engine

Use of the Local Policy Decision Engine requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The Local Policy Engine is an event-driven rules engine that offers Gx-like QoS and policy controls to enable user or application entitlements. As the name suggests, it is designed to provide a subset of a PCRF in cases where an operator elects not to use a PCRF or scenarios where connections to an external PCRF are disrupted.

Local policies are used to control different aspects of a session like QoS, data usage, subscription profiles, and server usage by means of locally defined policies. A maximum of 1,024 local policies can be provisioned on a P-GW system.

Local policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Potential uses cases for the Local Policy Decision Engine include:

- Disaster recovery data backup solution in the event of a loss of PCRF in a mobile core network.
- Dedicated bearer establishment for emergency voice calls.
- Network-initiated bearer establishment on LTE to non-3GPP inter-domain handovers.



Important For more information on configuring the Local Policy Decision Engine, refer to the *Configuring Local QoS Policy* section in the *PDN Gateway Configuration* chapter of this guide.

Modify Bearer Response using controlled parameters

The P-GW service provides configurable parameters to include Charging-ID, Charging FQDN or Charging Gateway address, and MSISDN in Modify Bearer Response. All Modify Bearer Response messages will send these parameters if CLI is enabled irrespective of scenarios like S-GW relocation and GnGp to LTE handover. This feature is not license-controlled and the behavior is controlled using CLI.

For more information on this feature, refer to the *Modify Bearer Response using controlled parameters* chapter in this guide.

MPLS Forwarding with LDP

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

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.

MPLS 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 label switching 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 the 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, the MPLS backbone automatically negotiates routes using the labels bound with the IP packets. Cisco P-GW 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 P-GW.

Important For more information on MPLS support, refer to the *Multi-Protocol Label Switching (MPLS) Support* chapter in this guide.

NEMO Service Supported

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

The P-GW may be configured to enable or disable Network Mobility (NEMO) service.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on 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).

Important For more information on NEMO support, refer to the *Network Mobility (NEMO)* chapter in this guide.

NEMO Support in GGSN

Use of Dynamic Network Mobile Routing (NEMO) for GGSN requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

NEMO support is added to P-GW and GGSN so that NEMO can be supported for subscribers roaming out on 3G (UMTS/GERAN) networks.

This feature supports standards-based NEMO feature on GGSN, which allows operators to support Enterprise VPN service with the advantage of faster deployment and flexible bandwidth arrangement for customers.

NEMO (NEtwork MObility) provides wireless connectivity between enterprise core network and remote sites over 3G/4G network. The wireless connection can be used as either primary link or backup link. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Enterprise VPN service is one of the main use case for this feature. Fast deployment and flexible bandwidth arrangement for customers are some of the advantages of this service. Customers include banks, financial institutions, multi-sited enterprises, city public safety departments, transportation fleet, etc.

Network Provided Location Information for IMS

Use of NPLI requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature enables the P-GW to provide the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone

AVP as requested by the PCRF. The P-GW will also provide the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

During bearer deactivation or UE detach procedure, the P-GW will provide the access network information to the PCRF within the 3GPP-User-Location-Info AVP and information on when the UE was last known to be in that location within User-Location-Info-Time AVP. If the PCRF requested User location info as part of the Required-Access-Info AVP and it is not available in the P-GW, then the P-GW will provide the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP.

Previously, the P-GW notified ULI/MS-TimeZone/PLMN-ID to ECS/IMSA/PCRF only when their value changed. With this feature, the P-GW receives NetLoc indication in the rules sent by ECS regardless of whether the values changed and it sends this to the ECS/IMSA/PCRF. If the P-GW receives NetLoc as '1', then it will inform MS-Timezone. If the P-GW receives NetLoc as '0', then it will inform ULI and ULI Timestamp. If ULI is not available in that case, then the PLMN-ID is sent. If NetLoc indication is received for an update, then the P-GW will indicate this information to the access side in the UBReq using the RetLoc Indication flag.

This is required for VoLTE and aids in charging and LI functionality in IMS domain. This feature allows EPC core to support an efficient way of reporting ULI and Time-Zone information of the subscriber to the IMS core network.

New Call Policy for Stale Sessions

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

If the new call policy is set to **reject release-existing-session** and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with new call policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

Non-standard QCI Support

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported on P-GW/GGSN (not standalone GGSN) and carriers can define QCI 128-254 to differentiate between various services/applications carriers provide to the end users in their network.



Important For more information on non-standard QCI support, refer to the *Extended QCI Options* chapter in this guide.

NetLoc for WiFi EPC

With this feature, the IMS network can retrieve location information of the UE from WLAN access network. This improves location related feature and functionality for the operator. This feature also helps in charging subscribers based on location information.

Please note that the support for LTE NetLoc already exists from prior releases. With this release, NetLoc support is extended for WLAN access. Basic implementation is already supported for passing necessary parameter to different internal modules like SM, IMSA and ECS. For more information, see *NetLoc for WiFi EPC* section.

Overcharging Protection Support

Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.

P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn't desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.

Once the criterion to signal "stop charging" is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. MBReq will have a new private extension IE to send "stop charging" and "start charging" indication to P-GW.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume sending downlink packets after receiving "stop charging" request when either of these conditions is met:

- When the S-GW (which had earlier sent "stop charging" in MBReq) sends "start charging" in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).



Important When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

Paging Policy Differentiation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram

packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.

Important P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Important For more information on paging policy differentiation, refer to the *Paging Policy Differentiation* chapter in this guide.

Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

Important For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

The existing **show apn statistics name** *apn-name* and **show apn statistics** *Exec Mode* CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.

Important For more detailed information, refer to the *Extended QCI Options* chapter in this guide.

Licensing

ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Piggyback Support on S2b Interface

This feature supports piggybacking of "Create Session Response" and "Create Bearer Request" messages on ePDG and P-GW over the S2b interface. If piggybacking flag is set by the ePDG in the Create Session Request, P-GW can now send Create Session Response and Create Bearer Request together to the ePDG and eliminate the possibility of reordering of these messages.

R12 GTP-C Load and Overload Support

GTP-C Load Control feature is a licensed, optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control information in order to mitigate overload situations for the overloaded node through actions taken by the peer node(s). This feature is supported over S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control Information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.

In brief, load control and overload control can be described in this manner:

- Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.



Important Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

R12 Load and Overload Factor Calculation Enhancement

In capacity testing and also in customer deployments it was observed that the chassis load factor for the R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

A new CLI command is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.



Important For more detailed information on this feature, refer to the *GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in this guide.

Operation

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, ((number of active sessions per service / max session allowed for the service license) * 100).

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

Retrieve MDN from S6b

As per the current implementation, during an initial attach, P-GW selects Mobile Directory Number (MDN) or Mobile Station International Subscriber Directory Number (MSISDN) from the S6b interface. Later, when the call is handed off from P-GW to other services like eHRPD/trusted WiFi/untrusted WiFi or the handoff is done from these services to the P-GW, then the MDN/MSISDN is picked from the create session (CS) request and the S6b authorized MDN/MSISDN is lost. As a result, different values of MDN/MSISDN are sent in the Rf records. Since, typically, operators use MDN to charge subscribers, this results in revenue loss.

This feature retains the MDN/MSISDN value from the S6b interface or the CS request, during the initial attach and even during handoff between P-GW and eHRPD/ trusted WiFi/untrusted WiFi. The MDN/MSISDN value does not change in the call lifetime. As a result, all Rf records of a session have the same MDN/MSISDN values.

A new keyword retain-mdn has been added to the CLI command authorize-with-hss. This CLI command keyword, when configured, retains the MDN/MSISDN value. If the CLI command keyword is not configured, the MDN/MSISDN value is not received from the S6b interface. In this case, the MDN/MSISDN value received in the CS request is used.



Important This feature is not applicable to GnGp handoff.

For more information on this feature, see *Retrieve MDN from S6b* chapter of this guide.

Session Recovery Support

The feature use license for Session Recovery on the P-GW is included in the P-GW session use license.

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

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. StarOS Release 9.0 adds the ability to support stateful intra-chassis session recovery for P-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active PSC/PSC2 during the upgrade process.



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

Smartphone Tethering Detection Support

Use of Smartphone Tethering Detection requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

On the P-GW, using the inline heuristic detection mechanism, it is now possible to detect and differentiate between the traffic from the mobile device and a tethered device connected to the mobile device.

Traffic Policing

Use of Per-Subscriber Traffic Policing requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Traffic policing allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers.

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APNs 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".



Important For more information on traffic policing, refer to the *Traffic Policing and Shaping* chapter in this guide.

Traffic Shaping

Traffic Shaping is a rate limiting method similar to Traffic Policing, but provides a buffer facility for packets exceeding the configured limit. Once packets exceed the data-rate, the packet is 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, the system can be configured to either drop the packets or retain it for the next scheduled traffic session.

Traffic will be shaped to the configured APN-AMBR value. Previously, data carried on non-GBR bearers was policed at the configured APN-AMBR rate. APN-AMBR policing dropped the data that did not match the configured APN-AMBR. With APN-AMBR traffic shaping, non-GBR data that does not match the configured APN-AMBR rate will be buffered. When enough memory tokens are available, the data will be transmitted. In addition, operators still have the option to allow operators to drop or transmit the data when the buffer limit is reached.



Important For more information on traffic shaping, refer to the *Traffic Policing and Shaping* chapter in this guide.

UBR Suppression Feature

The Update Bearer Request (UBR) Suppression feature is a license controlled feature. Please contact your Cisco account or service representative for more information.

As the bit rate is expressed in bps on Gx and kbps on GTP, P-GW does a round-off to convert a Gx request into a GTP request. When P-GW receives RAR from PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in Kbps) is already set for the bearer. The UBR suppression feature enables P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

A new CLI command, **suppress-ubr no-bitrate-change**, has been added to the P-GW service configuration to enable UBR suppression. Once the CLI is configured, P-GW suppresses the UBR if the bit rate is the same after the round-off.

When UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

To summarize, if the license is enabled and the CLI command **suppress-ubr no-bitrate-change** is configured for UBR suppression, then UBR is suppressed if bit rates in kbps are the same after round-off and all other parameters, such as QCI, ARP, and TFT, that might trigger UBR are also unchanged.

User Location Information Reporting

Use of User Location Information (ULI) Reporting requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

ULI Reporting allows the eNodeB to report the location of a UE to the MME, when requested by a P-GW.

The following procedures are used over the S1-MME interface to initiate and stop location reporting between the MME and eNodeB:

- **Location Reporting Control**: The purpose of Location Reporting Control procedure is to allow the MME to request that the eNodeB report where the UE is currently located. This procedure uses UE-associated signaling.
- **Location Report Failure Indication**: The Location Report Failure Indication procedure is initiated by an eNodeB in order to inform the MME that a Location Reporting Control procedure has failed. This procedure uses UE-associated signalling.
- **Location Report**: The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signalling.

The start/stop trigger for location reporting for a UE is reported to the MME by the S-GW over the S11 interface. The Change Reporting Action (CRA) Information Element (IE) is used for this purpose. The MME updates the location to the S-GW using the User Location Information (ULI) IE.

The following S11 messages are used to transfer CRA and ULI information between the MME and S-GW:

- **Create Session Request**: The ULI IE is included for E-UTRAN Initial Attach and UE-requested PDN Connectivity procedures. It includes ECGI and TAI. The MME includes the ULI IE for TAU/ X2-Handover procedure if the P-GW has requested location information change reporting and the MME support location information change reporting. The S-GW includes the ULI IE on S5/S8 exchanges if it receives the ULI from the MME. If the MME supports change reporting, it sets the corresponding indication flag in the Create Session Request message.
- **Create Session Response**: The CRA IE in the Create Session Response message can be populated by the S-GW to indicate the type of reporting required.

- **Create Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Modify Bearer Request**: The MME includes the ULI IE for TAU/Handover procedures and UE-initiated Service Request procedures if the P-GW has requested location information change reporting and the MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Modify Bearer Response**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Delete Session Request**: The MME includes the ULI IE for the Detach procedure if the P-GW has requested location information change reporting and MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Update Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Change Notification Request**: If no existing procedure is running for a UE, a Change Notification Request is sent upon receipt of an S1-AP location report message. If an existing procedure is running, one of the following messages reports the ULI:
  - Create Session Request
  - Create Bearer Response
  - Modify Bearer Request
  - Update Bearer Response
  - Delete Bearer Response
  - Delete Session Request

If an existing Change Notification Request is pending, it is aborted and a new one is sent.



Important Information on configuring User Location Information (ULI) Reporting support is located in the *Configuring Optional Features on the MME* section of the *Mobility Management Entity Configuration* chapter in the *MME Administration Guide*.

3GPP ULI Reporting Support Enhanced

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

Feature Change

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is

reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Actiontowards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

Behavior Change

Previous of Change Reporting Action: Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

Behavior of MS Info Change Reporting Action: Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

Limitations

1. In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
2. In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.

Configurable Behavior on PDN Type IPv4v6

With this enhancement, P-GW/GGSN provided a new CLI configuration to enable the following four options when MME/SGSN sets PDN type to IPv4v6 and Dual Address Flag (DAF) is set to False in Create Session Request or Create PDP Request.

1. Option 1: Assign IPv6 address using current method and respond with Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
2. Option 2: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
3. Option 3: Assign IPv6 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".
4. Option 4: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".

When the CLI is not configured, the default behavior is Option 1. The gateway supports multiple PDN connections for the same APN to accommodate for Option 1, Option 2, and the UE attempting a second PDN connection. It is possible to configure the CLI for each APN differently.

Previously, there was no configurable support for the type of PDN assigned and the cause code returned in a Create Session Response or Create PDP Response when a Create Session Request or CPC was received for IPv4v6 PDN with DAF False at the P-GW and GGSN.

How the PDN Gateway Works

This section provides information on the function of the P-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The P-GW supports the following network flows:

- PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network
- GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network

PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network

The following topics and procedure flows are included:

- Initial Attach with IPv6/IPv4 Access, on page 95
- PMIPv6 Lifetime Extension without Handover, on page 96
- PDN Connection Release Initiated by UE, on page 97
- PDN Connection Release Initiated by HSGW, on page 98
- PDN Connection Release Initiated by P-GW, on page 99

Initial Attach with IPv6/IPv4 Access

This section describes the procedure of initial attach and session establishment for a subscriber (UE).

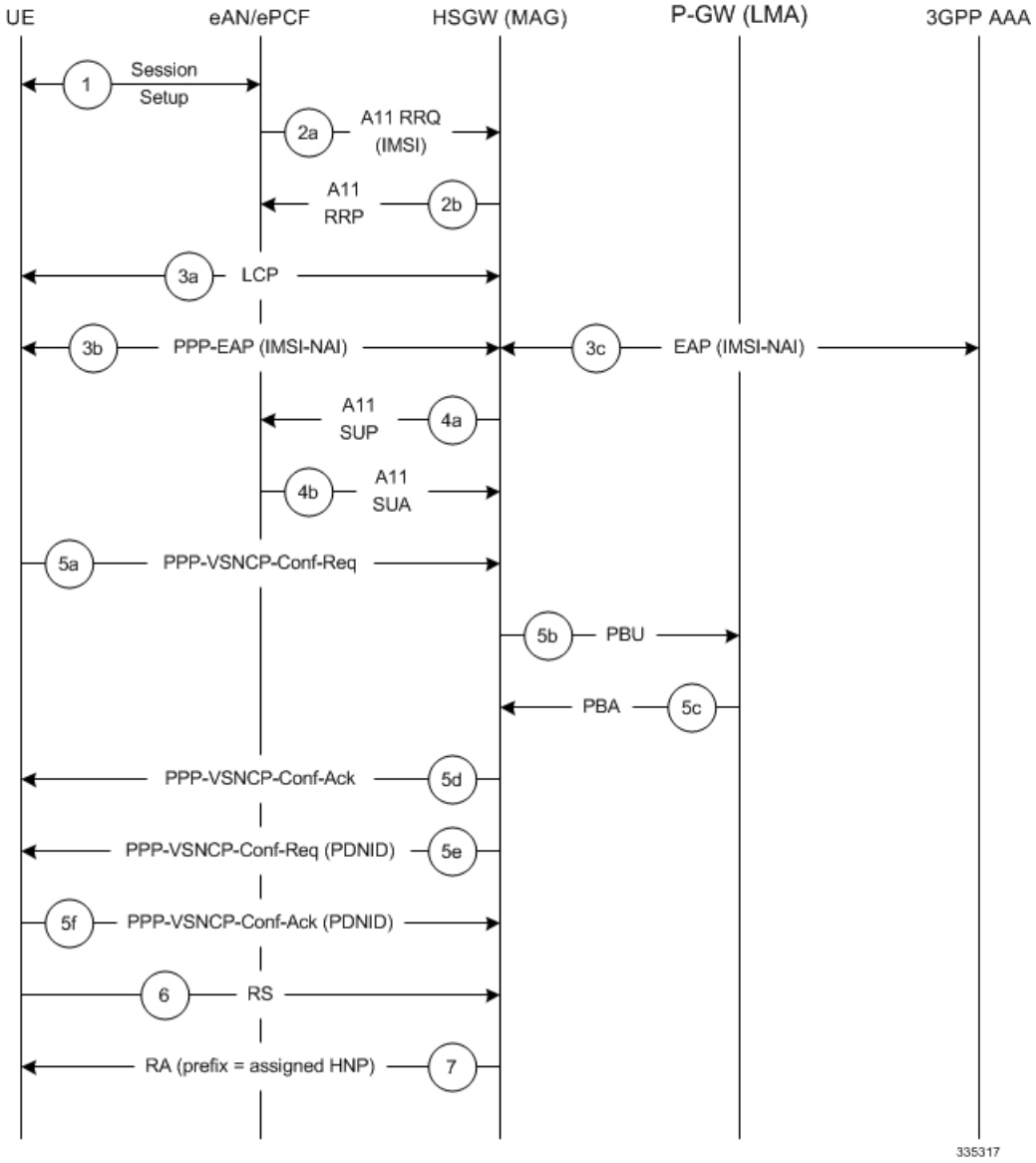


Table 6: Initial Attach with IPv6/IPv4 Access Call Flow Description

Step	Description
1	The subscriber (UE) attaches to the eHRPD network.
2a	The eAN/PCF sends an A11 RRQ to the HSGW. The eAN/PCF includes the true IMSI of the UE in the A11 RRQ.
2b	The HSGW establishes A10s and respond back to the eAN/PCF with an A11 RRP.
3a	The UE performs LCP negotiation with the HSGW over the established main A10.

Step	Description
3b	The UE performs EAP over PPP.
3c	EAP authentication is completed between the UE and the 3GPP AAA. During this transaction, the HSGW receives the subscriber profile from the AAA server.
4a	After receiving the subscriber profile, the HSGW sends the QoS profile in A11 Session Update Message to the eAN/PCF.
4b	The eAN/PCF responds with an A11 Session Update Acknowledgement (SUA).
5a	The UE initiates a PDN connection by sending a PPP-VSNCP-Conf-Req message to the HSGW. The message includes the PDNID of the PDN, APN, PDN-Type=IPv6/[IPv4], PDSN-Address and, optionally, PCO options the UE is expecting from the network.
5b	The HSGW sends a PBU to the P-GW.
5c	The P-GW processes the PBU from the HSGW, assigns an HNP for the connection and responds back to the HSGW with PBA.
5d	The HSGW responds to the VSNCP Conf Req with a VSNCP Conf Ack.
5e	The HSGW sends a PPP-VSNCP-Conf-Req to the UE to complete PPP VSNCP negotiation.
5f	The UE completes VSNCP negotiation by returning a PPP-VSNCP-Conf-Ack.
6	The UE optionally sends a Router Solicitation (RS) message.
7	The HSGW sends a Router Advertisement (RA) message with the assigned Prefix.

PMIPv6 Lifetime Extension without Handover

This section describes the procedure of a session registration lifetime extension by the P-GW without the occurrence of a handover.

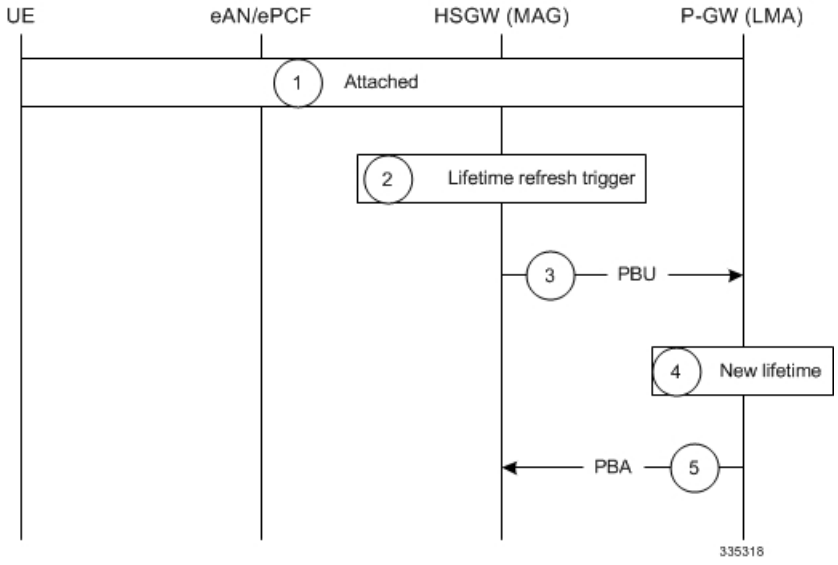


Table 7: PMIPv6 Lifetime Extension (without handover) Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW where PDNID=x and an APN with assigned HNP.
2	The HSGW MAG service registration lifetime nears expiration and triggers a renewal request for the LMA.
3	The MAG service sends a Proxy Binding Update (PBU) to the P-GW LMA service with the following attributes: Lifetime, MNID, APN, ATT=HRPD, HNP.
4	The P-GW LMA service updates the Binding Cache Entry (BCE) with the new granted lifetime.
5	The P-GW responds with a Proxy Binding Acknowledgment (PBA) with the following attributes: Lifetime, MNID, APN.

PDN Connection Release Initiated by UE

This section describes the procedure of a session release by the UE.

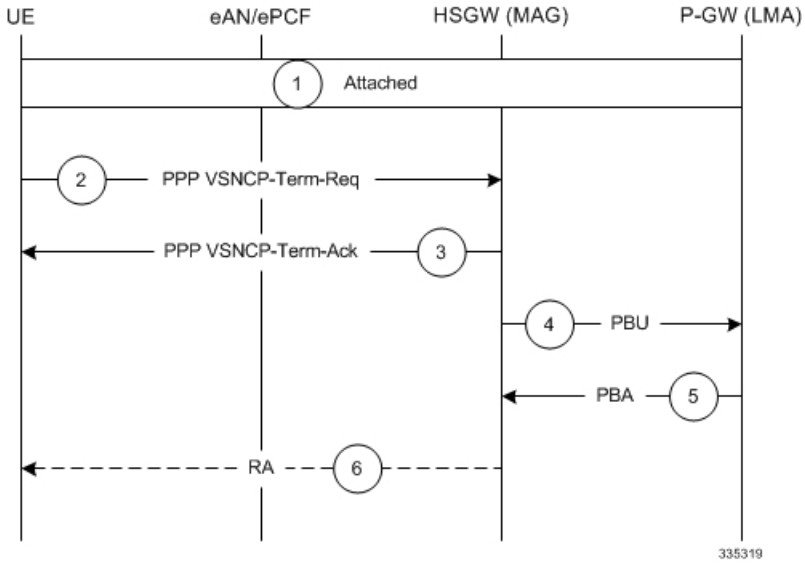


Table 8: PDN Connection Release by the UE Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The UE decides to disconnect from the PDN and sends a PPP VSNCP-Term-Req with PDNID=x.
3	The HSGW starts disconnecting the PDN connection and sends a PPP-VSNCP-Term-Ack to the UE (also with PDNID=x).
4	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, ATT=HRPD, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.

Step	Description
5	The P-GW looks up the Binding Cache Entry (BCE) based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).
6	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

PDN Connection Release Initiated by HSGW

This section describes the procedure of a session release by the HSGW.

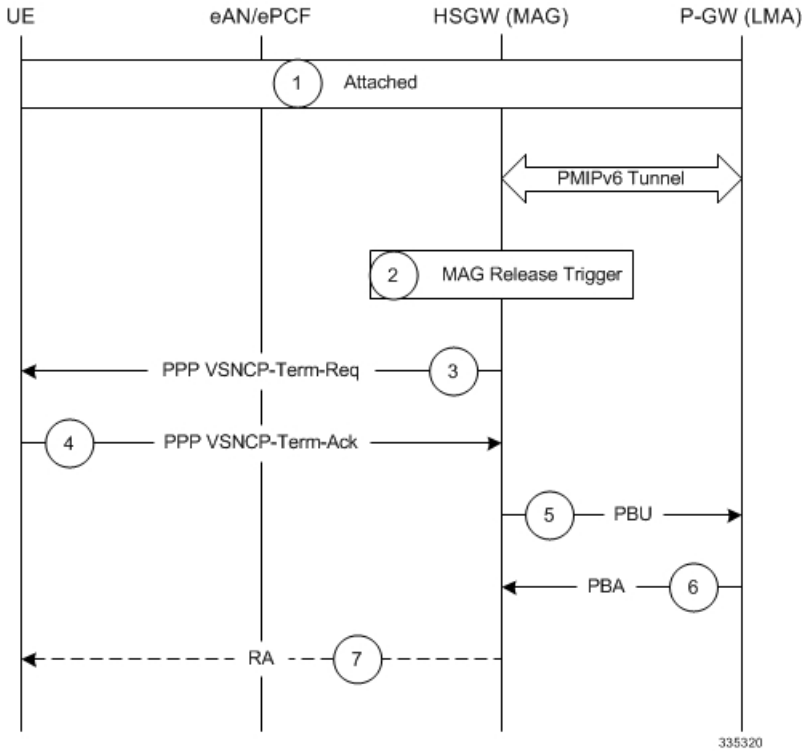


Table 9: PDN Connection Release by the HSGW Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The HSGW MAG service triggers a disconnect of the PDN connection for PDNID=x.
3	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
4	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).
5	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.

Step	Description
6	The P-GW looks up the BCE based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

PDN Connection Release Initiated by P-GW

This section describes the procedure of a session release by the P-GW.

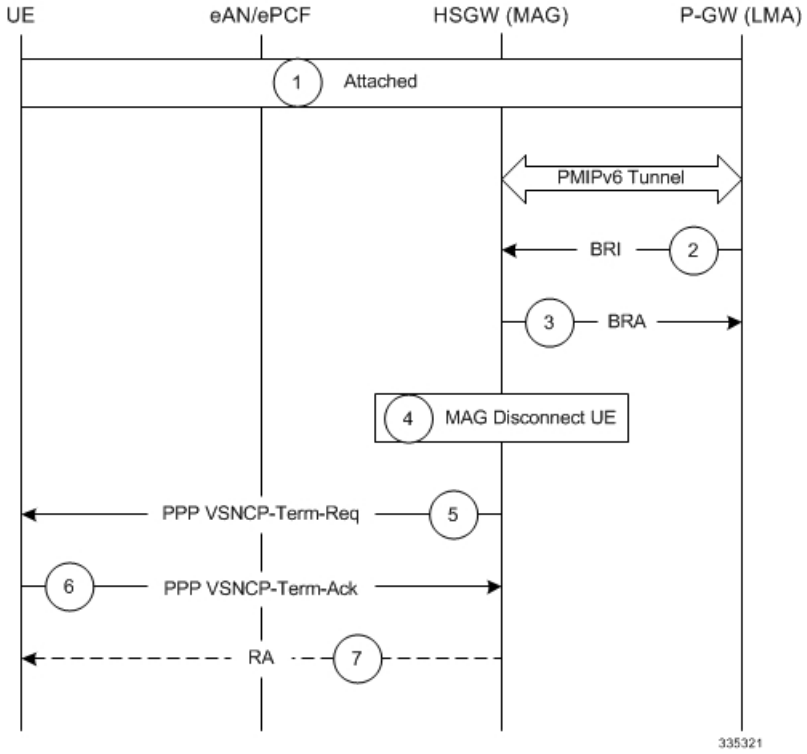


Table 10: PDN Connection Release by the P-GW Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	A P-GW trigger causes a disconnect of the PDN connection for PDNID=x and the PGW sends a Binding Revocation Indication (BRI) message to the HSGW with the following attributes: MNID, APN, HNP.
3	The HSGW responds to the BRI message with a Binding Revocation Acknowledgment (BRA) message with the sane attributes (MNID, APN, HNP).
4	The HSGW MAG service triggers a disconnect of the UE PDN connection for PDNID=x.
5	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
6	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network

The following topics and procedure flows are included:

- Subscriber-initiated Attach (initial), on page 100
- Subscriber-initiated Detach, on page 102

Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

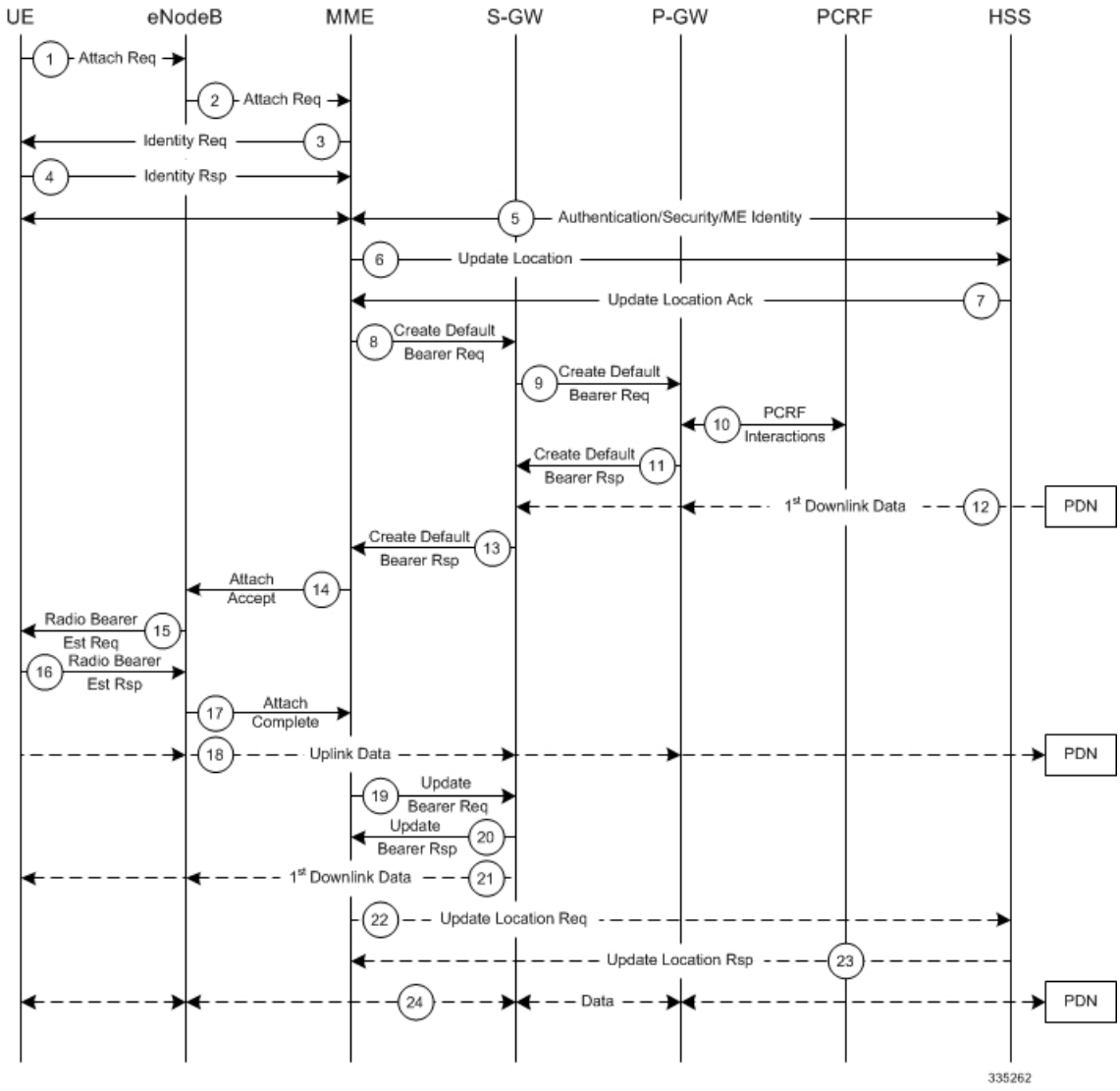


Table 11: Subscriber-initiated Attach (initial) Call Flow Description

Step	Description
1	The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an "MME selection function". The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.
8	The MME selects an S-GW using "Serving GW selection function" and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause "PDN GW selection function". Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.
9	The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.
10	If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.

Step	Description
11	The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.
12	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
13	The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.
14	The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.
15	The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.
16	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
17	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
18	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW.
19	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
20	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
21	The S-GW sends its buffered downlink packets.
22	After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.
23	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
24	Bidirectional data is passed between the UE and PDN.

Subscriber-initiated Detach

This section describes the procedure of detachment from the EPC network by a subscriber.

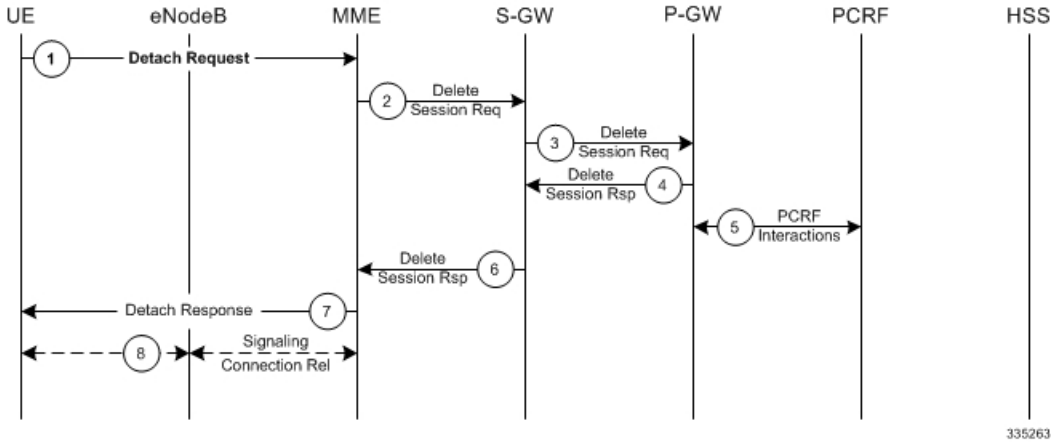


Table 12: Subscriber-initiated Detach Call Flow Description

Step	Description
1	The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.
2	The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.
8	The MME releases the S1-MME signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

Supported Standards

The P-GW service complies with the following standards.

- Release 12 3GPP References, on page 104
- Release 11 3GPP References, on page 104
- Release 10 3GPP References, on page 105
- Release 9 3GPP References, on page 105
- Release 8 3GPP References, on page 106
- 3GPP2 References, on page 107
- IETF References, on page 107
- Object Management Group (OMG) Standards, on page 109

Release 12 3GPP References



Important The P-GW currently supports the following Release 12 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

Release 11 3GPP References



Important The P-GW currently supports the following Release 11 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

Release 10 3GPP References



Important The P-GW currently supports the following Release 10 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.203: Policy and charging control architecture; Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)

Release 9 3GPP References



Important The P-GW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 22.115: Service aspects; Charging and billing
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.207: End-to-end Quality of Service (QoS) concept and architecture
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols

- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230: Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging application

Release 8 3GPP References



Important The P-GW currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture

- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 23.869: Support for Internet Protocol (IP) based IP Multimedia Subsystem (IMS) Emergency calls over General Packet Radio Service (GPRS) and Evolved Packet Service (EPS)
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 27.060: Mobile Station (MS) supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.210. Charging rule provisioning over Gx interface
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 36.300. EUTRA and EUTRAN; Overall description Stage 2
- 3GPP TS 36.412. EUTRAN S1 signaling transport
- 3GPP TS 36.413. EUTRAN S1 Application Protocol (S1AP)

3GPP2 References

- X.S0057-0 v3.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

IETF References

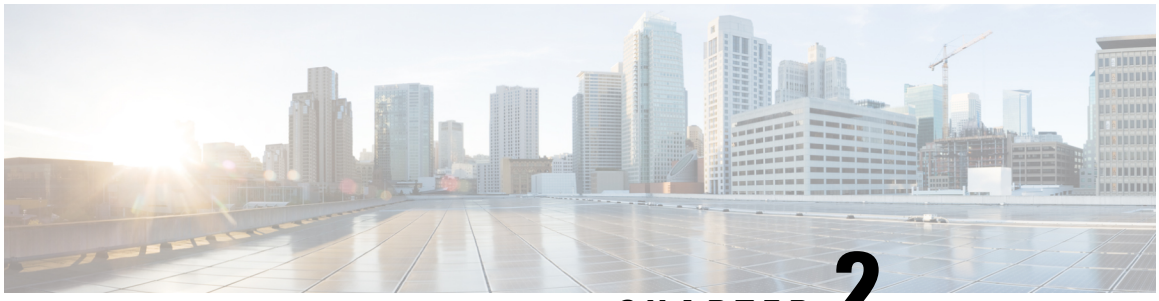
- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 1701, Generic Routing Encapsulation (GRE)

- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2473: Generic Packet Tunneling in IPv6 Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3162: RADIUS and IPv6
- RFC 3266: Support for IPv6 in Session Description Protocol (SDP)
- RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3589: Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3775: Mobility Support in IPv6
- RFC 3948: UDP Encapsulation of IPSec ESP Packets
- RFC 4004: Diameter Mobile IPv4 Application
- RFC 4005: Diameter Network Access Server Application
- RFC 4006: Diameter Credit-Control Application
- RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4306: Internet Key Exchange Protocol Version 2
- RFC 4739: Multiple Authentication Exchange in IKEv2 protocol
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5149: Service Selection for Mobile IPv6

- RFC 5213: Proxy Mobile IPv6
- RFC 5447: Diameter Mobile IPv6: Support for NAS to Diameter Server Interaction
- RFC 5555: Mobile IPv6 Support for Dual Stack Hosts and Routers
- RFC 5844: IPv4 Support for Proxy Mobile IPv6
- RFC 5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5846: Binding Revocation for IPv6 Mobility
- RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
- Internet-Draft (draft-ietf-dime-qos-attributes-07): QoS Attributes for Diameter
- Internet-Draft (draft-ietf-mip6-nemo-v4traversal-06.txt): Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-02.txt) IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress
- Internet-Draft (draft-meghana-netlmm-pmipv6-mipv4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group



CHAPTER 2

PDN Gateway Configuration

This chapter provides configuration information for the PDN Gateway (P-GW).

Important Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the P-GW product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

- Configuring the System as a Standalone eGTP P-GW, on page 111
- Configuring the System as a Standalone PMIP P-GW in an LTE-SAE Network, on page 137
- Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network, on page 156
- Configuring Optional Features on the P-GW, on page 173

Configuring the System as a Standalone eGTP P-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an eGTP P-GW in a test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- Information Required, on page 111
- How This Configuration Works, on page 118
- eGTP P-GW Configuration, on page 120

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 13: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	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.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 14: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S5/S8 Interface Configuration (To/from S-GW)	

Required Information	Description
Interface name	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.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.
IP address	S5/S8 interface IPv4 address.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).
eGTP Service Configuration	
eGTP Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 15: Required Information for PDN Context Configuration

Required Information	Description
PDN context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the PDN context is recognized by the system.

Required Information	Description
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 16: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

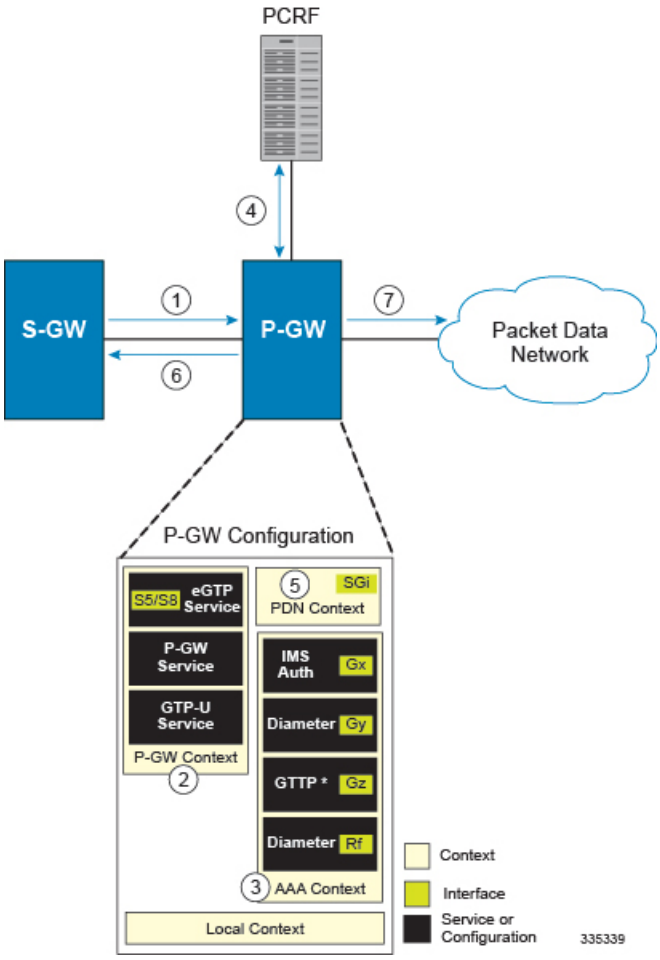
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.
Gz Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.

Figure 7: GTP P-GW Configuration Elements

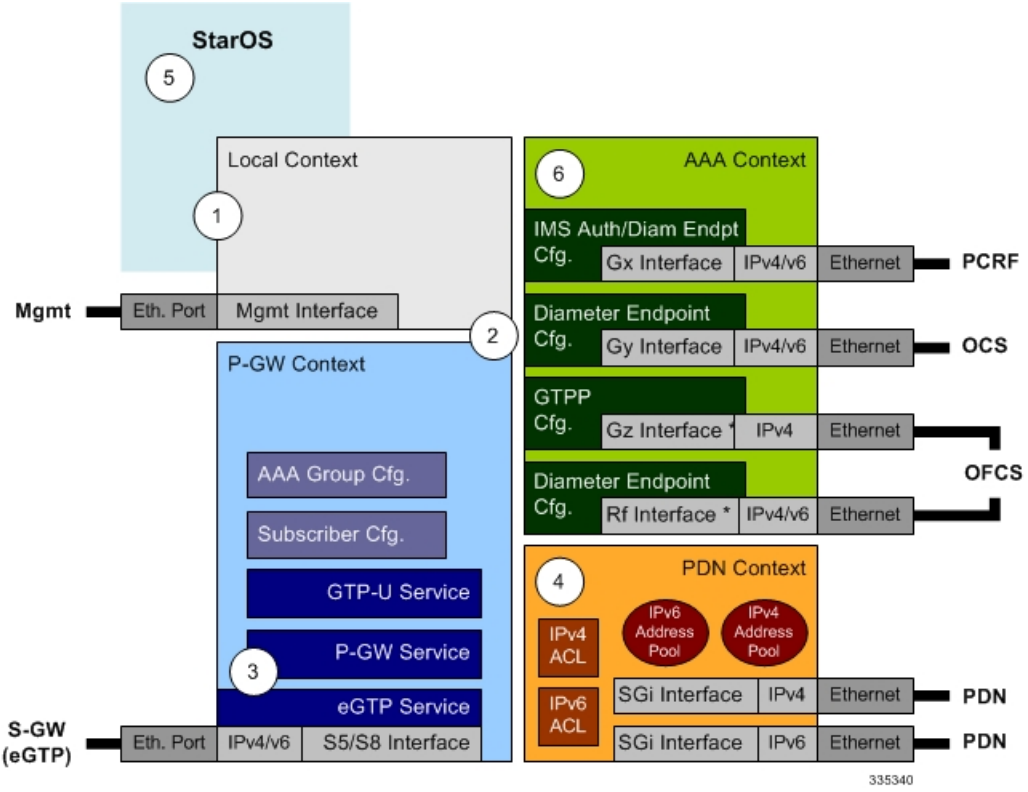


1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

eGTP P-GW Configuration

To configure the system to perform as a standalone eGTP P-GW:

Figure 8: eGTP P-GW Configurables



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the Initial Configuration, on page 121.

Step 3 Configure the system to perform as an eGTP P-GW and set basic P-GW parameters such as eGTP interfaces and IP routes by applying the example configurations presented in the P-GW Service Configuration, on page 125.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration, on page 125.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration, on page 126.

Step 6 Create a AAA context and configure parameters for policy by applying the example configuration in the Policy Configuration, on page 128.

Step 7 Verify and save the configuration by following the steps found in Verifying and Saving the Configuration, on page 130.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 121.

Step 2 Create the context where the eGTP service will reside by applying the example configuration in Creating and Configuring an eGTP P-GW Context, on page 121.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 122.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 123.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in Creating and Configuring an eGTP Service, on page 124.

Step 6 Create and configure a GTP-U service within the P-GW context by applying the example configuration in Creating and Configuring a GTP-U Service, on page 124.

Step 7 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 124.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

Creating and Configuring an eGTP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv4 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```
configure
  gtpp single-source
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name>
      ip address <ipv4_address>
      exit
    gtpp group default
      gtpp charging-agent address <gz_ipv4_address>
      gtpp echo-interval <seconds>
      gtpp attribute diagnostics
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix <string>
      gtpp dictionary <name>
      gtpp server <ipv4_address> priority <num>
      gtpp server <ipv4_address> priority <num> node-alive enable
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    exit
  subscriber default
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

Notes:

- **gtpp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- The S5/S8 (P-GW to S-GW) interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.
- Set the GTPP group setting for Gz accounting.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
```

```
ims-auth-service <gx_ims_service_name>
aaa group <rf-radius_group_name>
dns primary <ipv4_address>
dns secondary <ipv4_address>
ip access-group <name> in
ip access-group <name> out
mediation-device context-name <pgw_context_name>
ip context-name <pdn_context_name>
ipv6 access-group <name> in
ipv6 access-group <name> out
active-charging rulebase <name>
end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The **associate accounting-policy** command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in the Creating and Configuring an eGTP P-GW Context, on page 121.

Use the following configuration to create an APN that includes Gz interface parameters:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      bearer-control-mode mixed
      selection-mode sent-by-ms
      accounting-mode gtpp
      gtpp group default accounting-context <aaa_context_name>
      ims-auth-service <gx_ims_service_name>
      ip access-group <name> in
      ip access-group <name> out
      ip context-name <pdn_context_name>
      active-charging rulebase <gz_rulebase_name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The accounting-mode GTPP and GTPP group commands configure this APN for Gz accounting.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
```

```
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
   aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

Creating and Configuring an eGTP Service

Use the following configuration example to create the eGTP service:

```
configure
   context <pgw_context_name>
      egtp-service <egtp_service_name> -noconfirm
         interface-type interface-pgw-ingress
         validation mode default
         associate gtpu-service <gtpu_service_name>
         gtpc bind address <s5s8_interface_address>
         end
```

Notes:

- Co-locating a P-GW service on the same ASR 5500 requires that the **gtpc bind address** command uses the same IP address the P-GW service is bound to.

Creating and Configuring a GTP-U Service

Use the following configuration example to create the GTP-U service:

```
configure
   context <pgw_context_name>
      gtpu-service <gtpu_service_name> -noconfirm
         bind ipv4-address <s5s8_interface_address>
         end
```

Notes:

- The **bind** command can also be specified as an IPv6 address using the **ipv6-address** command.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure
   context <pdn_context_name> -noconfirm
```

```
interface <sgi_ipv4_interface_name>
   ip address <ipv4_address>
interface <sgi_ipv6_interface_name>
   ipv6 address <address>
   end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service, on page 125.

Step 2 Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring a Static IP Route, on page 125.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-service <pgw_service_name> -noconfirm
           plmn id mcc <id> mnc <id>
           associate egtp-service <egtp_service_name>
           associate qci-qos-mapping <name>
           end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to the Configuring QCI-QoS Mapping, on page 130 for more information.
- Co-locating a P-GW service on the same ASR 5500 requires the configuration of the **associate pgw-service** *name* command within the P-GW service.

Configuring a Static IP Route

Use the following example to configure an IP Route for control and user plane data communication with an eGTP Serving Gateway:

```
configure
   context <pgw_context_name>
      ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>
      end
```

P-GW PDN Context Configuration

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```
configure
   context <pdn_context_name> -noconfirm
```

```
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
      aaa group default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv4_interface_name> <pdn_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv6_interface_name> <pdn_context_name>
    end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
```

```
ruledef static
  icmp any-match = TRUE
  exit
charging-action <name>
  <action>
    .
    .
  <action>
  exit
charging-action icmp
  billing-action egcdr
  exit
charging-action qci3
  content-id <id>
  billing-action rf
  qos-class-identifier <id>
  allocation-retention-priority <priority>
  tft packet-filter qci3
  exit
charging-action static
  service-identifier <id>
  billing-action rf
  qos-class-identifier <id>
  allocation-retention-priority <priority>
  tft packet-filter qci3
  exit
packet-filter <packet_filter_name>
  ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
  ip remote-port { = <port_number> | range <start_port_number> to
<end_port_number> }
  exit
rulebase default
          exit
rulebase <name>
  <rule_base>
    .
    .
  <rule_base>
  exit
rulebase <gx_rulebase_name>
  dynamic-rule order first-if-tied
  egcdr tariff minute <minute> hour <hour>(optional)
  billing-records egcdr
  action priority 5 dynamic-only ruledef qci3 charging-action qci3
  action priority 100 ruledef static charging-action static
  action priority 500 ruledef default charging-action icmp
  action priority 570 ruledef icmp-pkts charging-action icmp
  egcdr threshold interval <interval>
  egcdr threshold volume total <bytes>
  end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Charging actions define the action to take when a rule definition is matched.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- The billing-action egcdr command in the charging-action *qc13*, *icmp*, and *static* examples is required for Gz accounting.
- The Gz rulebase example supports the Gz interface for offline charging. The **billing-records egcdr** command is required for Gz accounting. All other commands are optional.



Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

Policy Configuration

Procedure

Step 1 Configure the policy and accounting interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 128.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 130.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind Ethernet ports to interfaces supporting traffic between this context and a PCRF, an OCS, and an OFCS:

```
configure
   context <aaa_context_name> -noconfirm
      interface <gx_interface_name>
         ipv6 address <address>
         exit
      interface <gy_interface_name>
         ipv6 address <address>
         exit
      interface <gz_interface_name>
         ip address <ipv4_address>
         exit
      interface <rf_interface_name>
         ip address <ipv4_address>
         exit
```

```
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
        diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gz_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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*.

DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using the following method, as configured within an APN:

DHCP-proxy: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

There are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.

Important This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer to the *DHCP Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and P-GW service as described in *eGTP P-GW Configuration* section of this chapter.

To configure the DHCP service:

Procedure

Step 1 Create the DHCP service in system context and bind it by applying the example configuration in the DHCP Service Creation, on page 131.

Step 2 Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the DHCP Server Parameter Configuration, on page 131.

Step 3 Verify your DHCP Service configuration by following the steps in the DHCPv6 Service Configuration Verification, on page 137.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* section.

DHCP Service Creation

Use the following example to create the DHCP service to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
        bind address <ip_address> [nexthop-forwarding-address <nexthop_ip_address>
 [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1>
[out_mpls_label_value2]]]
         end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <*nexthop_ip_address*> **[mpls-label input** <*in_mpls_label_value*> **output** <*out_mpls_label_value1*> **[** *out_mpls_label_value2* **]]** applies DHCP over MPLS traffic.

DHCP Server Parameter Configuration

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
```

```
dhcp-service <dhcp_svc_name>
   dhcp server <ip_address> [priority <priority>
   dhcp server selection-algorithm {first-server | round-robin}
   lease-duration min <minimum_dur> max <max_dur>
   dhcp deadtime <max_time>
   dhcp detect-dead-server consecutive-failures <max_number>
   max-retransmissions <max_number>
   retransmission-timeout <dur_sec>
   end
```

Notes:

- Multiple DHCP services can be configured. Each service can have multiple DHCP servers configured by entering **dhcp server** command multiple times. A maximum of 225 DHCP services can be configured with maximum of 8 DHCP servers configurations per DHCP service.
- The **dhcp detect-dead-server** command and **max-retransmissions** command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with **max-retransmissions** command.

DHCP Service Configuration Verification

Procedure

Step 1 Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

show dhcp service all

This command produces an output similar to that displayed below where DHCP name is *dhcp1*:

```
Service name:                      dhcp1
Context:                                isp
Bind:                                   Done
Local IP Address:                       150.150.150.150
Next Hop Address:                       192.179.91.3
             MPLS-label:
              Input:                    5000
         Output:                        1566    1899
Service Status:                         Started
Retransmission Timeout:                 3000 (milli-secs)
Max Retransmissions:                    2
Lease Time:                             600 (secs)
Minimum Lease Duration:                 600 (secs)
Maximum Lease Duration:                 86400 (secs)
DHCP Dead Time:                         120 (secs)
DHCP Dead consecutive Failure:          5
DHCP T1 Threshold Timer:                50
DHCP T2 Threshold Timer:                88
DHCP Client Identifier:                 Not Used
DHCP Algorithm:                         Round Robin
DHCP Servers configured:
 Address: 150.150.150.150               Priority: 1
DHCP server rapid-commit:               disabled
DHCP client rapid-commit:               disabled
DHCP chaddr validation:                 enabled
```

Step 2 Verify the DHCP service status by entering the following command in Exec Mode:

```
show dhcp service status
```

DHCPv6 Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) for IPv6 to enable the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCPv6 configuration is done within an APN.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and APN as described in P-GW PDN Context Configuration, on page 151.

To configure the DHCPv6 service:

Procedure

Step 1 Create the DHCPv6 service in system context and bind it by applying the example configuration in the DHCPv6 Service Creation, on page 133.

Step 2 Configure the DHCPv6 server and other configurable values for Renew Time, Rebind Time, Preferred Lifetime, and Valid Lifetime by applying the example configuration in the DHCPv6 Server Parameter Configuration, on page 134.

Step 3 Configure the DHCPv6 client and other configurable values for Maximum Retransmissions, Server Dead Tries, and Server Resurrect Time by applying the example configuration in the DHCPv6 Client Parameter Configuration, on page 134.

Step 4 Configure the DHCPv6 profile by applying the example configuration in the DHCPv6 Profile Configuration, on page 135.

Step 5 Associate the DHCPv6 profile configuration with the APN by applying the example configuration in the Associate DHCPv6 Configuration, on page 136.

Step 6 Verify your DHCPv6 Service configuration by following the steps in the DHCPv6 Service Configuration Verification, on page 137.

Step 7 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

DHCPv6 Service Creation

Use the following example to create the DHCPv6 service to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         bind address <ipv6_address> port <port>
         end
```

Notes:

- To ensure proper operation, DHCPv6 functionality should be configured within a destination context.

- The Port specifies the listen port and is used to start the DHCPv6 server bound to it. It is optional and if unspecified, the default port is 547.

DHCPv6 Server Parameter Configuration

Use the following example to configure the DHCPv6 server parameters to support DHCPv6-based address assignment:

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-server
      renew-time <renewal_time>
      rebind-time <rebind_time>
      preferred-lifetime <pref_lifetime>
      valid-lifetime <valid_lifetime>
      end
```

Notes:

- Multiple DHCP can be configured by entering **dhcp server** command multiple times. A maximum of 256 services (regardless of type) can be configured per system.
- **renew-time** configures the renewal time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **rebind-time** configures the rebind time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **preferred-lifetime** configures the preferred lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.
- **valid-lifetime** configures the valid lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.

DHCPv6 Client Parameter Configuration

Use the following example to configure the DHCPv6 client parameters to support DHCPv6-based address assignment:

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-client
        server-ipv6-address <ipv6_addr> port <port> priority <priority>
        max-retransmissions <max_number>
        server-dead-time <dead_time>
        server-resurrect-time <revive_time>
        end
```

Notes:

- DHCPv6 client configuration requires an IPv6 address, port, and priority. The port is used for communicating with the DHCPv6 server. If not specified, default port 547 is used. The Priority parameter defines the priority in which servers should be tried out.
- **max-retransmissions** configures the max retransmission that DHCPV6-CLIENT will make towards DHCPV6-SERVER. Default is 20.

- **server-dead-time**: PDN DHCPV6-SERVER is considered to be dead if it does not respond after given tries from client. Default is 5.
- **server-resurrect-time**: PDN DHCPV6-SERVER is considered alive after it has been dead for given seconds. Default is 20.

DHCPv6 Profile Configuration

Use the following example to configure the DHCPv6 profile:

```
configure
  context <dest_ctxt_name>
    dhcp-server-profile <server_profile>
      enable rapid-commit-dhcpv6
     process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority <priority>

      dhcpv6-server-preference <pref_value>
      enable dhcpv6-server-unicast
      enable dhcpv6-server-reconf
      exit
    dhcp-client-profile <client_profile>
      dhcpv6-client-unicast
      client-identifier { IMSI | MSISDN }
      enable rapid-commit-dhcpv6
      enable dhcp-message-spray
      request dhcp-option dns-address
      request dhcp-option netbios-server-address
      request dhcp-option sip-server-address
      end
```

Notes:

- **dhcp-server-profile** command creates a server profile and then enters the DHCP Server Profile configuration mode.
- **enable rapid-commit-dhcpv6** command enables rapid commit on the DHCPv6 server. By default it is disabled. This is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the UE.
- **process dhcp-option-from** command configures in what order the configuration options should be processed for a given client request. For a given client configuration, values can be obtained from either AAA, PDN-DHCP-SERVER, or LOCAL. By default, AAA is preferred over PDN-DHCP, which is preferred over LOCAL configuration.
- **dhcpv6-server-preference**: According to RFC-3315, DHCPv6-CLIENT should wait for a specified amount of time before considering responses to its queries from DHCPv6-SERVERS. If a server responds with a preference value of 255, DHCPv6-CLIENT need not wait any longer. Default value is 0 and it may have any configured integer between 1 and 255.
- **enable dhcpv6-server-unicast** command enables server-unicast option for DHCPv6. By default, it is disabled.
- **enable dhcpv6-server-reconf** command configures support for reconfiguration messages from the server. By default, it is disabled.

- **dhcpv6-client-unicast** command Enables client to send messages on unicast address towards the server.
- **dhcp-client-profile** command creates a client profile and then enters the DHCP Client Profile configuration mode.
- **client identifier** command configures the client-identifier, which is sent to the external DHCP server. By default, IMSI is sent. Another available option is MSISDN.
- **enable rapid-commit-dhcpv6** command configures the rapid commit for the client. By default, rapid-commit option is enabled for both DHCPv4 & DHCPv6.
- **enable dhcp-message-spray** command enables dhcp-client to spray a DHCP message to all configured DHCP servers in the PDN. By default this is disabled. With Rapid-Commit, there can only be one server to which this can be sent.
- **request dhcp-option** command configures DHCP options which can be requested by the dhcp-client. It supports the following options:
  - dns-address
  - netbios-server-address
  - sip-server-address

Associate DHCPv6 Configuration

Use the following example to associate the DHCPv6 profile with an APN:

```
configure
   context dest_ctxt_name
      apn apn_name
         dhcpv6 service-name dhcpv6_svc_name server-profile server_profile
client-profile client_profile
         dhcpv6 ip-address-pool-name dhcpv6_ip_pool allow-static-allocation
         dhcpv6 context-name <dest_ctxt>
         end
```

NOTES:

- **dhcpv6 service-name** *dhcpv6_svc_name* **server-profile** *server_profile* **client-profile** *client_profile*: Allows the system to enter the DHCPv6 Server Configuration Mode where parameters are configured for the DHCPv6 server.
- **dhcpv6 service-name** *dhcpv6_svc_name* **client-profile** *client_profile*: Allows the system to enter the DHCPv6 Client Configuration Mode where parameters are configured for the DHCPv6 client.
- **dhcpv6 ip-address-pool-name** *dhcpv6_ip_pool* **allow-static-allocation**: Associates the DHCPv6 profile with an APN.



Note Use the **allow-static-allocation** parameter only when configuring the IPv6 pool.

DHCPv6 Service Configuration Verification

Procedure

Step 1 Verify that your DHCPv6 servers configured properly by entering the following command in Exec Mode:

show dhcpv6-service all

This command produces an output similar to that displayed below where DHCPv6 service name is *dhcp6-service*:

```
Service name:                dhcpv6-service
Context:                             A
Bind Address:                        2092::192:90:92:40
Bind :                               Done
Service Status:                      Started
Server Dead Time:                    120 (secs)
Server Dead consecutive Failure:5
Server Select Algorithm:             First Server
Server Renew Time:                   400 (secs)
Server Rebind Time:                  500 (secs)
Server Preferred Life Time:          600 (secs)
Server Valid Life Time:              700 (secs)
Max Retransmissions:                 3 (secs)
Server Dead Tries:                   4 (secs)
Server Resurrect Time:               10 (secs)
ipv6_nd_flag:                        O_FLAG
DHCPv6 Servers configured:
          Address:                   2092::192:90:92:40 Priority: 1    enabled
```

Step 2 Verify the DHCPv6 service status by entering the following command in Exec Mode:

show dhcpv6 status service *dhcpv6_service_name*

Configuring the System as a Standalone PMIP P-GW in an LTE-SAE Network

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a P-MIP P-GW in an LTE-SAE test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- Information Required, on page 138Information Required
- How This Configuration Works, on page 145
- P-MIP P-GW (LTE) Configuration, on page 146

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 17: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	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.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 18: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S5/S8 Interface Configuration (To/from S-GW)	
Interface name	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.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
LMA Service Configuration	
LMA Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the LMA service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 19: Required Information for PDN Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context is recognized by the system.
IP Address Pool Configuration	

Required Information	Description
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 20: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
S6b Interface Configuration (to 3GPP AAA server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
S6b Diameter Endpoint Configuration	

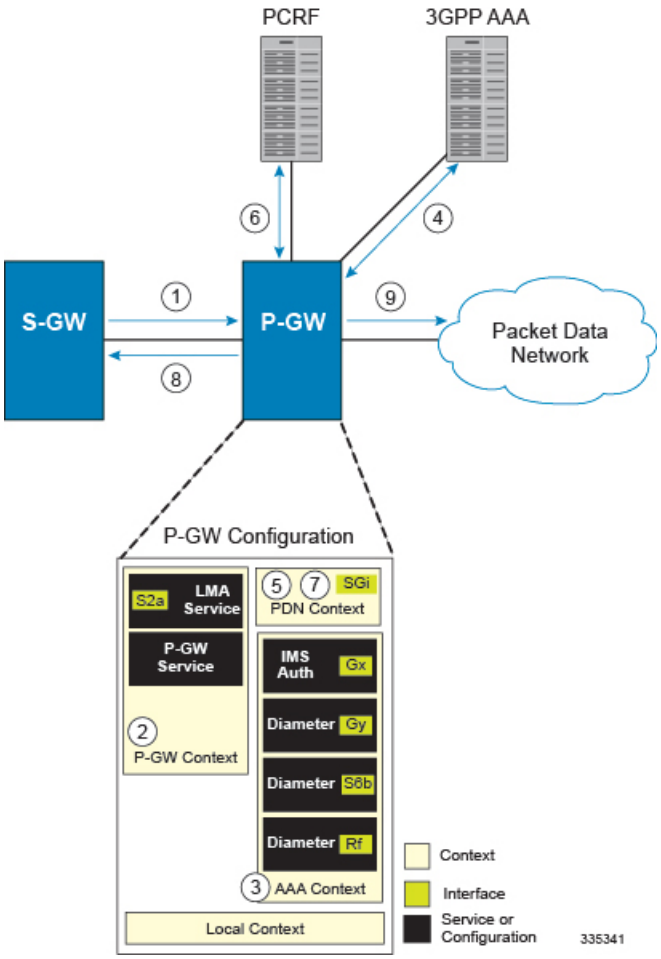
Required Information	Description
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6b Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6b origin host is recognized by the system.
Origin host address	The IP address of the S6b interface.
Peer name	The S6b endpoint name described above.
Peer realm name	The S6b origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The S6b endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.

Required Information	Description
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The Gy endpoint name described above.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the PMIP LTE network.

Figure 9: Elements of the PMIP P-GW in the LTE Network



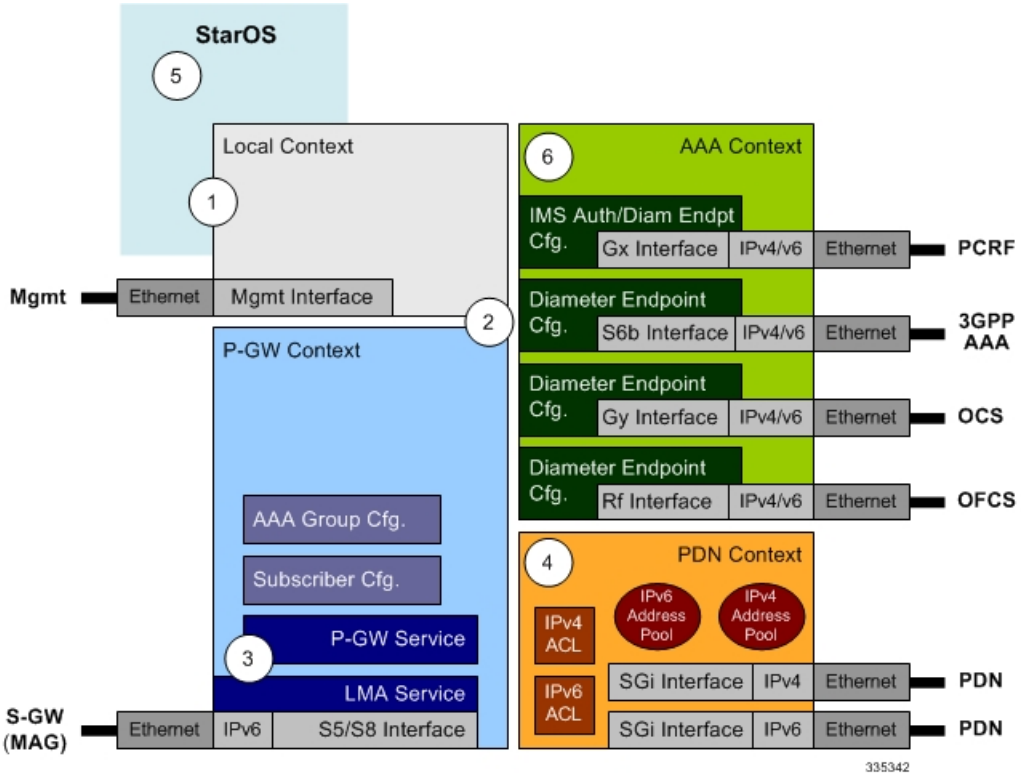
1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.

6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

P-MIP P-GW (LTE) Configuration

To configure the system to perform as a standalone P-MIP P-GW in an LTE-SAE network environment, review the following graphic and subsequent steps.

Figure 10: PMIP P-GW (LTE) Configurables



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the Initial Configuration, on page 147.

Step 3 Configure the system to perform as a PMIP P-GW and set basic P-GW parameters such as PMIP interfaces and an IP route by applying the example configurations presented in the P-GW Service Configuration, on page 150.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration, on page 151.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration, on page 151.

Step 6 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in the AAA and Policy Configuration, on page 171.

Step 7 Verify and save the configuration by following the instructions in the Verifying and Saving the Configuration, on page 155.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 147.

Step 2 Create the context where the P-GW service will reside by applying the example configuration in Creating and Configuring a P-MIP P-GW Context, on page 148.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 148.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 149.

Step 5 Create and configure a Local Mobility Anchor (LMA) service within the newly created context by applying example configuration in Creating and Configuring an LMA Service, on page 149.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 150.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
```

```
   bind interface <lcl_cntxt_intrfc_name> local
   end
```

Creating and Configuring a P-MIP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv6 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```
configure
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <ipv6_address>
      tunnel-mode ipv6ip
      source interface <name>
      destination address <ipv6 address>
      exit
    exit
  policy accounting <rf_policy_name> -noconfirm
    accounting-level {level_type}
    accounting-event-trigger interim-timeout action stop-start
    operator-string <string>
    exit
  subscriber default
    exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

Notes:

- The S5/S8 (P-GW to S-GW) interface must be an IPv6 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
```

```
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

Creating and Configuring an LMA Service

Use the following configuration example to create the LMA service:

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s5s8_ipv6_address>
      end
```

Notes:

- The **no aaa acounting** command is used to prevent duplicate accounting packets.

- Enabling revocation provides for MIP registration revocation in the event that MIP revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a revocation message to the MAG.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure
   context <pdn_context_name> -noconfirm
      interface <sgi_ipv4_interface_name>
         ip address <ipv4_address>
      interface <sgi_ipv6_interface_name>
         ipv6 address <address>
         end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service, on page 150.

Step 2 Specify an IP route to the P-MIP Serving Gateway by applying the example configuration in the Configuring a Static IP Route, on page 151.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-service <pgw_service_name> -noconfirm
         plmn id mcc <id> mnc <id>
         associate lma-service <lma_service_name>
         associate qci-qos-mapping <name>
         authorize external
         fqdn host <domain_name> realm <realm_name>
         end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to the *Configuring QCI-QoS Mapping* section for more information.
- External authorization is performed by the 3GPP AAA server through the S6b interface. Internal authorization (APN) is default.
- The **fqdn host** command configures a Fully Qualified Domain Name for the P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Configuring a Static IP Route

Use the following example to configure static IP routes for data traffic between the P-GW and the S-GW:

```
configure
   context <pgw_context_name>
      ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
      end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

P-GW PDN Context Configuration

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```
configure
   context <pdn_context_name> -noconfirm
      interface <pdn_sgi_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <pdn_sgi_ipv6_interface_name>
         ip address <ipv6_address>
         exit
      ip pool <name> range <start_address end_address> public <priority>
      ipv6 pool <name> range <start_address end_address> public <priority>
      subscriber default
      ip access-list <name>
         redirect css service <name> any
         permit any
         exit
      ipv6 access-list <name>
         redirect css service <name> any
         permit any
         exit
      aaa group default
         exit
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_ipv4_interface_name> <pdn_context_name>
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_ipv6_interface_name> <pdn_context_name>
      end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
      content-id <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    charging-action static
      service-identifier <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
              exit
```

```
rulebase <name>
   <rule_base>
      .
      .
   <rule_base>
   end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- Charging actions define the action to take when a rule definition is matched.



Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

AAA and Policy Configuration

Procedure

Step 1 Configure AAA and policy interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 153.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 155 section.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind the port to interface supporting traffic between this context and a PCRF:

```
configure
   context <aaa_context_name> -noconfirm
      interface <s6b_interface_name>
         ip address <ipv4_address>
         exit
      interface <gx_interface_name>
         ipv6 address <address>
         exit
      interface <gy_interface_name>
         ipv6 address <address>
         exit
      interface <rf_interface_name>
```

```
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
        diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <s6b_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv4_address>
      peer <s6b_cfg_name> realm <name> address <aaa_ipv4_addr>
      route-entry peer <s6b_cfg_name>
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The S6b interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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 the System as a Standalone PMIP P-GW Supporting an eHRPD Network

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a P-MIP P-GW supporting an eHRPD test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- Information Required, on page 156
- How This Configuration Works, on page 163
- P-MIP P-GW (eHRPD) Configuration, on page 164

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 21: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	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.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.

Required Information	Description
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 22: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S2a Interface Configuration (To/from HSGW)	
Interface name	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.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).

Required Information	Description
LMA Service Configuration	
LMA Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the LMA service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 23: Required Information for PDN Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context is recognized by the system.
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets

Required Information	Description
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 24: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
S6b Interface Configuration (to 3GPP AAA server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
S6b Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6b Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6b origin host is recognized by the system.
Origin host address	The IP address of the S6b interface.
Peer name	The S6b endpoint name described above.
Peer realm name	The S6b origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The S6b endpoint name described above.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

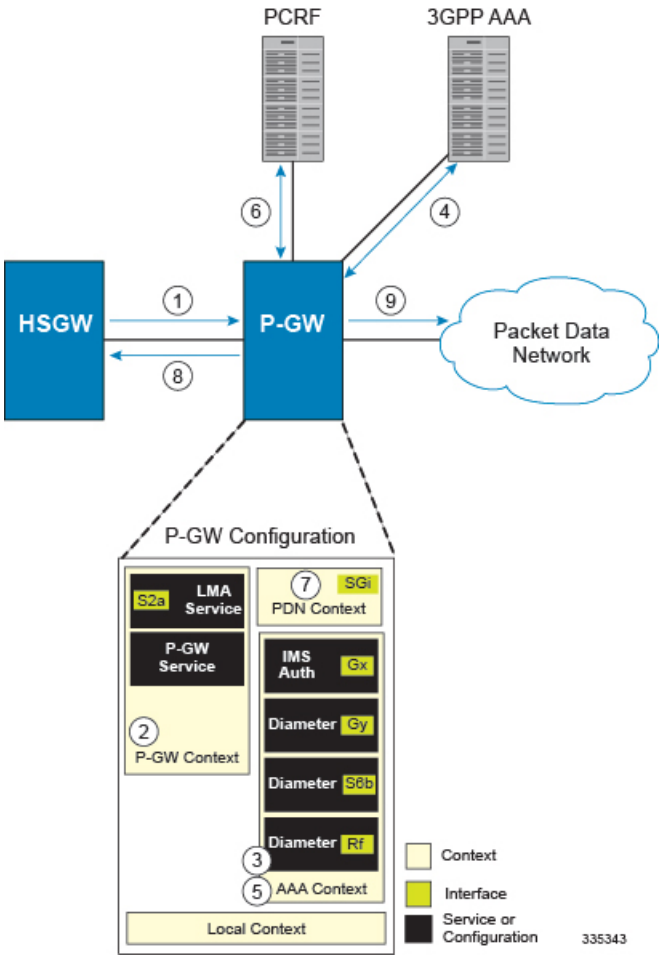
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.

Required Information	Description
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.

Figure 11: Elements of the PMIP P-GW Supporting an eHRPD Network

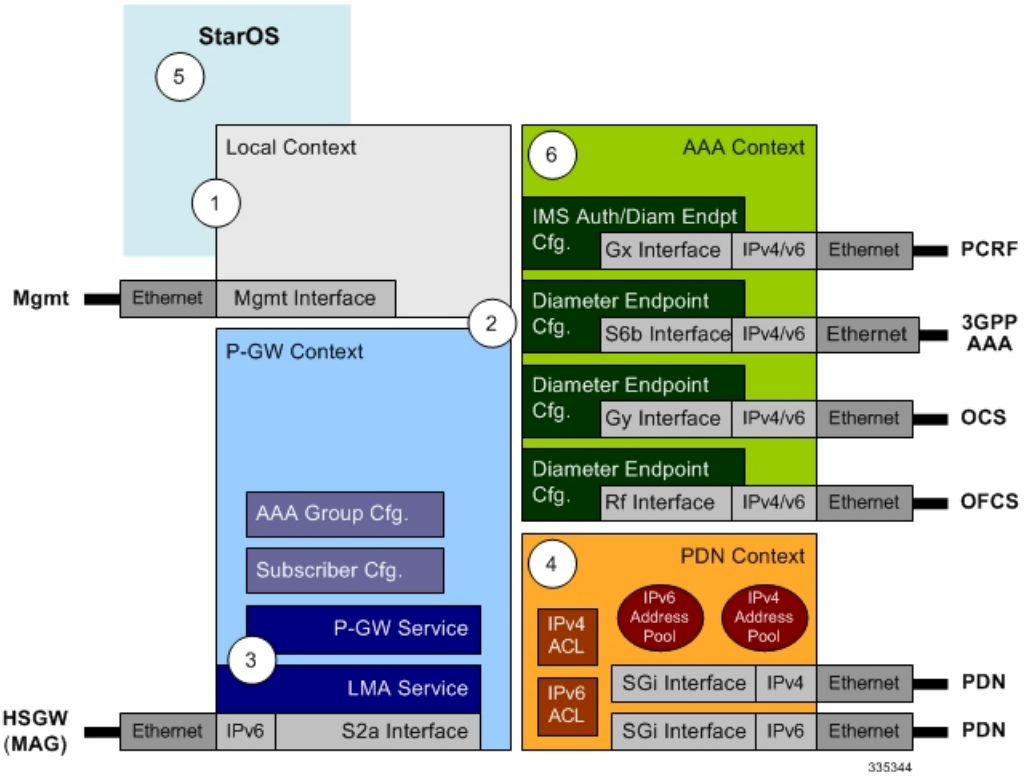


1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

P-MIP P-GW (eHRPD) Configuration

To configure the system to perform as a standalone P-MIP P-GW in an eHRPD network environment, review the following graphic and subsequent steps.

Figure 12: P-MIP P-GW (eHRPD) Configuration



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in Initial Configuration.

Step 3 Configure the system to perform as a P-MIP P-GW and set basic P-GW parameters such as P-MIP interfaces and an IP route by applying the example configurations presented in P-GW Service Configuration, on page 168.

Step 4 Configure the PDN context by applying the example configuration in P-GW PDN Context Configuration, on page 169.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in Active Charging Service Configuration, on page 170.

Step 6 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in AAA and Policy Configuration.

Step 7 Verify and save the configuration by following the instruction in Verifying and Saving the Configuration, on page 173.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 165.

Step 2 Create the context where the P-GW service will reside by applying the example configuration in Creating and Configuring a P-MIP P-GW Context, on page 166.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 166.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 167 section.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in Creating and Configuring an LMA Service, on page 168.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 168.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
      exit
```

```
    server ftpd
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

Creating and Configuring a P-MIP P-GW Context

Use the following example to create a P-GW context, create an S2a IPv6 interface (for data traffic to/from the HSGW), and bind the S2a interface to a configured Ethernet port:

```
configure
  context <pgw_context_name> -noconfirm
    interface <s2a_interface_name> tunnel
      ipv6 address <address>
      tunnel-mode ipv6ip
        source interface <name>
        destination address <ipv4 or ipv6 address>
        exit
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    subscriber default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s2a_interface_name> <pgw_context_name>
    end
```

Notes:

- The S2a (P-GW to HSGW) interface must be an IPv6 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The associate accounting-policy command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in Creating and Configuring a P-MIP P-GW Context, on page 166.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
```

```
diameter authentication server <s6b_cfg_name> priority <num>
diameter accounting server <rf_cfg_name> priority <num>
```

Creating and Configuring an LMA Service

Use the following configuration example to create the LMA service:

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s2a_ipv6_address>
      end
```

Notes:

- The **no aaa acounting** command is used to prevent duplicate accounting packets.
- Enabling revocation provides for MIP registration revocation in the event that MIP revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a revocation message to the MAG.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interfaces.

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
      end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in Configuring the P-GW Service, on page 168.

Step 2 Specify an IP route to the HRPD Serving Gateway by applying the example configuration in Configuring a Static IP Route, on page 169.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
  context <pgw_context_name>
    pgw-service <pgw_service_name> -noconfirm
      associate lma-service <lma_service_name>
```

```
associate qci-qos-mapping <name>
authorize external
fqdn host <domain_name> realm <realm_name>
plmn id mcc <id> mnc <id>
end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to Configuring QCI-QoS Mapping, on page 173 for more information.
- External authorization is performed by the 3GPP AAA server through the S6b interface. Internal authorization (APN) is default.
- The **fqdn host** command configures a Fully Qualified Domain Name for the P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Configuring a Static IP Route

Use the following example to configure static IP routes for data traffic between the P-GW and the HSGW:

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <hsgw_addr> interface
<pgw_hsgw_intrfc_name>
    end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

P-GW PDN Context Configuration

Use the following example to configure IP pools and IP Access Control Lists (ACLs), and bind ports to the interfaces in the PDN context:

```
configure
  context <pdn_context_name> -noconfirm
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
    aaa group default
      exit
        exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
      bind interface <pdn_sgi_ipv4_interface_name> <pdn_context_name>
      exit
    port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_sgi_ipv6_interface_name> <pdn_context_name>
      end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { < ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
    exit
    rulebase <name>
      <rule_base>
        .
        .
      <rule_base>
      end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- Active charging in optimized mode enables the service as part of the session manager instead of part of ACS managers.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- Charging actions define the action to take when a rule definition is matched.



Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

AAA and Policy Configuration

Procedure

Step 1 Configure AAA and policy interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 171 section.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 173 section.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind ports to interfaces supporting traffic between this context, a PCRF, a 3GPP AAA server, an on-line charging server, and an off-line charging server:

```
configure
  context <aaa_context_name> -noconfirm
    interface <s6b_interface_name>
      ip address <ipv4_address>
      exit
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    subscriber default
```

```
    exit
  ims-auth-service <gx_ims_service_name>
    p-cscf discovery table <#> algorithm round-robin
    p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
    policy-control
      diameter origin endpoint <gx_cfg_name>
      diameter dictionary <name>
      diameter host-select table <#> algorithm round-robin
     diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

      exit
    exit
  diameter endpoint <s6b_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_ctx_ipv4_address>
    peer <s6b_cfg_name> realm <name> address <aaa_ip_addr>
    route-entry peer <s6b_cfg_name>
    exit
  diameter endpoint <gx_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <gx_cfg_name> realm <name> address <pcrf_ipv6_addr>
    route-entry peer <gx_cfg_name>
    exit
  diameter endpoint <rf_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_ip_address>
    peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>
    route-entry peer <rf_cfg_name>
    exit
  diameter endpoint <gy_cfg_name>
    use-proxy
    origin realm <realm_name>
    origin host <name> address <aaa_ip_address>
    connection retry-timeout <seconds>
    peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
    route-entry peer <gy_cfg_name>
    exit
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <s6b_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gx_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gy_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
```

```
no shutdown
bind interface <rf_interface_name> <aaa_context_name>
end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The S6b interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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 Optional Features on the P-GW

The configuration examples in this section are optional and provided to cover the most common uses of the P-GW in a live network. The intent of these examples is to provide a base configuration for testing.

Configuring ACL-based Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IKEv2/IPSec ACL-based node-to-node tunnel endpoint on the S5 interface.



Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring a Crypto Access Control List

The following example configures a crypto ACL (Access Control List), which defines the matching criteria used for routing subscriber data packets over an IPSec tunnel:

```
configure
  context <pgw_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp host <source_host_address> host <dest_host_address>
      end
```

Notes:

- The **permit** command in this example routes IPv4 traffic from the server with the specified source host IPv4 address to the server with the specified destination host IPv4 address.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- IKEv2 ACL mode with NATT is not supported.
- IKEv2 with VRF is not supported.

Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map:

```
configure
  context <pgw_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      ikev2-ikesa transform-set list  <name1> . . . name6>
      payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
```

```
    interface <s5_intf_name>
      ip address <ipv4_address>
      crypto-map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5_intf_name> <pgw_context_name>
    end
```

Notes:

- The type of crypto map used in this example is IKEv2/IPv4 for IPv4 addressing. An IKEv2/IPv6 crypto map can also be used for IPv6 addressing.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Configuring APN as Emergency

The configuration example in this section configures an emergency APN for VoLTE based E911 support.

In APN Configuration Mode, specify the name of the emergency APN and set the emergency inactivity timeout as follows. You may also configure the P-CSCF FQDN server name for the APN.

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      emergency-apn
      timeout emergency-inactivity <seconds>
      p-cscf fqdn <fqdn>
      end
```

Notes:

- By default, an APN is assumed to be non-emergency.
- The **timeout emergency-inactivity** command specifies the timeout duration, in seconds, to check inactivity on the emergency session. <*seconds*> must be an integer value from 1 through 3600.
- By default, emergency inactivity timeout is disabled (0).
- The **p-cscf fqdn** command configures the P-CSCF FQDN server name for the APN. <*fqdn*> must be a string from 1 to 256 characters in length.
- P-CSCF FQDN has more significance than CLI-configured P-CSCF IPv4 and IPv6 addresses.

Configuring Common Gateway Access Support

This section describes some advance feature configuration to support multiple access networks (CDMA, eHRPD ,and LTE) plus a GSM/UMTS for international roaming with the same IP addressing behavior and access to 3GPP AAA for subscriber authorization. Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

This configuration combines 3G and 4G access technologies in a common gateway supporting logical services of HA, P-GW, and GGSN to allow subscribers to have the same user experience, independent of the access technology available.



Important This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and P-GW service.

To configure the S6b and other advance features:

1. Configure Diameter endpoint by applying the example configuration in Diameter Endpoint Configuration, on page 177.
2. Create or modify AAA group by applying the example configuration in AAA Group Configuration, on page 177.
3. Modify P-GW service to allow authorization with HSS by applying the example configuration in Authorization over S6b Configuration, on page 178.
4. *Optional*. Create and associate DNS client parameters by applying the example configuration in DNS Client Configuration, on page 178.
5. *Optional*. Modify P-GW service to accept duplicate calls when received with same IP address by applying the example configuration in Duplicate Call Accept Configuration, on page 178.
6. Verify your S6b configuration by following the steps in Common Gateway Access Support Configuration Verification, on page 179.
7. Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Diameter Endpoint Configuration

Use the following example to configure the Diameter endpoint:

```
configure
  context <pgw_ctxt_name> -noconfirm
    diameter endpoint <s6b_endpoint_name>
      origin host <host_name> address <ip_address>
      peer <peer_name> realm <realm_name> address <ip_address> port <port_num>
    end
```

Notes:

- <*pgw_ctxt_name*> is name of the context which contains P-GW service on system.

AAA Group Configuration

Use the following example create/modify the AAA group for this feature.

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
        diameter authentication endpoint <s6b_endpoint_name>
        diameter authentication server <server_name> priority <priority>
        end
```

Notes:

- <*s6b_endpoint_name*> is name of the existing Diameter endpoint.

Authorization over S6b Configuration

Use the following example to enable the S6b interface on P-GW service with 3GPP AAA/HSS:

```
configure
   context <pgw_ctxt_name>
      pgw-service <pgw_svc_name>
         plmn id mcc <number> mnc <number>
         authorize-with-hss
         fqdn host <host_name> realm <realm_name>
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

DNS Client Configuration

Use the following example to enable the S6b interface on P-GW service with 3GPP AAA/HSS:

```
configure
   context <pgw_ctxt_name>
      ip domain-lookup
      ip name-servers <ip_address/mask>
      dns-client <dns_name>
         bind address <ip_address>
         resolver retransmission-interval <duration>
         resolver number-of-retries <retrie>
         cache ttl positive <ttl_value>
         exit
      pgw-service <pgw_svc_name>
         default dns-client context
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

Duplicate Call Accept Configuration

Use the following example to configure P-GW service to accept the duplicate session calls with request for same IP address:

```
configure
   context <pgw_ctxt_name>
      pgw-service <pgw_svc_name>
         newcall duplicate-subscriber-requested-address accept
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

Common Gateway Access Support Configuration Verification

1. Verify that your common gateway access support is configured properly by entering the following command in Exec Mode:

   show pgw-service all

   The output from this command should look similar to the sample shown below. In this example P-GW service named *PGW1* was configured in the *vpn1* context.

```
Service name:                   pgw1
Context:                        cn1
Associated PGW svc:             None
Associated GTPU svc:            None
Accounting Context Name:        cn1
dns-client Context Name:        cn1
Authorize:                      hss
Fqdn-name:                      xyz.abc@starent.networks.com
Bind:                           Not Done
Local IP Address:               0.0.0.0          Local IP Port:
2123
Self PLMN:                      Not defined
Retransmission Timeout:         5 (secs)
```

Configuring Dynamic Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IPSec/IKEv2 dynamic node-to-node tunnel endpoint on the S5 interface.



Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.

- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header, including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      ikev2-ikesa transform-set list <name1> . . . <name6>
      ikev2-ikesa rekey
      payload <name> match childsa match ipv4
        ipsec transform-set list <name1> . . . <name4>
```

```
      rekey
      end
```

Notes:

- The **ikev2-ikesa transform-set list** command specifies up to six IKEv2 transform sets.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Binding the S5 IP Address to the Crypto Template

The following example configures the binding of the S5 interface to the crypto template:

```
configure
  context <pgw_ingress_context_name> -noconfirm
    gtpu-service <gtpu_ingress_service_name>
      bind ipv4-address <s5_interface_ip_address> crypto-template
<sgw_s5_crypto_template>
      exit
    egtp-service <egtp_ingress_service_name>
      interface-type interface-pgw-ingress
      associate gtpu-service <gtpu_ingress_service_name>
      gtpc bind ipv4-address <s5_interface_ip_address>
      exit
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id> primary
      associate egtp-service <egtp_ingress_service_name>
      end
```

Notes:

- The **bind** command in the GTP-U and eGTP service configuration can also be specified as an IPv6 address using the **ipv6-address** command.

Configuring Guard Timer on Create Session Request Processing

P-GW has an existing timer "session setup-timeout" which is hard coded to 60 seconds, which is used as a guard timer for session creation. This timer is used for all APNs and is started when a Create Session Request is received for any session creation.

Internal or external processing issues or delay at external interfaces, for example, Gx/Gy, can cause Create Session Request processing to run longer than time expected in end to end call setup. If the session processing is not complete when the timer expires, the Create Session Request processing is stopped and the P-GW performs an internal cleanup by stopping all other corresponding sessions, for example Gx/Gy. The P-GW responds with a Create Session Failure response stating that no resources are available to S-GW. In successful cases when there's no delay timer is stopped during sending out the Create Session Response.

A new CLI command has been introduced to allow a configurable value to override the previously hardcoded default session setup timeout value of 60 seconds. This will help to fine tune the call setup time at P-GW with respect to end to end call setup time.

Configuring Session Timeout

The following configuration example makes a P-GW session setup timeout configurable.

```
configure
  context  context_name
    pgw-service  service_name
      setup-timeout  timer-value
      [  default | no ] setup-timeout
      end
```

Notes:

- **setup-timeout**: Specifies the session setup timeout period, in seconds. If P-GW is able to process the Create Session Request message before the timer expires, P-GW stops the timer and sends a successful Create Session Response.

  timer_value must be an integer from 1 to 120.

  Default: 60 seconds

- **default**: Default value is 60 seconds. If no value is set, the P-GW service sets the timer to the default value.
- **no**: Sets the timer to the default value of 60 seconds.

Configuring the GTP Echo Timer

The GTP echo timer on the ASR 5500 P-GW can be configured to support two different types of path management: default and dynamic. This timer can be configured on the GTP-C and/or the GTP-U channels.

Default GTP Echo Timer Configuration

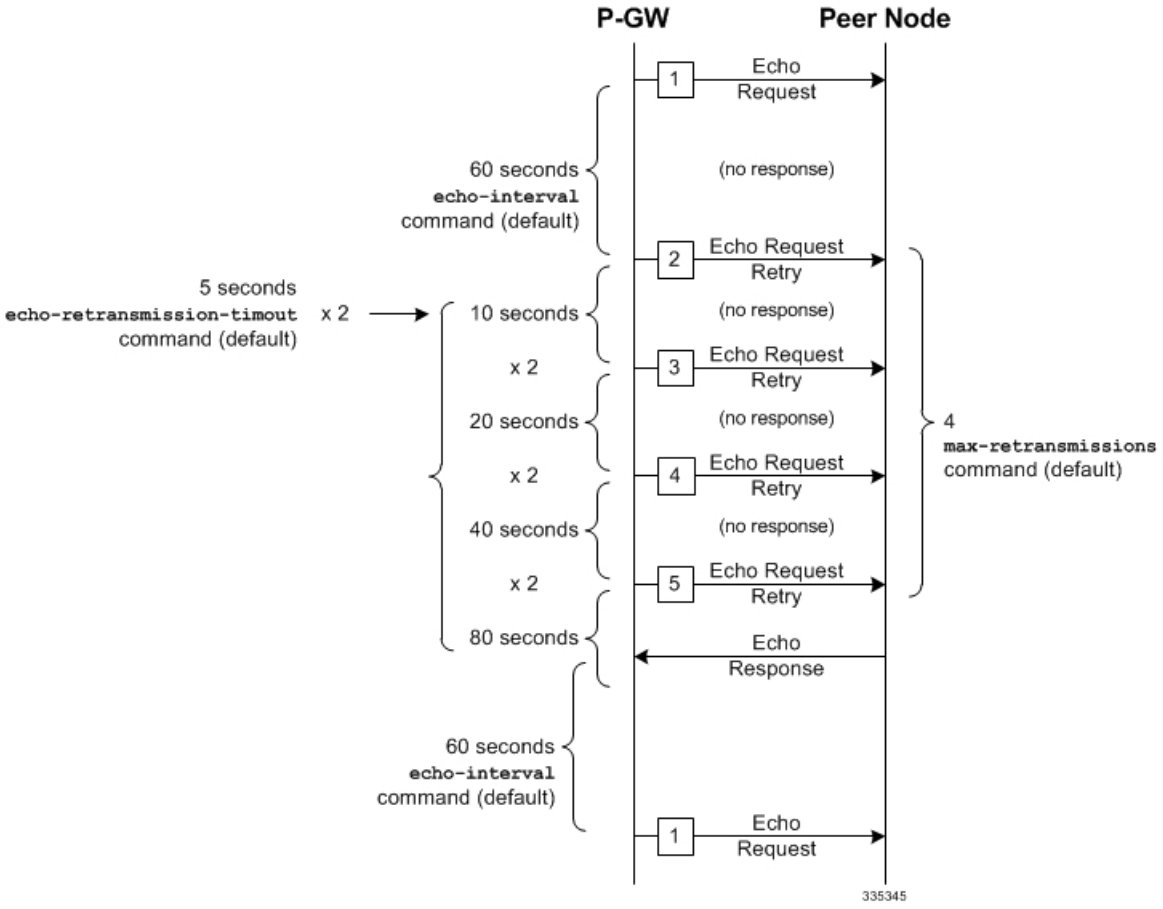
The following examples describe the configuration of the default eGTP-C and GTP-U interface echo timers:

eGTP-C

```
configure
     configure
          context <context_name>
               egtp-service <egtp_service_name>
                    gtpc echo-interval <seconds>
                    gtpc echo-retransmission-timeout <seconds>
                    gtpc max-retransmissions <num>
                    end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above:



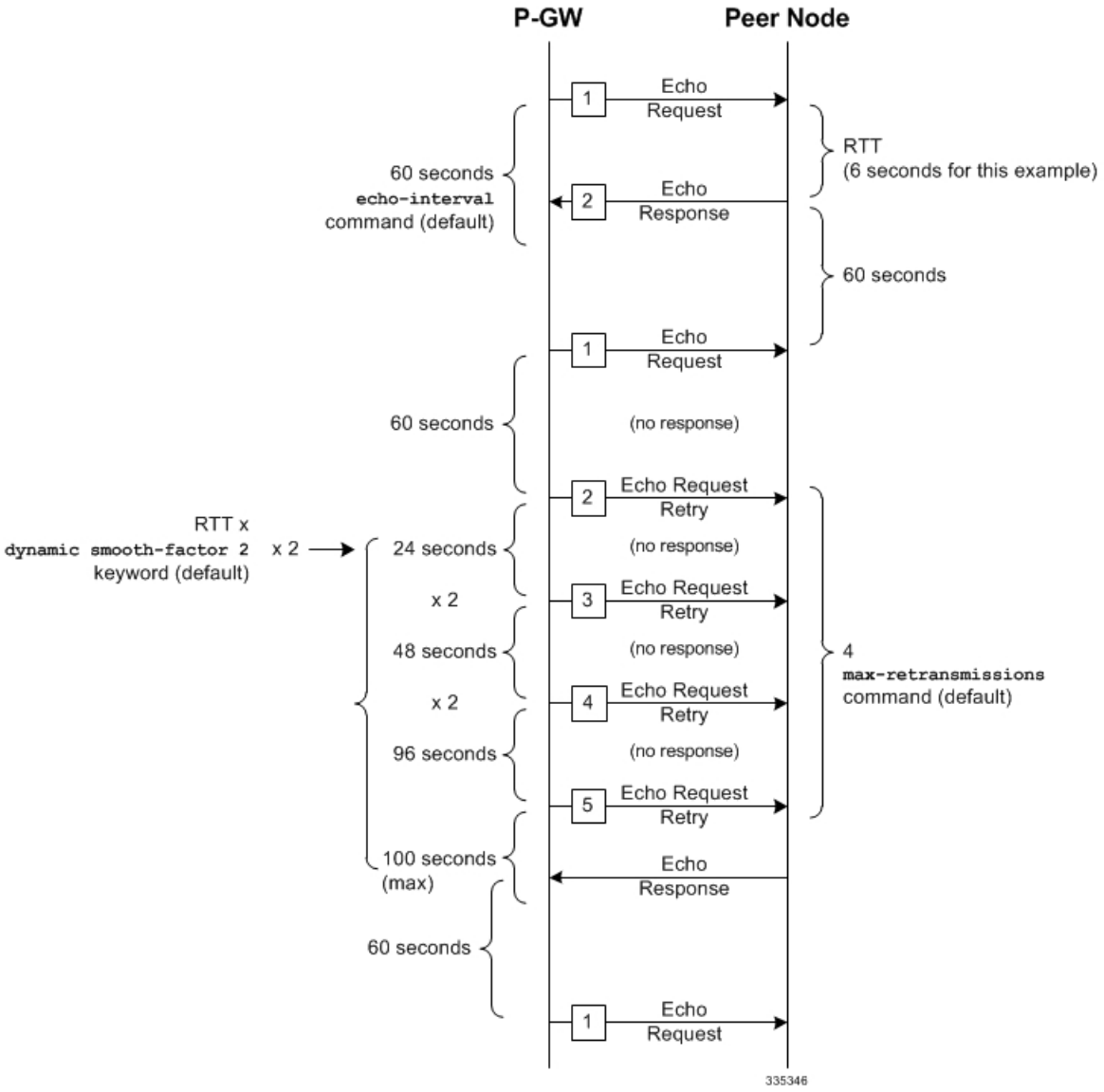
- The multiplier (x2) is system-coded and cannot be configured.

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three GTP-U commands in the example above:



- The multiplier (x2) is system-coded and cannot be configured.

Dynamic GTP Echo Timer Configuration

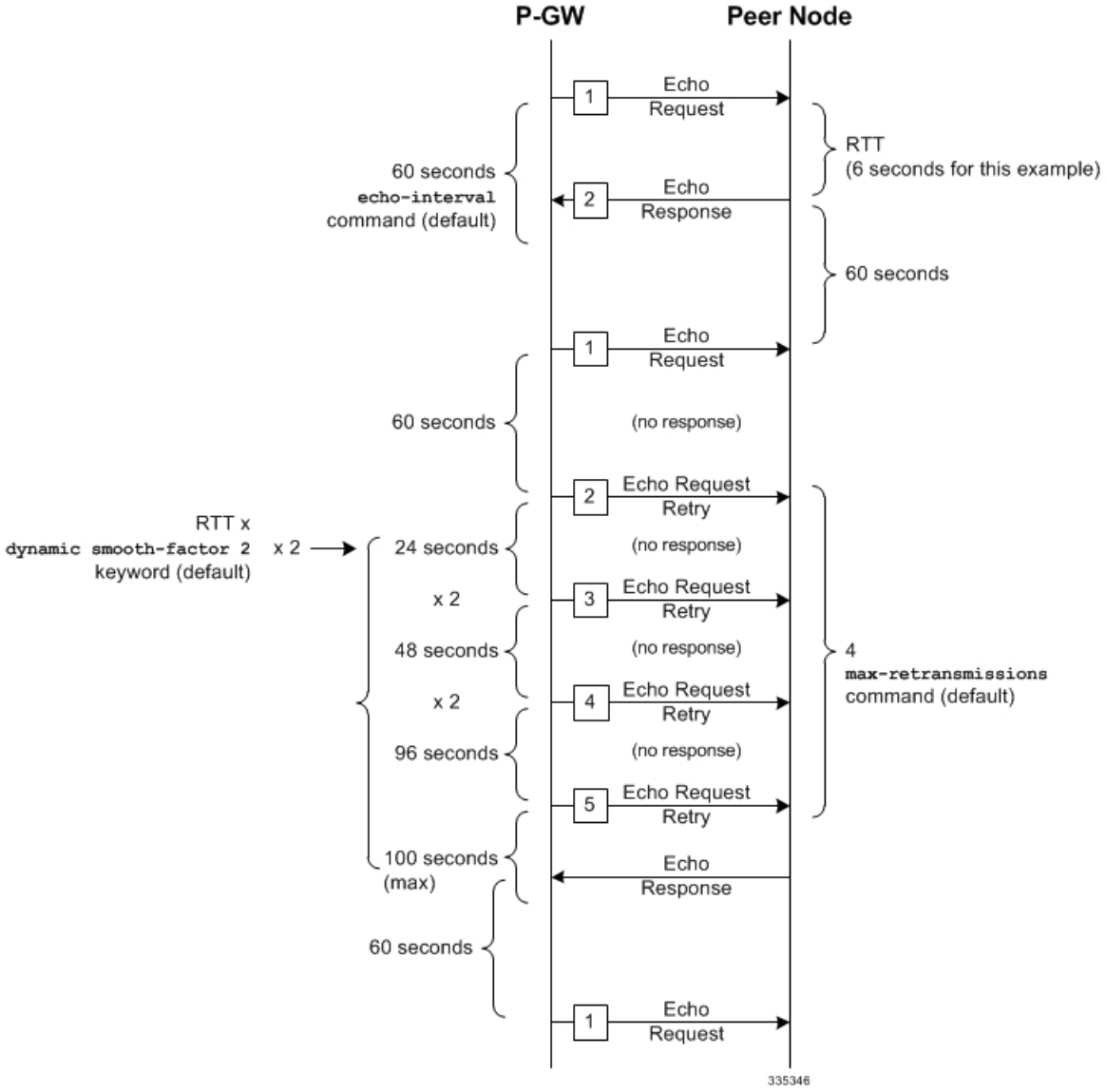
The following examples describe the configuration of the dynamic eGTP-C and GTP-U interface echo timers:

eGTP-C

```
configure
  configure
    context <context_name>
      egtp-service <egtp_service_name>
        gtpc echo-interval <seconds> dynamic smooth-factor <multiplier>
        gtpc echo-retransmission-timeout <seconds>
        gtpc max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above and an example round trip timer (RTT) of six



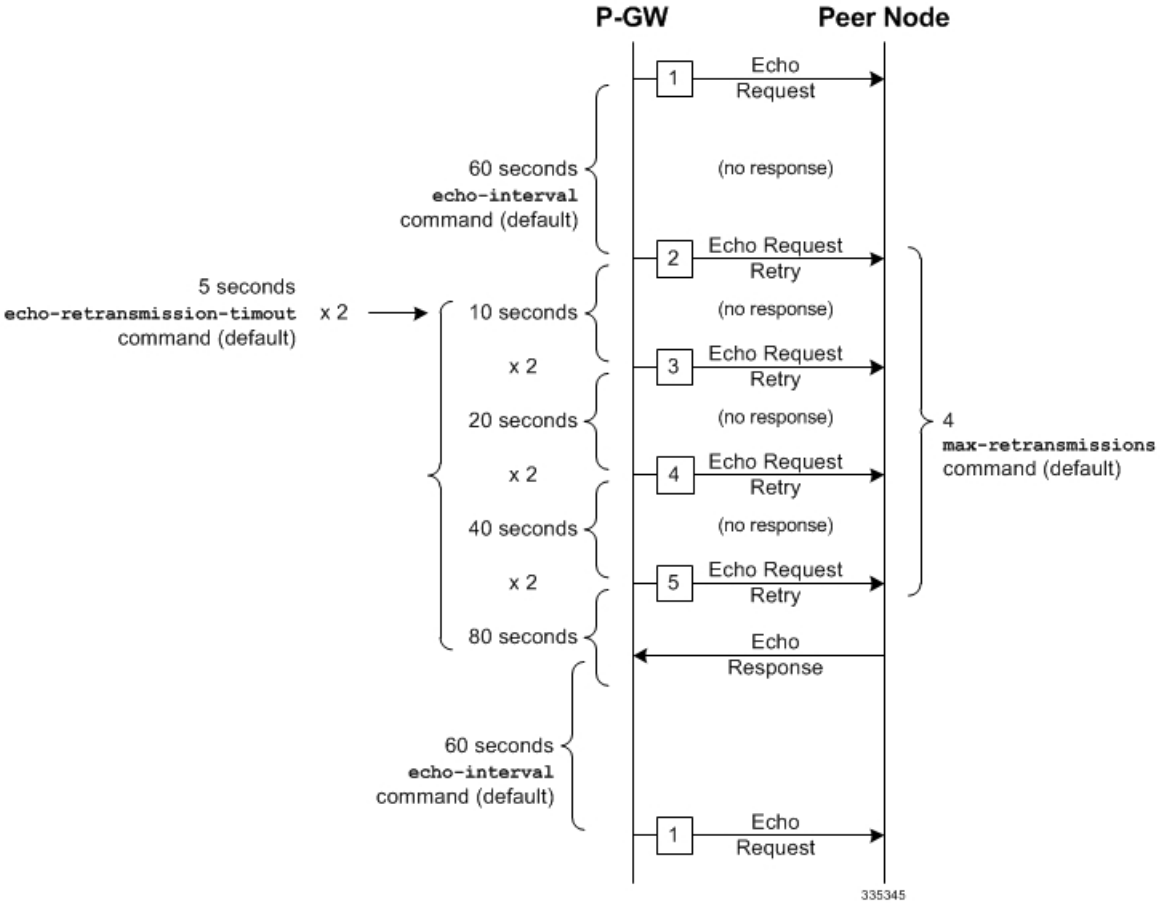
- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds> dynamic smooth-factor <multiplier>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above and an example round trip timer (RTT) of six seconds:



- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

Configuring GTPP Offline Accounting on the P-GW

By default the P-GW service supports GTPP accounting. To provide GTPP offline charging, configure the P-GW with the example parameters below:

```
configure
      gtpp single-source
      context <ingress_context_name>
            subscriber default
                  accounting mode gtpp
                  exit
            gtpp group default
                  gtpp charging-agent address <gz_ipv4_address>
                  gtpp echo-interval <seconds>
                  gtpp attribute diagnostics
                  gtpp attribute local-record-sequence-number
                  gtpp attribute node-id-suffix <string>
                  gtpp dictionary <name>
                  gtpp server <ipv4_address> priority <num>
                  gtpp server <ipv4_address> priority <num> node-alive enable
```

```
            exit
      policy accounting <gz_policy_name>
            accounting-level {type}
            operator-string <string>
            cc profile <index> buckets <num>
            cc profile <index> interval <seconds>
            cc profile <index> volume total <octets>
            exit
      exit
context <ingress_context_name>
      apn apn
            associate accounting-policy <gz_policy_name>
            exit
      interface <gz_interface_name>
            ip address <address>
            exit
      exit
port ethernet <slot_number/port_number>
      no shutdown
      bind interface <gz_interface_name> <ingress_context_name>
      end
```

Notes:

- **gtpp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- **gtpp** is the default option for the **accounting mode** command.
- An accounting mode configured for the call-control profile will override this setting.
- **accounting-level** types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Configuring GTP Throttling Feature

The GTP Throttling feature allows the operator to control the rate of incoming/outgoing messages on P-GW/GGSN.

Configuring the Outgoing Control Message Throttling

The following configuration helps to enable outgoing control message throttling.

```
configure
  context context_name
  [no] gtpc overload-protection egress rlf-template rlf_template_name
throttling-overload-policy throttling_overload_policy_name
  end
```

Configuring the Incoming Control Message Throttling

The following configuration helps to enable incoming control message throttling.

```
configure
  context context_name
  [no] gtpc overload-protection ingress msg-rate msg_rate [delay-tolerance
```

```
msg_queue_delay ] [ queue-size queue_size ]
 end
```

Configuring Local QoS Policy

The configuration examples in this section create a local QoS policy. A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

Important Use of the Local QoS Policy feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring a Local QoS Policy

The following configuration example enables a local QoS policy on the P-GW:

```
configure
  local-policy-service <name> -noconfirm
    ruledef <ruledef_name> -noconfirm
      condition priority <priority> <variable> match <string_value>
      condition priority <priority> <variable> match <int_value>
      condition priority <priority> <variable> nomatch <regex>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    eventbase <eventbase_name> -noconfirm
      rule priority <priority> event <list_of_events> ruledef <ruledef_name>
actiondef <actiondef_name>
      end
```

Notes:

- A maximum of 16 local QoS policy services are supported.
- A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.
- The **condition** command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.
- A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons.
- The **action** command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.
- Currently, only one eventbase is supported and must be named "default".

- The **rule** command can be entered multiple times to configure multiple rules for an eventbase.
- A maximum of 256 rules are suggested in an eventbase for performance reasons.
- Rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of **continue** is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Binding a Local QoS Policy

Option 1: The following configuration example binds the previously configured local QoS policy:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      ims-auth-service <local-policy-service name>
      end
```

Notes:

- A maximum of 30 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- Useful in case of emergency calls; PCRF is not involved.

Option 2: The following configuration example may also be used to bind the previously configured local QoS policy or a failure handling template:

```
configure
  context <pgw_context_name> -noconfirm
    ims-auth-service <auth_svc_name>
      policy-control
        associate failure-handling-template <template_name>
        associate local-policy-service <service_name>
        end
```

Notes:

- Only one failure handling template can be associated with the IMS authorization service. The failure handling template should be configured prior to issuing this command.
- The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- You must select "local-fallback" in the failure handling template to support fallback to local policy.
- To support fallback to local policy in case of failure at PCRF, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.

Verifying Local QoS Policy

The following configuration example verifies if local QoS service is enforced:

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

Notes:

- Please take extreme caution not to use logging feature in console port and in production nodes.

Configuring X.509 Certificate-based Peer Authentication

The configuration example in this section enables X.509 certificate-based peer authentication, which can be used as the authentication method for IP Security on the P-GW.



Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration example enables X.509 certificate-based peer authentication on the P-GW.

In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure
  certificate name <cert_name> pem url <cert_pem_url> private-key pem url
<private_key_url>
  ca-certificate name <ca_cert_name> pem url <ca_cert_url>
  end
```

Notes:

- The **certificate name** and **ca-certificate list ca-cert-name** commands specify the X.509 certificate and CA certificate to be used.
- The PEM-formatted data for the certificate and CA certificate can be specified, or the information can be read from a file via a specified URL as shown in this example.

When creating the crypto template for IPSec in Context Configuration Mode, bind the X.509 certificate and CA certificate to the crypto template and enable X.509 certificate-based peer authentication for the local and remote nodes, as follows:

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      certificate name <cert_name>
      ca-certificate list ca-cert-name <ca_cert_name>
      authentication local certificate
      authentication remote certificate
      end
```

Notes:

- A maximum of 16 certificates and 16 CA certificates are supported per system. One certificate is supported per service, and a maximum of four CA certificates can be bound to one crypto template.
- The **certificate name** and **ca-certificate list ca-cert-name** commands bind the certificate and CA certificate to the crypto template.
- The **authentication local certificate** and **authentication remote certificate** commands enable X.509 certificate-based peer authentication for the local and remote nodes.

Configuring RFL Bypass Feature

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature. The RLF feature allows the operator to control the bypassing of some messages being throttled.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.

Configuring the Throttling Override Policy Mode

The following configuration helps to create a GTP-C Throttling Override Policy and to enter GTP-C Throttling Override Policy mode.

```
configure
  throttling-override-policy throttling-override-policy_name
```

Notes:

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-throttling-override-policy)#
```

Configuring the RLF Bypass Feature

The following configuration configures message types which can bypass the rate limiting function.

```
configure
  throttling-override-policy  throttling-override-policy_name
    [  default | no ] egress bypass-rlf pgw { msg-type { cbr | dbr | ubr
 | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 … | 15 }+ | apn-names
  <apn-name1>  <apn-name2>  <apn-name3>   }
    end
```

Notes:

- If an empty throttling-override-policy is created, then the default values for all the configurables are zeros/disabled.
- If no throttling-override-policy is associated, then **show service configuration** for P-GW will show it as "n/a".
- Maximum number of throttling-override-policy that can be added are 1024. This limit is the same as max RLF templates.

Example

The following command configures Create Bearer Request message type at the P-GW node to bypass throttling.

```
egress bypass-rlf pgw msg-type cbr
```

Auto Correction of VoLTE Sessions

Feature Information

Summary Data

Status	Modified 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)	CSCvc72275
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 dynamic rules for IP Multimedia Subsystem (IMS) sessions are lost after a switchover, VoLTE calls are impacted. To recover the calls, the IMS sessions have to be cleared manually to re-establish the PDN with the correct dynamic rules. The Auto Correction of VoLTE Sessions feature enables a dynamic rule check such that when the P-GW receives an RAR (Re-Auth-Request) message, it automatically identifies and rectifies

the issue without manual intervention. This features only applies to the APN that is configured on that uses the "RAR" message as a trigger for the check.

How It Works

After the APN receives any RAR message from the Policy Control and Charging Rules Function (PCRF), a Re-Auth- Answer (RAA) message is immediately sent. When the feature is enabled, an additional check is done at the P-GW to verify if there are any dynamic rules associated with the default bearer. Assuming the Session Initiation Protocol (SIP) rule on the default bearer is recovered, other dedicated bearers are also recovered. If dynamic rules are not associated with the default bearer, the call is terminated. Then, a Delete Bearer Request is sent for the default bearer with the cause code - Reactivation Required. To ensure the reason code is sent, the APN must be configured with "pdn-behavior ims". Subsequently, a Credit-Control-Request-Type (CCR-T) is sent to PCRF and other diameter interfaces (s6b, Gy, and Rf). Thereby, the automatic recovery procedure involves termination of a subscriber connection when an anomaly is detected. The subscriber has to then reconnect to the network. The mobile originated or terminated call is rejected for the subscriber where the dynamic rules are lost after a switchover.

Configuring the Auto Correction of VoLTE Sessions Feature

The following section provides the configuration commands to enable or disable the feature.

Enabling or Disabling the Dynamic Rule Check

The new CLI command, **pdn validate-post-switchover**, is added to enable the dynamic rule check for the auto correction of the VoLTE session. To enable this feature, configure the command at the base APN. This feature should be configured only for the VoLTE/IMS APNs for which auto recovery is required.

This feature is disabled by default.

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

```
configure
   context <context_name>
      apn <apn_name>
         [no] pdn validate-post-switchover
         end
```

Notes:

- **no:** Disables the configured Auto correction of VoLTE sessions on the base APN.
- **pdn validate-post-switchover:** Validates the dynamic rules for automatic recovery after a switchover.

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs in support of the Auto Correction of VoLTE Sessions feature.

Show Commands

This section lists all the show commands available to monitor this feature.

show configuration apn

The above CLI command is introduced to check if the feature is enabled at the APN level. If "pdn validate-post-switchover" is present then the feature is enabled.

show active-charging service statistics

This command has been modified to display the following output:

```
show active-charging service statistics
ACS Data Statistics:
  Packets Dropped due to System-Limit L4-Flows:                          0
  Packets Dropped - Invalid Len in IP Hdr(Dwlink):                       0
  Packets Dropped - Invalid Ver in IP Hdr(Dwlink):                       0
  Packets Not Processed due to Flow-limit:                               0
  Packets Not Processed due to CLP not found:                            0
  Packets Dropped CLP in Preservation Mode:                              0
  Total Pkts:                                                            0
  Total Collisions in data session hash:                                 0

ACS Reject Reason:
  RuleBase Mismatch  :                                                   0
  Bandwidth-Policy Mismatch  :                                           0
  CBB-Policy Mismatch  :                                                 0
  CF Policy Mismatch  :                                                  0
  No RuleBase configured in APN/Subs:                                    0
  No active rule in Rulebase/Subs:                                       0
  No Bandwidth-Policy configured in APN/Subs:                            0
  No Resources:                                                          0
  Max Sessions:                                                          0
  Reject Probability Exceeded:                                           0
  Rule Recovery Failed:                                                  0
  CDR Flow Control Initiated:                                            0

Protocol Reject stats:
  WTP Non-initial PDU:                                                   0
  WSP-CO Non-initial Connect PDU                                         0

Dynamic Rule Statistics:
  Total Subscribers:                0   Current Subscribers:             0
  Charging Msg Received:            0   Rule Defn Received:              0
  Installs Received:                0   Removes Received:                0
  Installs Succeeded:               0   Removes Succeeded:               0
  ADC Rules Received:               0   Total ADC Rules:                 0
  ADC Install Succeeded:            0   ADC Install Failed:              0
  ADC Custom Mute Received:         0   ADC Custom Unmute Received:      0
  ADC Start Sent:                   0   ADC Stop Sent:                   0
  L7 Rules Received:                0
  L7 Install Succeeded:             0   L7 Install Failed:               0
  Installs Failed:                  0   Removes Failed:                  0
  Install Failure Reason:
    No Resources:                   0   No Rulebase Match:               0
    No RuleName Match:              0   Rulebase Count Exceeded:         0
    Local Copy Failed:              0   Invalid Protocol:                0
    Invalid Source Mask:            0   Invalid Dest Mask:               0
    No Grp-of-Rdef Match:           0
    ADC Invalid Rule:               0   ADC Invalid Readdress:           0
    L7 Rule Invalid:                0
    L7 Protocol Invalid:            0   L7 Field Invalid:                0
    L7 Operator Invalid:            0   L7 Value Invalid:                0
    L7 Case-Sens Invalid:           0
  Remove Failure Reason:
    No RuleName Match:              0   No Grp-of-Rdef Match:            0
```

```
    Local Copy Failed:              0

Bandwidth Limiting Statistics:
    ITC Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0
    Dynamic Rule Bandwidth Limiting Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0
    Per-Bearer Bandwidth Limiting Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0

Credit-Control Group Statistics:
  CC Dropped Uplink Packets:        0  CC Dropped Uplink Bytes:           0
  CC Dropped Downlink Packets:      0  CC Dropped Downlink Bytes:         0

Readdressing Failure Statistics (Packets):
  Non SYN Flow:                     0  Duplicate Key:                     0
  Dropped Pkts:                     0


First-request-only redirections:                                         0

Fallback Statistics:
  Bandwidth Policy Applied:                                              0
  Bandwidth Policy Failed:                                               0
```

Bulk Statistics

This section lists all the bulk statistics that have been added, modified, or deprecated to support this feature.

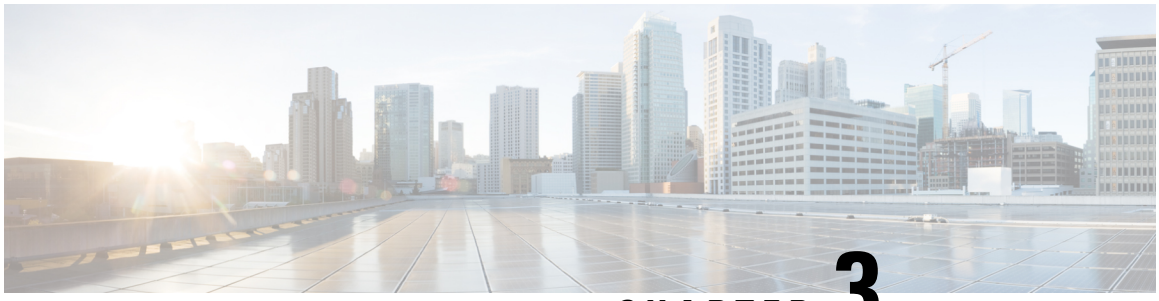
ECS Schema

This section displays the new bulk stats that have been added to indicate dynamic recovery failure :

- dyn_rule_recovery_failure:

  The total number of sessions terminated due to dynamic rule recovery failure.
- dyn_rule_recovery_num_sess_not_terminated:

  The total number of sessions that are not terminated after switchover because dynamic rules were not installed on the default bearer.



CHAPTER 3

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* for a detailed listing of these traps.

This chapter includes the following topics:

- Monitoring System Status and Performance, on page 197
- Clearing Statistics and Counters, on page 203
- 64 Bit Conversion on SAEGW and P-GW Counters, on page 204

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*.

Table 25: System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Congestion-Control Information	
View Congestion-Control Statistics	**show congestion-control statistics {a11mgr | ipsecmgr}**
View GTP Information	
View eGTP-C service statistics for a specific service	**show egtpc statistics egtpc-service** *name*
View GTP-U service statistics for all GTP-U data traffic on the system	**show gtpu statistics**

To do this:	Enter this command:
View Infrastructure-DNS Queries	
Verify Infrastructure-DNS queries to resolve P-CSCF FQDN	**dns-client query client-name** *client_name* **query-type AAAA query-name** <*p-cscf.com*>
View IP Information	
Display BGP Neighbors	
Verify BGP neighbors on egress P-GW context	**context** *egress_pgw_context_name* **show ip bgp summary** **Note** StarOS considers the below address range as Martian and hence rejects any BGP updates falling under this range. Also, StarOS does not allow BGP network command to configure from the below ranges. • 127.x.x.x • 128.0.x.x • 191.255.x.x • 192.0.0.x • 223.255.255.x
Verify BGP neighbors on ingress P-GW context	**context** *ingress_pgw_context_name* **show ip bgp summary** **Note** StarOS considers the below address range as Martian and hence rejects any BGP updates falling under this range. Also, StarOS does not allow BGP network command to configure from the below ranges. • 127.x.x.x • 128.0.x.x • 191.255.x.x • 192.0.0.x • 223.255.255.x
Display IP Connectivity State	

To do this:	Enter this command:
Verify IP connectivity to the diameter servers for various components/interfaces; all peers should be in OPEN or WAIT_DWR state	**show diameter peers full all |grep State**
Display IP Interface Status	
Verify IP interfaces are up on each context	**show ip interface summary** **show ipv6 interface summary**
Display IP Pool Configuration	
Verify IPv4 pools have been created and are available	**context** *egress_pgw_context_name* **show ip pool summary**
Verify IPv6 pools have been created and are available	**context** *egress_pgw_context_name* **show ipv6 pool summary**
View LMA Service Information	
View LMA service statistics for a specific service	**show lma-service statistics lma-service** *service_name*
View P-GW Service Information	
View P-GW service statistics	**show pgw-service statistics all**
Verify P-GW services	**context** *ingress_pgw_context_name* **show pgw-service all |grep Status** **show lma-service all |grep Status** **show egtp-service all |grep Status** **show gtpu-service all |grep State**
View QoS/QCI Information	
View QoS Class Index to QoS mapping tables	**show qci-qos-mapping table all**
View RF Accounting Information	
Confirm the PGW is sending Rf accounting records: • Verify "Message sent" is non-zero • Verify active charging sessions are present	**show diameter accounting servers |grep Message** **show active-charging sessions all |more**
View Session Subsystem and Task Information	
Display Session Subsystem and Task Statistics **Important** Refer to the *System Software Task and Subsystem Descriptions* appendix in the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	

To do this:	Enter this command:
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View AAA Proxy statistics	**show session subsystem facility aaaproxy all**
View LMA Manager statistics	**show session subsystem facility hamgr all**
View Session Manager statistics	**show session subsystem facility sessmgr all**
View Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View Session Recovery Information	
View session recovery status	**show session recovery status [verbose]**
View Subscriber Information	
Display NAT Information	
View the private IP assigned to the NAT user, along with any other public IPs assigned	**show subscriber full username** *user_name*
View NAT realms assigned to this user	**show subscriber full username** *user_name* **|grep -i nat**
View active charging flows for a specific NAT IP address	**show active-charging flows full nat required nat-ip** *ip_address*
Display Session Resource Status	
View session resource status	**show resources session**
View Statistics for Subscribers using LMA Services on the System	
View statistics for subscribers using a specific LMA service on the system	**show subscribers lma-service** *service_name*
View Statistics for Subscribers using P-GW Services on the System	
View statistics for subscribers using any P-GW service on the system	**show subscribers pgw-only full**
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	**show subscribers all**
Display UE Attach Status	

To do this:	Enter this command:
Confirm that a UE has attached: • Displays IMSI with one entry for each bearer per APN connection • Verify active charging sessions are present • Verify peers are active. Peers should correspond to S-GW EGTP addresses • Verify "Create Session Request" and "Create Session Response" categories are incrementing • Verify "Total Data Stats:" are incrementing eHRPD: • Verify lma-sessions are present • Verify "Binding Updates Received:" categories are incrementing	**show subscriber pgw-only imsi** *ue_imsi* **show active-charging sessions all |more** **show egtpc peers** **show egtpc statistics** **show gtpu statistics** **eHRPD only** **show lma-service session username** *user_name* **show lma-service statistics**

Including the IMSI/IMEI in System Event Logs of Type Error and Critical

The P-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available. If the IMSI is not available, the P-GW will make a best effort to obtain the IMEI.

Table 26: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

Event Log	Description
New Events	
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: s, error code d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>]Sessmgr-d Recover call from CRR failed for callid:0xx reason=s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-d Ran out of session handles"
140075	Represents error_log1 in format "[IMSI <IMSI>]s"
Modified Events	
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=s(d) state=s(d) event=s(d)"

Event Log	Description
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=s(d) event=s(d)"
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-d: Request to s bearer rejected. Reason: s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code d"
12774	Represents pgw_purge_invalid_crr in format "[IMSI <IMSI>] Local s TEID [lu] Collision: Clp Connect Time: lu, Old Clp Callid: d, Old Clp Connect Time: lu s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <u>."
12858	Represnts ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <u>:pf_id_bitmap 0xx and tft_opcode: d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <u> rejected, due to <s>."
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <u>, due to <s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<s>,[event:<s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call."
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0xx> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] s"

Event Log	Description
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code d"
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <s> in state <s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <s> in state <s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <s> in state <s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] s"

Configuring the P-GW to Include the IMSI/IMEI in System Event Logs of Type Error and Critical

The **include-ueid** keyword has been added to the **logging** command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
configure
    logging include-ueid
    no logging include-ueid
    end
```

Notes:

- **no** disables the inclusion of the IMSI/IMEI in system event logs of type error and critical.
- Use the **show configuration** command to view the current configuration status of the **logging include-ueid** command.
    - logging include-ueid (when enabled)
    - no logging include-ueid (when disabled.

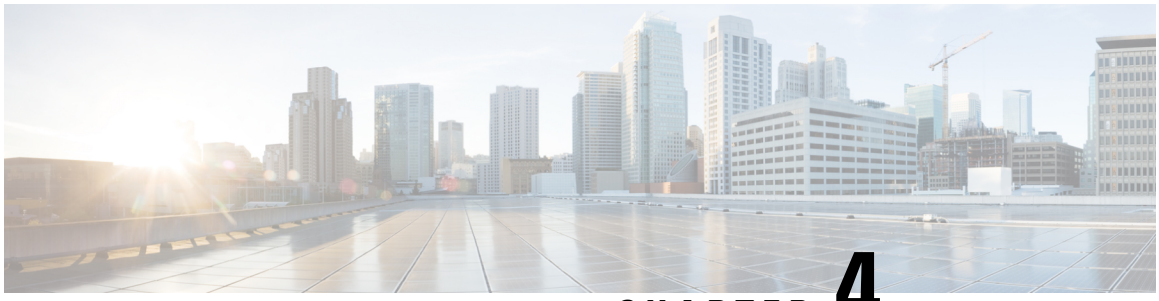
Clearing Statistics and Counters

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 Reference* for detailed information on using this command.

64 Bit Conversion on SAEGW and P-GW Counters

Most of the P-GW and SAEGW bulk statistic counters are INT32 type and they do not provide accurate statistics during a specific period of time. These counters also roll over during a specific time period. In order to avoid the roll-over and stop the over flow of the counter, the Int32 to Int64 in bulk statistics schema and SessMgr is introduced. For more information see the *Statistics and Counters Reference Guide*.



CHAPTER 4

3GPP Changes to the Gx Interface

- Feature Information, on page 205
- Feature Changes, on page 206
- Limitations, on page 206

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	Yes, only for Customer specific Gx Dictionary.
Related CDETS ID(s)	CSCvc99275
Related Changes in This Release	Not Applicable
Related Documentation	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
Modified in this release.	21.2	April 27, 2017

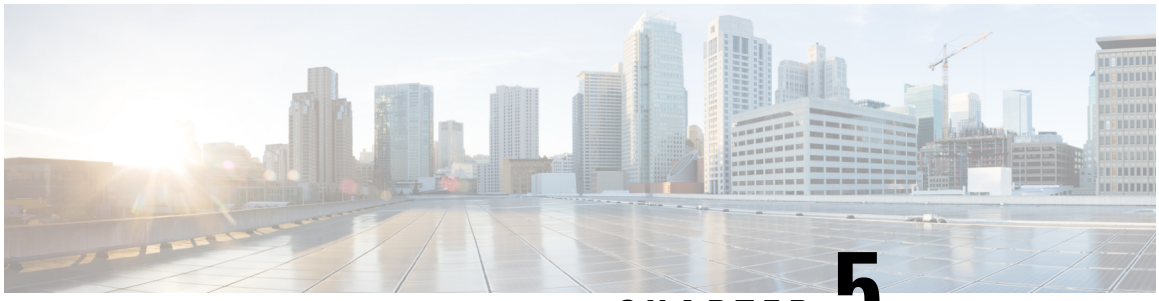
Feature Changes

Currently, P-GW sends 3GPP-User-Location-Info AVP in CCR-U for the event trigger Successful_Resource_Allocation, only if there is a change in the ULI. This feature has been implemented to comply with the 3GPP specifications. With this feature, P-GW sends 3GPP-User-Location-Info in CCR-U for the event trigger Successful_Resource_Allocation, even if there is no a change in the ULI. If the Resource-Allocation-Notification AVP is included in the Charging-Rule-Install AVP, 3GPP-User-Location-Information is included in the CCR-U sent towards the PCRF.

Limitations

Following are the limitations of this feature:

1. This feature works with diameter dictionary dpca-custom8.
2. Resource-Allocation-Notification AVP should be included within a Charging-Rule-Install AVP while installing/modifying rule.



CHAPTER 5

5G Non Standalone

This chapter describes the 5G Non Standalone (NSA) feature in the following sections:

- Feature Summary and Revision History, on page 207
- Feature Description, on page 208

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

The 5G NSA solution for SAEGW supports dcca-custom26 dictionary.	21.26
The 5G NSA solution for SAEGW supports Secondary RAT Usage IE during GnGp handover.	21.22
The 5G NSA solution for SAEGW supports dcca-custom1, dcca-custom7 and dcca-custom8 dictionaries.	21.11
The 5G NSA solution for SAEGW supports the following functionality: • P-GW Custom Dictionaries support over Gz for extended bitrate • S-GW Custom Dictionaries support over Gz for extended bitrate • P-GW Custom Dictionaries support over Gy and Rf for extended bitrate • S-GW support of Secondary RAT Data Usage Report in Gz CDRs	21.10
The 5G NSA solution for SAEGW supports the following functionality: • P-GW support of Secondary RAT Data Usage Report in Gz CDRs • P-GW support of Secondary RAT Data Usage Report in Rf CDRs • S-GW and P-GW support of statistics for DCNR PDNs	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
The 5G NSA solution for SAEGW supports the following functionality: • Feature License • Dedicated Bearers • Gy interface • URLLC QCI	21.8
First introduced.	21.6

Feature Description

Important 5G NSA feature is license controlled from release 21.8 onwards. Contact your Cisco account representative for detailed information on specific licensing requirements.

The 5G NSA solution for SAEGW supports the following functionalists:

- **High Throughput**

5G NR offers downlink data throughput up to 20 Gbps and uplink data throughput up to 10 Gbps. Some interfaces in EPC have the support to handle (encode/decode) 5G throughput. For example, NAS supports up to 65.2 Gbps (APN-AMBR) and S5/S8/S10/S3 (GTP-v2 interfaces) support up to 4.2 Tbps. The diameter interfaces S6a and Gx support only up to 4.2Gbps throughput, S1-AP supports only up to 10 Gbps and NAS supports up to 10 Gbps (MBR, GBR). New AVP/IE have been introduced in S6a, Gx , S1-AP, and NAS interfaces to support 5G throughput. See the *How It Works* section for more information.

- **DCNR Support on P-GW:**

  Supports configuration of DCNR feature at the P-GW-service, by configuring “Extended-BW-NR” feature in IMSA service. Advertises the DCNR feature support by sending “Extended-BW-NR” feature bit in “Feature-List-ID-2” towards PCRF. Forwards AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in CCR messages when it receives APN-AMBR values greater than 4.2Gbps from MME/S-GW. Decodes the extended AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" when it is received from PCRF.

- Sends AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when it receives MBR and GBR values greater than 4.2Gbps from MME/S-GW. Decodes the AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when received from PCRF. Supports dedicated bearer establishment with extended QoS. Sends AVP Extended-Max-Requested-BW-UL and "Extended-Max-Requested-BW-DL" in Gy records.

- **Ultra Low Latency Support**:

  Supports 5G requirements of Ultra-Reliable and Low Latency Communications (URLLC). 3GPP introduced URLCC QCI 80 (Non-GBR resource type), QCI 82 and 83 (GBR resource type). P-GW establishes default bearers with URLLC QCI 80, which is typically used by low latency eMBB applications. P-GW establishes dedicated bearers with URLLC QCI 82 and 83 (also with QCI 80 if dedicated bearers of Non-GBR type to be established), which is typically used by discrete automation services (industrial automation).

- **ICSR Support**

  With release 21.10 onwards ICSR for 5G NSA on SAEGW is supported.

- **Dynamic S-GW and P-GW selection by MME for DCNR capable UE**

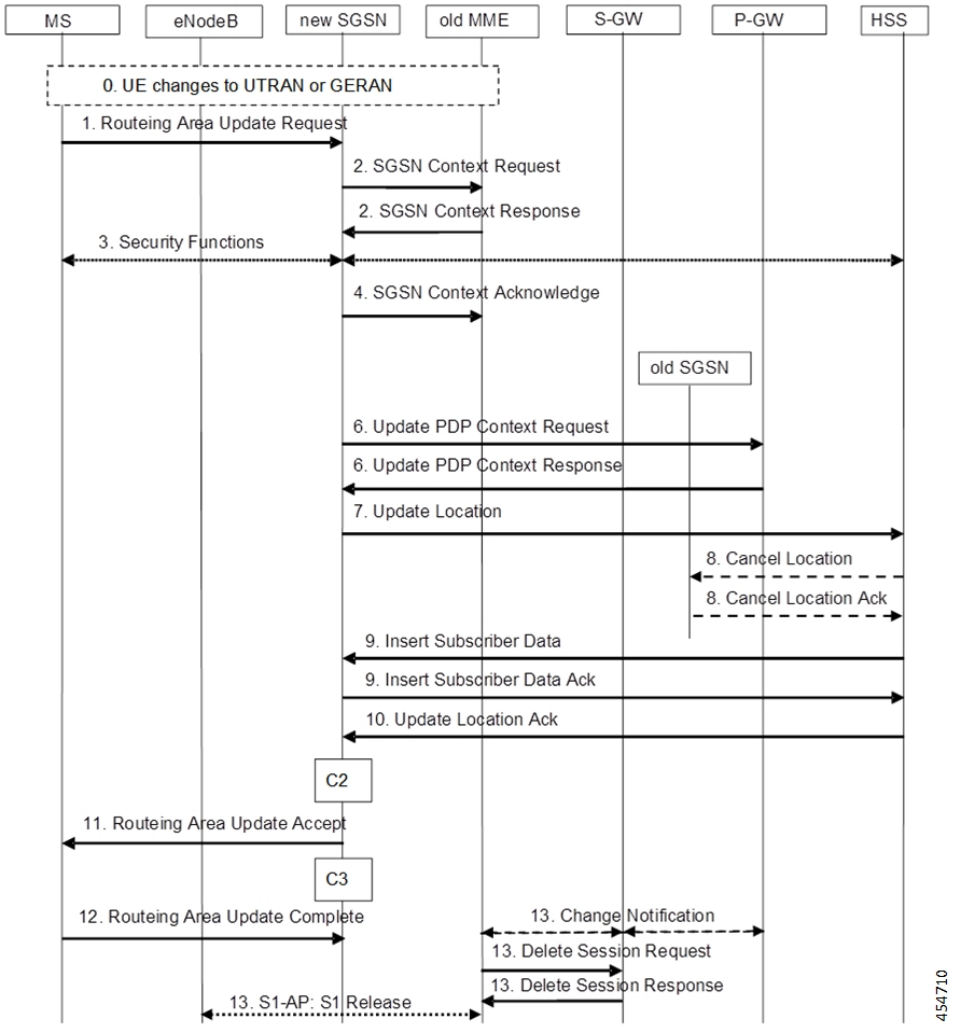
  When DCNR capable UE attempts to register in MME and when all DCNR validations are successful (for example DCNR feature configuration on MME, HSS not sending access-restriction for NR, and son on), the MME sets “UP Function Selection Indication Flags” IE with DCNR flag set to 1 in “Create Session Request” message. This feature is relevant for CUPS architecture to help SGW-C and PGW-C to select SGW-U and PGW-U which supports dual connectivity with NR. When S-GW receives this IE over S11, it sends this IE over S5 to P-GW. S-GW ignores IE if it receives it in Non-CUPS deployment.

- **P-GW Secondary RAT Usage Data Report Handling:**

  P-GW supports custom24 and custom44 for Gz and aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries for Rf to support Secondary RAT Data Usage Report in CDRs.

Support for Secondary RAT Usage During GnGp Handover

This feature supports the Secondary RAT usage reported in change notification request during 4G to 3G handover. The support is for handling the change notification with Secondary RAT Usage during the GnGp handover. Step 13 is added in the following diagram in support of this feature. The usage must be reported in next CDR generation.



IMSI Not Known

If there's no context found for IMSI specified in Secondary RAT Usage IE of change notification request Message, it returns the change notification response with cause value "IMSI/IMEI not known".

Limitations

Following are the known limitations for this feature:

- This feature only supports the handling of the secondary RAT usage IE.
- During the 4G to 3G handover, dedicated bearers are retained and Secondary RAT usage is reported for both Default and Dedicated bearers.

Enabling Secondary RAT Data Usage Report

Use the following configuration to enable Secondary RAT Data Usage Report:

```
configure
  context context_name
    pgw-service service_name
      dcnr
      end
```

Note The GGSN service associated with the P-GW service must have the DCNR enabled using the preceding CLI.

- **Statictics support for DCNR PDNs:**

  S-GW and P-GW statistics support for DCNR PDNs

- **S-GW Secondary RAT Usage Data Report Handling:**

  S-GW supports custom24 and custom6 dictionaries to support Secondary RAT Data Usage Report in CDRs over Gz.

- **P-GW Custom Dictionaries Support over Gz:**

  P-GW supports Custom44 and Custom24 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Multiple Presence Reporting Area Support:**

  S-GW supports Multiple-PRA action and Multiple-PRA Information over S11/S4 and S5/S8 interfaces. P-GW supports Multiple-PRA Action and Multiple-PRA Information over S5/S8 and Gx interfaces.

- **S-GW Custom Dictionaries Support over Gz :**

  S-GW supports custom24 and custom6 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gx:**

P-GW supports dpca-custom15, dpca-custom11, dpca-custom23, dpca-custom19 and dpca-custom17, dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

- Extended-Max-Requested-BW-UL
- Extended-Max-Requested-BW-DL
- Extended-GBR-DL
- Extended-GBR-UL
- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gy:**

  P-GW supports dcca-custom1, dcca-custom7, dcca-custom8, dcca-custom13 and dcca-custom26 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Rf:**

  P-GW supports aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

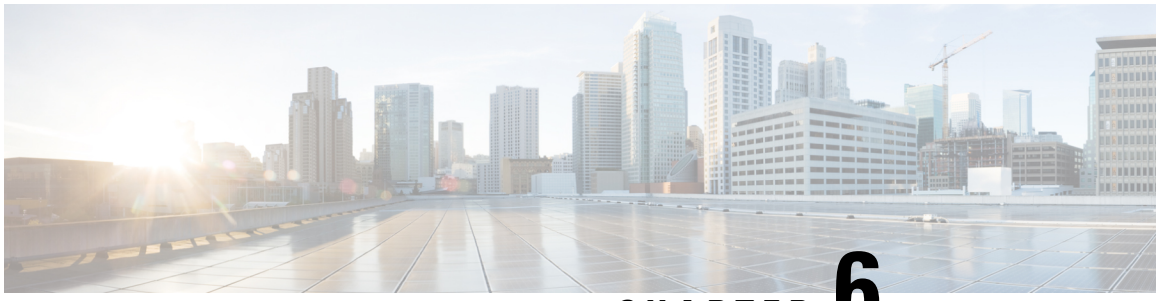
  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

Multiple Presence Reporting Area

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.



Note This feature is introduced in release 21.9.1. For more information, refer to the *Presence Reporting Area* chapter in the *P-GW Administration Guide*.



CHAPTER 6

Adding ECPD Identification and Account Numbers to Pilot Packets

- Feature Summary and Revision History, on page 215
- Feature Description, on page 216
- Configuring Pilot Packet, on page 217

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *GGSN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The Pilot Packet feature provides key information about a subscriber session, such as subscriber identity and subscriber IP address, to an external element. When the subscriber allocates or deallocates IP address during an event trigger, a “pilot” packet is generated. Using this information new service such as Subscriber Analytics are enabled and sent in UDP transport.

Pilot Packet consists of the following information in the form of Type Length Values (TLVs):

- Allocation/De-allocation Flag
- MSISDN (MDN)
- IMSI
- Allocated Address-IPv4
- Allocated Address-IPv6-Address
- Allocated NAT IPv4 Address
- NAT Address Port Chunk Start
- NAT Address Port Chunk Size
- Serving Network Identifier
- Foreign Agent IP Address
- NAI
- RAT Type

The operator enables the network element with Pilot packet to gain and report enterprise-level information through the Flexible-Services-Container TLV on SGi interface.

Flexible-Services-Container consists of the following enterprise-level information:

- Enterprise Customer Profile Database Identification (ECPD ID)
- Account Number

For example: ECPD ID = 3458312; Account Number = 0442058164-00001

Notes

Following are the important notes:

- P-GW adds new TLV to the Pilot packet for subscribers, only if configured through CLI and received on S6b in AAA message.
- P-GW ignores Flexible-Services-Container received in the Re-Auth procedure.
- The contents and interpretation of the enterprise information (ECPD ID and Account Number) is not required for P-GW or GGSN services. The data is not parsed by P-GW or GGSN and passed transparently in Pilot packet.

Configuring Pilot Packet

To configure Pilot Packets containing key information about a subscriber session to third-party network elements, use the following configuration:

```
configure
   context context_name
     pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type
 | serving-nw-id | flexible-services-container } | name server_name
source-ip-address source_ip_address destination-ip-address destination-ip_address
 destination-udp-port udp_port_value [ dscp-marking dscp-value ] | trigger
rat-change generate { nat-info-only | user-info-and-nat-info |
user-info-only } }
     default pilot-packet { attribute { foreign-agent-ip-address | nai |
 rat-type | serving-nw-id | flexible-services-container } | trigger
rat-change }
     no pilot-packet { attribute { foreign-agent-ip-address | nai |
rat-type | serving-nw-id | flexible-services-container } | name server_name
 | trigger rat-change }
     end
```

NOTES:

- **pilot-packet { attribute flexible-services-container}**: Sends the optional flexible-services-container in Pilot packets.
- **default pilot-packet { attribute flexible-services-container }**: Does not send the optional flexible-services -container in Pilot packets.
- **no pilot-packet { attribute flexible-services-container }**: Disables flexible services container information in Pilot packets.

Verifying the Configuration

Use the following commands to verify the Pilot packets configuration.

- **show configuration**
- **show configuration verbose**

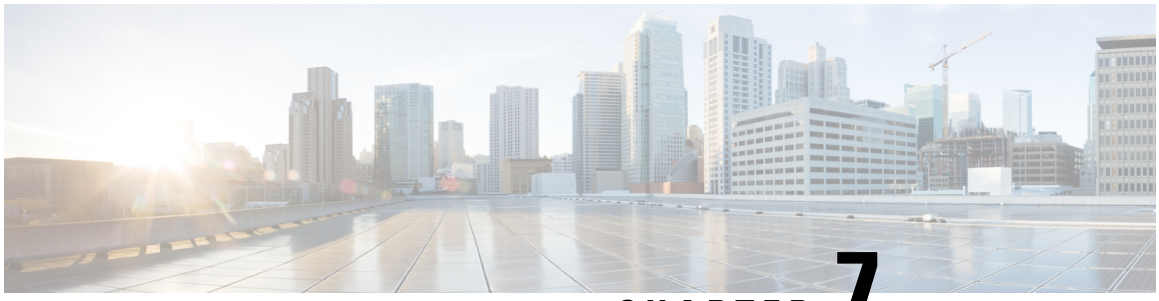
show configuration

The output of this command includes the following field.

Table 27: show config Command Output Description

Field	Description
flexible-services-container	Indicates that an optional TLV Flexible Services Container is sent in Pilot packets.

The **show config verbose** command also includes similar field output.



CHAPTER 7

APN-Backoff Timer Support

This chapter describes StarOS support for the APN-Backoff Timer feature on the P-GW and SAEGW.

- Feature Description, on page 219
- Configuring APN Backoff Timer Support on the P-GW/SAEGW, on page 221
- Monitoring the Feature, on page 222

Feature Description

Previously, the P-GW did not distinguish signaling traffic from Delay Tolerant or Low Priority devices such as low priority machine-to-machine traffic.

The UE was able to indicate its device profile to the MME via NAS and Attach Request messages. The MME was able to pass this information to the P-GW via the Signaling Priority Indication Information Element (IE) on the S5 interface. Some UEs may not have supported the sending of the Signaling Priority Indication IE on the S5 interface to the P-GW. As a result, the P-GW could not distinguish between the signaling types. With the current release, the P-GW can distinguish between these signaling types.

In addition, during overload situations, the P-GW previously allowed new sessions from Low Access Priority Indicator (LAPI) devices and treated the traffic from LAPI devices with the same priority as the normal UEs. With the current StarOS release, during overload conditions, the P-GW can be configured to back off the traffic that is identified as LAPI. The identification is based on either the APN configuration or the Signaling Priority Indicator IE.

The backoff timer algorithm and the R12 GTP-C Load/Overload Control algorithm work together. This feature provides the benefit of rejecting low priority calls in turn allowing more bandwidth for high priority calls.

Functionality

The following functionality has been implemented to support the APN Backoff Timer functionality:

1. The Signaling Priority Indication IE on the S5 interface in the Create Session Request message identifies the low priority devices.
2. A LAPI APN can be configured. Any call landing on that APN is considered a LAPI call.
3. A back off timer value is configured in the APN. The backoff timer is sent in Create Session Response messages in the P-GW Back-Off Timer IE.

4. If the following conditions are met, the call is rejected with the cause APN Congestion. The configured backoff timer value is inserted in the Back Off Timer IE in the Create Session Response message.
   - Once an incoming call is identified as LAPI due to condition 1 or 2 above.
   - The P-GW is in the overload state.
   - The backoff timer is configured.
5. The M2M license must be present and enabled on the system. The GTP-C Load/Overload feature's configuration and backend reporting of overload parameters works with the M2M license.
6. In some dictionaries (for example, custom35) CDRs have a LAPI field for LAPI calls. This field is populated when the Signaling Priority Indication IE indicates that the call is a LAPI call. However, if the call is of type LAPI due to the LAPI APN configuration, then the CDR should not have the LAPI field.
7. Bulk statistics, counters, and statistics have been implemented at the APN and P-GW service level to show the number of calls rejected due to the APN Backoff Timer feature.

GTP-C Overload Feature and the M2M License

To detect whether the P-GW/SAEGW is in the overload state, the GTP-C Overload feature's framework has been used. It is tied to the M2M license so that only overload configuration and reporting of the overload state is enabled. The remaining overload features such as, sending the OCI towards the peers, throttling, and receiving OCIs from peers do not work. This leads to the following behavioral scenarios:

If a Call is a LAPI call and the Backoff Timer is Configured and the P-GW is in the Overload State:

- Only M2M License: Call is rejected with cause APN Congestion.
- Only GTP-C Overload Enabled: Not applicable as backoff timer cannot be configured.
- Both M2M and Overload Enabled: Call is rejected with cause APN Congestion. That is, LAPI takes priority over the GTP-C Load/Overload feature.

If a Call is Not LAPI or Backoff Timer is Not Configured and the P-GW is in the Overload State:

- Only M2M License Enabled: No impact. Call is accepted normally.
- Only Overload License Enabled: Call accepted. OCI will be sent in the Create Session Response message. Overload feature works normally.
- Both M2M and Overload Features Enabled: Call accepted. OCI is sent in the Create Session Response message. Overload feature works normally. Backoff Timer feature is ignored.

Licensing



Important The APN Backoff Timer feature requires that the M2M license be enabled on the P-GW/SAEGW. Contact your Cisco account or support representative for licensing details.

Configuring APN Backoff Timer Support on the P-GW/SAEGW

This section describes how to configure APN Backoff Timer Support on the P-GW/SAEGW. The procedure consists of the following tasks:

1. Configuring LAPI Behavior
2. Configuring the Backoff Timer
3. Verifying the Configuration

Configuring LAPI Behavior

Use the following example to configure LAPI behavior:

```
configure
  apn apn_name
    pdn-behavior lapi
    end
```

To disable LAPI behavior:

```
configure
  apn apn_name
    no pdn-behavior
    end
```

Notes:

- **pdn-behavior lapi** configures the APN as a LAPI APN.
- **no pdn-behavior** disables the LAPI APN configuration.



Caution Do not configure the emergency APN and **pdn-behavior lapi** settings in the same APN, as these two settings are mutually exclusive. If both settings are configured in the same APN the **pdn-behavior lapi** configuration takes priority. As a result, if both settings are configured and the system is overloaded, the call will be rejected.

To determine if both settings are configured in the same APN, execute the **show configuration error verbose** command in *Exec Mode*. The command output contains a warning if both settings are configured in the same APN.

Configuring the APN Backoff Timer and Jitter Values

The P-GW requires a fixed value and a jitter to introduce randomness in the Backoff Timer value that is returned to the MME for different sessions; this helps prevent a session storm after the Backoff Timer expiry.

Use the example below to configure the APN Backoff Timer and Jitter Values:

```
configure
  apn apn_name
```

```
backoff timer-value seconds [ jitter seconds ]
end
```

To disable Backoff Timer functionality:

```
configure
  apn apn_name
    no backoff timer-value
    end
```

Notes:

- **backoff timer-value** *seconds* configures the backoff timer value, in seconds. Valid entry is an integer from 0 to 576000 seconds. There is no default setting.
- **jitter** *seconds* configures the jitter value, in seconds. Valid entry is from 0 to 1000 seconds. There is no default setting.

Verifying the Configuration

To verify the configuration:

In *Exec Mode*, issue the **show apn name** *apn_name* command, *apn_name* is the name of the APN for which you want to view configuration settings.

In the command output, look for the following fields:

- pdn behavior: <*lapi*> or <*no pdn-behavior*>
- Backoff Timer Value: <*seconds*> Jitter: <*seconds*>

Verify that the configuration settings are correct. If any of the settings are incorrect, use the configuration procedure in this chapter to reconfigure the incorrect setting(s).

Monitoring the Feature

This section provides information that enables operators to monitor the APN Backoff Timer feature.

Bulk Statistics

APN Schema

The following bulk statistics have been added to the APN Schema to support the APN Backoff Timer feature:

- rej-pdn-backofftimer

P-GW Schema

The following bulk statistic has been added to the P-GW schema to support the APN Backoff Timer feature.

- sessstat-rej-pdn-backofftimer

SAEGW Schema

The following bulk statistic has been added to the SAEGW schema to support the APN Backoff Timer feature:

- pgw-sessstat-rej-pdn-backofftimer

Show Command Output

This section describes the Exec Mode show commands and output available to monitor the APN Backoff Timer Support on the P-GW/SAEGW feature.

show apn name

The output of this command has been enhanced to show the configured backoff timer, jitter, and PDN behavior settings. These settings appear only if the M2M feature license is enabled.

- pdn behavior: lapi
- Backoff Timer Value: <*seconds*> Jitter: <*seconds*>

show apn statistics

The output of this command has been enhanced to indicate the number of PDNs rejected as a result of the configured backoff timer value.

- Number of PDNs rejected due to backoff algorithm:

show configuration apn name

The output of this command provides the operator with the current APN Backoff Timer settings.

- pdn-behavior lapi (if feature is enabled)
- backoff timer-value <*secs*> jitter <*secs*>

show pgw-service statistics

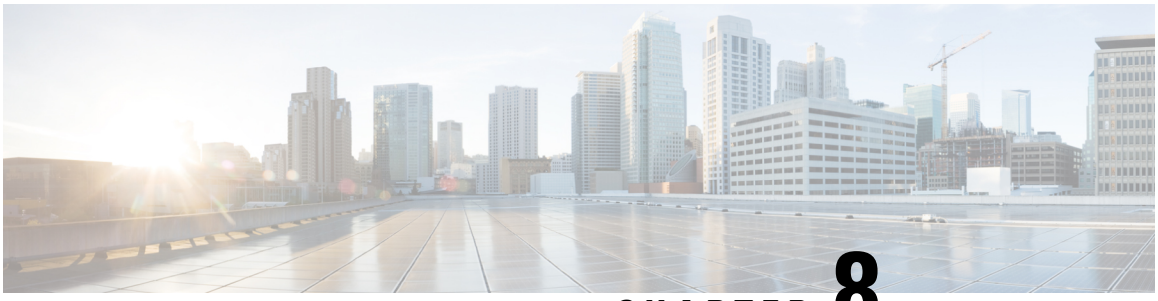
The output of this command has been enhanced to provide the total number of PDNs rejected due to the configured backoff timer value.

- PDNs Rejected By Reason:
  - APN-Backoff Timer

show session disconnect-reasons

The following disconnect reason has been added to support the APN Backoff Timer feature.

- apn-congestion



CHAPTER 8

APN Rate Control for CIoT Devices

This chapter contains the following topics:

- Feature Summary and Revision History, on page 225
- Feature Description, on page 226
- How it Works, on page 226
- Configuring the APN Rate Control for CIoT Devices Feature, on page 232
- Monitoring and Troubleshooting the APN Rate Control for CIoT Devices Feature, on page 232
- Accounting Support, on page 234

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• C-SGN • P-GW
Applicable Platform(s)	• UGP • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference* • *Ultra IoT C-SGN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.15

Feature Description

In usual scenarios, CIoT-enabled UE send data packets infrequently. However, in unusual scenarios, UE can send data packets frequently during a short period resulting in network congestion and affecting services. APN Rate Control is one of the 3GPP standards-compliant mechanisms for rate limiting when UEs send data packets.

APN Rate Control allows Home Public Land Mobile Network (HPLMN) operators to control the amount of user data sent in Downlink (DL) and Uplink (UL). This is done with help of policing the user data on a maximum number of user data packets per time-unit, and/or maximum number of user data octets per time-unit, for both DL and UL.

How it Works

APN Rate Control policing for DL is done in the P-GW or the SCEF, and the APN Rate Control policing for UL is done in the UE. The P-GW or SCEF can also do APN Rate Control UL policing. For more information on:

- APN Rate Control UL in the UE, see 3GPP TS 24.301.
- APN Rate Control in the SCEF, see 3GPP TS 29.128.

Note The existing AMBR mechanisms are not suitable for APN Rate Control for CIoT Devices considering radio efficiency and UE battery-life. For example, an AMBR greater than 100 Kbps translates to a potentially large daily data volume.

The P-GW or Service Capability Exposure Function (SCEF) sends an APN Uplink Rate Control command to the UE using the PCO information element (IE). The APN Uplink Rate Control applies to data PDUs sent on that APN by either Data Radio Bearers (S1-U) or Signaling Radio Bearers (NAS Data PDUs). The UE complies with this uplink rate control instruction. The UE considers the rate control instruction as valid until it receives a new one from either P-GW or from SCEF. The P-GW or SCEF enforces the Uplink Rate Control by discarding or delaying packets that exceed the rate as indicated to the UE.

APN Rate Control Indications

APN Rate Control Indication Status is sent as part of Protocol Configuration Options (PCO)/Extended Protocol Configuration Options (ePCO). If P-GW/MME supports the ePCO as part of its capability exchange, the P-GW/S-GW sends the APN Rate Control parameters as part of ePCO. If ePCO is not supported by these entities, the P-GW/S-GW sends the APN Rate Control parameters as part of PCO.

As part of PCO/ePCO, the APN Rate Control parameters are sent as “additional parameters list”. A specific “container identifier” identifies the type of the parameter that is carried in a container. The “container identifier” related to the APN Rate Control are:

- Mobile Station (MS) to network direction:
  - 0016H (APN rate control support indicator)
  - 0019H (Additional APN rate control for exception data support indicator)
- Network to MS direction:
  - 0016H (APN rate control parameters)
  - 0019H (Additional APN rate control for exception data parameters)

When the “container identifier” indicates APN Rate Control support indicator, the “container identifier contents” field is empty and the “length of container identifier contents” indicates a length equal to zero. If the “container identifier contents” field is not empty, it is ignored. This information indicates that the MS supports APN Rate Control functionality.

When the “container identifier” indicates APN Rate Control parameters, the “container identifier contents” field contains parameters for APN Rate Control functionality.

When the “container identifier” indicates Additional APN Rate Control for exception data support indicator, the “container identifier contents” field is empty and the “length of container identifier contents” indicates a length equal to zero. If the “container identifier contents” field is not empty, it is ignored. This information indicates that the MS supports additional APN Rate Control for exception data functionality.

When the “container identifier” indicates Additional APN Rate Control for exception data parameters, the “container identifier contents” field contains parameters for additional APN Rate Control for exception data functionality.

APN Rate Control Status

APN Rate Control Status is the new IE, added as part of Create Session Request (CSReq), Delete Bearer Request (DBReq), and Delete Session Response (DSRes), which holds information of APN Rate Control Value. This IE is encoded as part of CSReq on the UR reattach to denote the P-GW about the remaining limits available for the subscriber on the current timeout period.

P-GW includes this IE when the DBReq is sent only for the default bearer, so that it can be used when the UE is attaching again. In addition, the P-GW includes this IE when the DSRes is sent to MME through S-GW.

	Bits								
Octets	8	7	6	5	4	3	2	1	
1	Type = 204 (decimal)								
2 to 3	Length = n								
4	Spare				Instance				
5 to 8	Number of Uplink packets allowed								
9 to 12	Number of additional exception reports								
13 to 16	Number of Downlink packets allowed								

17 to 24	APN Rate Control Status validity Time	
25 to (n+4)	These octet(s) is/are present only if explicitly specified	

Octets 17 to 24 are coded as time in seconds relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where the binary encoding of the integer part is in the 32 most significant bits, and binary encoding of the fraction part in the 32 least significant bits. The fraction part is expressed with a granularity of 1/2**32 second.

The APN Rate Control Status information is sent by P-GW to MME through S-GW to store the APN Rate control parameters in Mobility Management (MM) context. This helps in restoring the rate control for the same subscriber when it is reestablished again after some time. The parameters are treated as the remaining messages on the remaining time period of the time-unit.

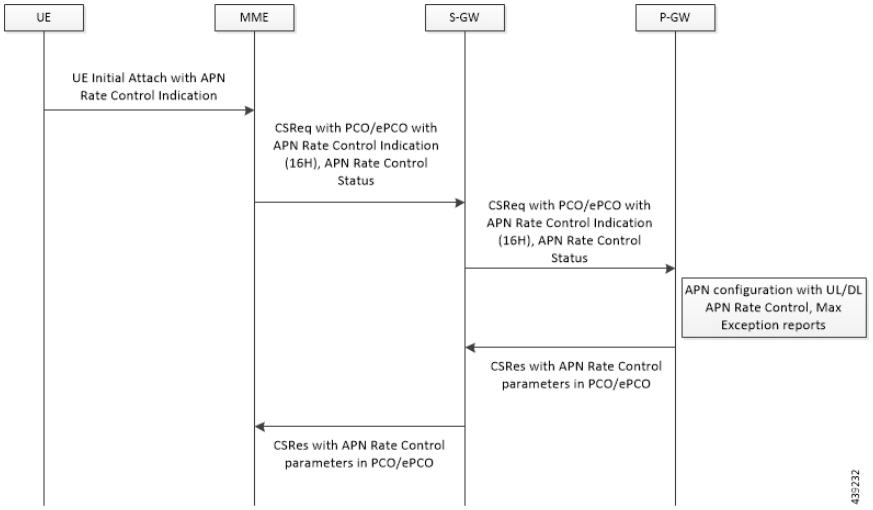
On reestablishment of the same subscriber (on first PDN for the same APN), the MME provides the information back to P-GW in PCO/ePCO. While processing, P-GW considers the values received from MME instead of its local configuration until the first timeout is complete.

Call Flows

This section describes the features' key call flows.

APN Rate Control Handling at P-GW on CSReq

On establishment or re-establishment of the subscriber for the APN, the MME sends the Indication Flags of APN Rate limit, Addition Exception indication, and APN Rate Control status in the CSReq.



Steps	Description
1	UE Initial Attach with APN Rate Control Indication is sent from UE to MME.
2	On receiving CSReq, the P-GW considers the APN Rate Control Status while encoding the APN Rate Control parameters in PCO, and while enforcing the APN Rate Control.
3	P-GW has two options to enforce the APN Rate Control:

Steps	Description
	1. On subsequent establishment of the first PDN connection for the given APN, the P-GW/SCEF receives the previously stored APN Rate Control Status, and if the first APN Rate Control validity period has not expired, it applies the received APN Rate Control Status and provides the related parameters to the UE in the PCO (instead of the configured APN Rate Control parameters). 2. If the initially applied parameters differ from the configured APN Rate Control parameters, the P-GW/SCEF uses the configured APN Rate Control parameters after the first APN Rate Control validity period expires, and sends an update to the UE with the configured APN Rate Control parameters.
4	P-GW sends CSRes to S-GW. P-GW prepares and encodes the APN Rate Control parameter into PCO/ePCO and sends back to S-GW in CSRes message with APN Rate Control parameters and Additional APN rate control parameters for exception data.
5	S-GW forwards the information (received from P-GW in Step 4) to MME.

APN Rate Control Parameter encodes information about Uplink time-unit and the Uplink rate supported.

8	7	6	5	4	3	2	1	
Spare				AER	Uplink time-unit			Octet 1
Maximum uplink rate								Octet 2 to Octet 4

Additional APN Rate control parameter for exception data encodes information about Uplink time-unit and the Uplink rate that is supported for the additional exception data.

8	7	6	5	4	3	2	1	
Spare					Uplink time-unit			Octet 1
Additional uplink rate for exception data								Octet 2 to Octet 3

Where Uplink Time-unit can take the value of any one as shown in the following format.

Uplink time-unit (Octet 1)	
Bit	
3 2 1	
0 0 0	Unrestricted
0 0 1	Minute
0 1 0	Hour
0 1 1	Day

1 0 0	Week

Maximum uplink rate (Octet 2 to Octet 4) is a binary coded representation of the maximum number of messages the UE is restricted to and sent per time-unit. If the uplink time-unit is set to "unrestricted", the maximum uplink data volume the UE can send is not restricted.

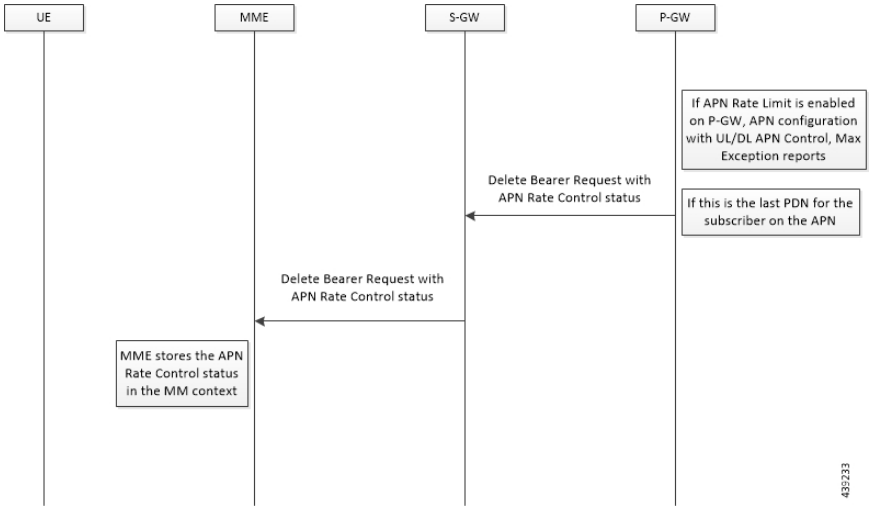
P-GW informs MME about UL APN Rate Control information in APN Rate Control Parameter, which is later stored by MME in MM context.

P-GW side APN Rate Control is based on “Maximum Allowed Rate” per direction. If P-GW provided the “number of additional allowed exception report packets per time unit” to the UE, then the "maximum allowed rate" is equal to the “number of packets per time unit” plus the “number of additional allowed exception report packets per time unit”. Otherwise, the “maximum allowed rate” is equal to the “number of packets per time unit”.

The P-GW enforces the uplink rate by discarding or delaying packets that exceed the “maximum allowed rate”. The P-GW enforces the downlink rate by discarding or delaying packets that exceed the downlink part of the “maximum allowed rate”.

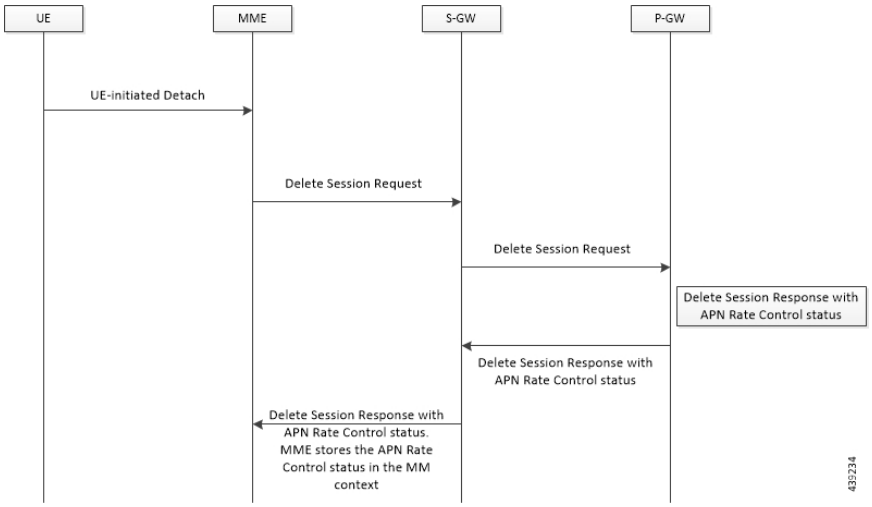
APN Rate Control Handling at P-GW on DBReq

On bearer deletion, if P-GW detects the current bearer is going to be the last bearer in the PDN for that specified APN, then it includes the APN Rate control status to MME through S-GW with the current quota of the rate limiting values (remaining messages on the remaining time-unit).



APN Rate Control Parameters on DSRes

On receiving the DSReq, P-GW clears the subscribers and sends the APN Rate Control status in CSRes with the remaining quota of the time and the messages for the subscriber to MME to update its MM context.



Licensing

The APN Rate Control for CIoT Devices is a license-controlled feature. Contact your Cisco Account representative for more information.

Standards Compliance

The APN Rate Control for CIoT Devices feature complies with the following standards:

- 3GPP TS 29.274 v15.8.0 - 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 23.401 v15.7.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

Limitations and Considerations

The APN Rate Control for CIoT Devices feature has the following limitations and restrictions:

- This feature takes highest priority and checks if the rate limit is done before checking for any other feature.
- Both uplink and downlink rate limit take same time-unit (unlimited, minute, hour, day, or week) value. It never accepts different values.
- Applicable for P-GW and Collapsed calls.
- Applicable only for CIoT subscribers; check on RAT Type is done to identify the CIoT subscribers.
- Applicable only for the CIoT IP PDNs. This feature is not applicable for Non-IP PDNs.
- This feature is implemented on I-CUPS on ASR 5500 in slow path if the amount of traffic for IoT is low. Only data packets of the APN Rate-controlled CIoT subscribers go in slow path. Remaining CIoT subscribers still proceed on the existing implementation.

- In case of reattach, P-GW sends the CSRes with APN Rate Control parameters which are remaining for the subscriber to UE to perform Uplink Rate control operation. On time-unit expiry, P-GW renews its quota, but it never shares the updated quota values to UE. UE gets the P-GW configured APN Rate Control values only at initial attach.
- If Virtual-APN concept is applied on the subscriber, the Gi-APN Rate Control parameters are considered.

Configuring the APN Rate Control for CIoT Devices Feature

Use the following configurations to enable the feature.

```
configure
   context context_name
      apn apn_name
        iot-rate-control time-unit { unrestricted | mins | hours | days |
 week } downlink packet-count dl_packet_count uplink packet-count ul_packet_count
 aer aer_value
        end
```

NOTES:

- **time-unit { unrestricted | mins | hours | days | week }**: Specifies the mode of time-unit.
- **downlink**: Applies the APN Rate Control in the downlink direction.
- **packet-count** *dl_packet_count*: Specifies the allowed number of downlink packets. The *dl_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on the downlink direction.
- **uplink**: Applies the APN Rate Control in the uplink direction.
- **packet-count** *ul_packet_count*: Specifies the allowed number of uplink packets. The *ul_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on the uplink direction.
- **aer** *aer_value*: Specifies the number of Additional Exception Reports (AER) in the uplink direction. The *aer_value* must be an integer ranging from 1 through 65535.
- If previously configured, use the **no iot-rate-control** CLI command to disable the feature.

Monitoring and Troubleshooting the APN Rate Control for CIoT Devices Feature

This section describes the CLI commands available to monitor and/or troubleshoot the feature.

Show Command Support

The following show CLI commands are available in support of the feature.

show apn statistics

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control:
  - Dropped UL packets: Displays the total number of APN Rate Control uplink packets that are dropped.
  - Dropped DL packets: Displays the total number of APN Rate Control downlink packets that are dropped.
  - Dropped UL bytes: Displays the total number of APN Rate Control uplink bytes that are dropped.
  - Dropped DL bytes: Displays the total number of APN Rate Control downlink bytes that are dropped.

show session subsystem facility sessmgr all debug-info

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control
  - Dropped UL packets: Displays the total number of APN Rate Control uplink packets that are dropped.
  - Dropped DL packets: Displays the total number of APN Rate Control downlink packets that are dropped.
  - Dropped UL bytes: Displays the total number of APN Rate Control uplink bytes that are dropped.
  - Dropped DL bytes: Displays the total number of APN Rate Control downlink bytes that are dropped.

show subscriber full all

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control:
  - Allowed UL limit: Displays the number of packets allowed for uplink direction.
  - Allowed DL limit: Displays the number of packets allowed for downlink direction.
  - Remaining UL limit: Displays the number of packets remaining for uplink direction.
  - Remaining DL limit: Displays the number of packets remaining for downlink direction.
  - Allowed Time unit: Displays the time-unit configured in either unrestricted, minutes, hours, days, or week mode.
  - Status Validity Time: Displays the validity time in YYYY-MM-DD HH:MM:SS format.

Bulk Statistics

This section provides information on the bulk statistics for the APN Rate Control for CIoT Devices feature.

APN Schema

The following bulk statistics are available in the APN schema in support of the APN Rate Control for CIoT Devices feature.

Bulk Statistics	Description
apn-rate-control-ul-pkt-drop	Indicates the total number of APN Rate Control uplink packets that are dropped.
apn-rate-control-dl-pkt-drop	Indicates the total number of APN Rate Control downlink packets that are dropped.
apn-rate-control-ul-bytes-drop	Indicates the total number of APN Rate Control uplink bytes that are dropped.
apn-rate-control-dl-bytes-drop	Indicates the total number of APN Rate Control downlink bytes that are dropped.

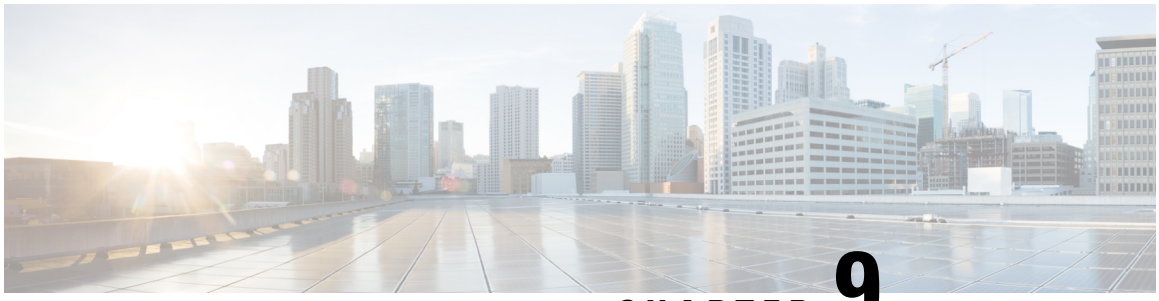
Accounting Support

The following table provides details of the GTPP dictionary available in support of the APN Rate Control for CIoT Devices feature.

CDR Dictionaries/Fields	
Type of dictionary change (New/Modified):	Modified
Dictionary name:	P-GW custom24 GTPP dictionary
Based on (3GPP specification):	3GPP TS 32.299
Applicable record type(s):	G-CDR
Applicable product:	P-GW

The following CDR fields are introduced in the P-GW custom24 GTPP dictionary:

1. Field name: datapacketsFBCDownlink
   - Description: Downlink Packets count
   - Format: Integer
   - CLI command to configure the field: **gtpp fbc-downlink-pkt-cnt**
   - Default value for field: 0
2. Field name: datapacketsFBCUplink
   - Description: Uplink Packets count
   - Format: Integer
   - CLI command to configure the field: **gtpp fbc-uplink-pkt-cnt**
   - Default value for field: 0



CHAPTER 9

Backup and Recovery of Key KPI Statistics

This feature allows the backup of GGSN, P-GW, SAEGW, and/or S-GW counters for recovery of key KPI counter values after a session manager (SessMgr) restart.

This chapter includes the following information:

- Feature Description, on page 235
- How It Works, on page 235
- Configuring Backup Statistics Feature, on page 237

Feature Description

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

How It Works

A key set of counters used in KPI computation will be backed up for recovery if a SessMgr task restarts. The counters that will be backed up are determined by the KPIs typically used in several operator networks.

The backup of counters is enabled or disabled via configuration. The configuration specifies the product (GGSN, P-GW, SAEGW, and/or S-GW) for which counters will be backed up and also a time interval for the backup of the counters.

Architecture

When this feature is enabled (see *Configuring Backup Statistics Feature* below), the GGSN, P-GW, SAEGW, and/or S-GW only backs up the counters maintained at the SessMgr. The recovery function does not need to be configured or started as it occurs automatically as needed when the feature is enabled.

The counters are backed up to the AAAMgr that is paired with the SessMgr.

Checkpointing

Node-level statistics are checkpointed at AAAMgr. Once statistics are backed up for a specific product, all the associated services, such as eGTP-C and GTP-U statistics, are also checkpointed.

Recovery

When SessMgr restarts, recovery is performed by receiving all the stored statistics from the mapped AAAMgr and the recovered values are added to the backup counters maintained at per-service level. This will not impact session recovery time as the backed up counters are pushed to SessMgr only after session recovery is complete.

Since session recovery is complete, the session managers may start processing calls. In such cases, the counters will continue to be incremented. The recovered values of the corresponding counters will always be added to the existing counters. Gauge counters are checkpointed but not recovered.

Order of Statistics Collection

The upper limit of checkpoint messaging is a maximum of 1 MB. Before picking any node to checkpoint, available memory is checked. If memory is insufficient, the whole node is discarded.

Since there is 1 MB limit, nodes/statistics to checkpoint are prioritized as follows:

1. SAEGW statistics:
   - P-GW and S-GW service node-level statistics collected
2. P-GW service node configuration will store the following statistics:
   - P-GW, eGTP-C ingress, GTP-U ingress, per-interface (s2a, s2b, s5s8), and GGSN (if associated) statistics collected
   - SAEGW associated P-GW service statistics not collected
3. S-GW service node configuration will store the following statistics:
   - S-GW, eGTP-C ingress/egress, and GTP-U ingress/egress statistics collected
   - SAEGW associated S-GW service statistics not collected
4. GGSN statistics:
   - GGSN service statistics, if not associated with P-GW service, collected
5. Session disconnect reasons collected if GGSN/P-GW/SAEGW/S-GW is enabled

Error Handling

If adding new statistics is going to cause overflow of 1 MB buffer, that service and the corresponding node will not be included. Checkpointing of any further nodes will also be stopped. Error level log will be flagged if total memory requirement goes above 1 MB.

Limitations

- A backup interval must be specified and counters are backed up only at the specified interval. For example, if the backup interval is specified as 5 minutes, then counters are backed up every 5 minutes. Suppose backup happened at Nth minute and the configured backup interval is for every 5 minutes, then if a task crash happens at N+4 minutes, the GGSN, P-GW, SAEGW, and/or S-GW recovers only the values backed up at Nth minute and the data for the past 4 minutes is lost.
- Only statistics maintained at the SessMgr are backed up. Statistics at other managers are not backed up or recovered.
- The following statistics are not considered for backup:
  - APN-level statistics
  - eGTP-C APN-QCI statistics
  - DemuxMgr statistics
- The CLI command **clear statistics** will not trigger checkpoint to delete the node statistics on AAAMgr. New checkpoint after timer expiry will overwrite the statistics.
- Maximum of 1 MB of statistics will be stored on AAAMgr. Services after the maximum size limit are not backed up.
- Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.
- If SessMgr restarts and AAAMgr restarts before SessMgr recovers statistics from AAAMgr, then backed up statistics are lost.
- This feature is not applicable for ICSR.

Configuring Backup Statistics Feature

For the Backup and Recovery of Key KPI Statistics feature to work, it must be enabled by configuring the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

Configuration

The following CLI commands are used to manage the functionality for the backing up of the key KPI statistics feature.

Enabling

The following configures the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW and enables the Backup and Recovery of Key KPI Statistics feature.

```
configure
     statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

Setting the Backup Interval

The following command configures the number of minutes (0 to 60) between each backup of the statistics. When the backup interval is not specified, a default value of 5 minutes is used as the backup interval

```
configure
     statistics-backup-interval minutes
     exit
```



Important Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.

Disabling

The following configures the GGSN, P-GW, SAEGW, and/or S-GW to disable the backing up of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

```
configure
     no statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

Verifying the Backup Statistics Feature Configuration

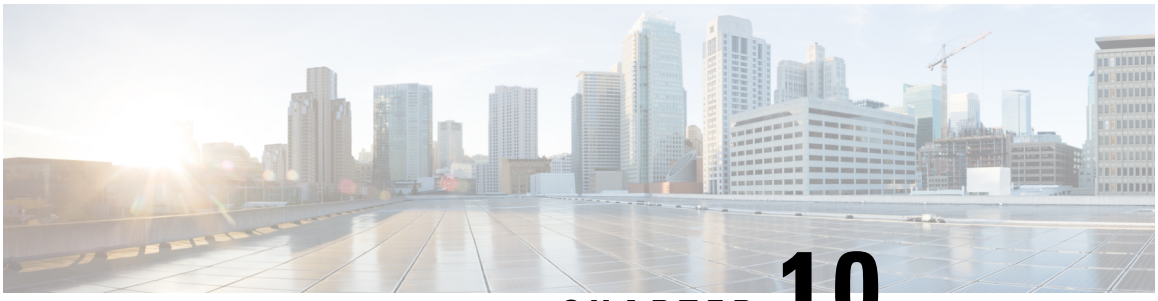
Use either the **show configuration** command or the **show configuration verbose** command to display the feature configuration.

If the feature was enabled in the configuration, two lines similar to the following will appear in the output of a **show configuration [verbose]** command:

```
statistics-backup  pgw
statistics-backup-interval 5
```

Notes:

- The interval displayed is 5 minutes. 5 is the default. If the **statistics-backup-interval** command is included in the configuration, then the 5 would be replaced by the configured interval number of minutes.
- If the command to disable the feature is entered, then no statistics-backup line is displayed in the output generated by a **show configuration [verbose]** command.



CHAPTER 10

Bearer Re-establishment

- Feature Summary and Revision History, on page 239
- Introduction to Bearer Re-establishment , on page 240
- How it Works, on page 240
- Enabling Modify Bearer Request Forward from S-GW to P-GW, on page 240
- P-GW Invokes Local Policy with New Event Restore-Bearers, on page 241
- Show Commands and Outputs, on page 242

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Table 28: Revision History

Revision Details	Release
First introduced	21.19

Introduction to Bearer Re-establishment

A UE Relay Network comprises of multiple RAN and EPC nodes.

In some deployments, one MME can play the role of both User-UE MME and Relay-UE MME.

In a UE Relay network, System Architecture Evolution Gateways (SAEGWs) are deployed to play the role of combined 'Relay-UE's SGW/P-GW'. The SAEGWs are configured using only local-policy (that is no connection to PCRF).

As part of initial attach request from Relay Node UE, P-GW (in the aforementioned SAEGW) creates dedicated bearers (for example, QCI-1 for GBR and QCI5 for non-GBR) on top of the default bearer (for example, QCI6). This is done based on an appropriate local policy configuration which is described in later sections of this chapter.

When RF condition degrades, Relay Node UE loses the RRC connection to macro eNB. As a result, macro eNB initiates an S1 Release procedure with abnormal cause (for example, 'Radio Connection with UE lost' or 'unspecified'). For these type of causes MME typically preserves non-GBR bearer and deletes GBR bearers. As a result, GBR bearers (for example, QCI-1 bearer) is deleted by the MME.

After the RRC Connection is re-established, the Relay Node UE sends Service Request to the MME. The MME sends Initial Context Setup Request to macro eNB to set up the previously preserved non-GBR bearers. The MME does not re-establish the GBR bearer since it was not preserved. As a result, Relay Node UE does not have the GBR bearer until a full re-attach procedure occurs.

Since GBR bearer is not re-established, the GBR traffic is carried over the default non-GBR bearer and the voice performance is degraded.

Using this feature SAEGW is able to re-establish the previously deleted GBR bearer when MME sends the Modify Bearer Request to re-establish the preserved the non-GBR bearers.

How it Works

SAEGW re-establishes the previously deleted GBR bearer when MME sends the Modify Bearer Request, to re-establish the preserved non-GBR bearers.

This is achieved in SAEGW using two different mechanisms:

- Forwarding the Modify Bearer Request from SGW to P-GW
- P-GW to invoke local policy with a new event restore-bearers

Enabling Modify Bearer Request Forward from S-GW to P-GW

Use the following configuraion to enable forced forwarding of Modify Bearer Request from S-GW to P-GW:

```
configure
  context context_name
    sgw-service service_name
      enable-bearer-restore
      end
```

In S-GW service, whenever **enable-bearer-restore** option is set, modify bearer request is forwarded by S-GW to P-GW. It happens when the S-GW service is under SAEGW service.

For example:

```
config
   context ingress
     sgw-service sgw-service
        enable-bearer-restore
```



Note

- Without this CLI, S-GW only forwards the Modify Bearer Request message to P-GW if certain conditions are met. For example. RAT change, TimeZone change, ULI change, Handover indication flag, and so on as per 3GPP specifications.
- To avoid forwarding Modify Bearer Requests unnecessarily to P-GW, **enable-bearer-restore** should only be used when local policy is configured for **restore-bearer** event as described in next section.

P-GW Invokes Local Policy with New Event Restore-Bearers

A list of events supported under `eventbase` is enhanced with `restore-bearers`. This event is invoked when P-GW gets a Modify Bearer Request from S-GW. If local policy configuration has the **restore-bearer** event under **eventbase** then corresponding rules are applied.

Use the following configuration to re-establish missing bearers under local policy:

```
configure
   local-policy-service local_policy_name
      eventbase eventbase_name
         [ no ] rule priority integer
            event restore-bearers ruledef ruledef_name actiondef actiondef_name
            end
```

Following is an example for local policy configuration:

```
  local-policy-service local_policy
    ruledef apn_apn2
      condition priority 100 apn match apn2.com
    #exit

ruledef apn_apn1
      condition priority 100 apn match apn1.com
    #exit

    ruledef ded_bearer_creation_fail
      condition priority 100 apn match apn2.com
      condition priority 200 cause-code match 72 73 90 100 110
    #exit

    actiondef apn2_newcall
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit

    actiondef apn2_restore_bearer_config
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
```

```
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit

    actiondef apn2_retry_dedicated_bearer
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
      action priority 700 retry-count 4
      action priority 2000 allow-session
    #exit

actiondef apn1_newcall
      action priority 100 allow-session
    #exit

eventbase default
      rule priority 100 event new-call ruledef apn_apn1 actiondef apn1_newcall
      rule priority 200 event new-call ruledef apn_apn2 actiondef apn2_newcall
     rule priority 400 event rule-report-status ruledef ded_bearer_creation_fail actiondef
 apn2_retry_dedicated_bearer
      rule priority 600 event restore-bearers ruledef apn_apn2 actiondef
apn2_restore_bearer_config
    #exit
```

The key point in the above configuration is that both "new-call" and "restore-bearers" events, the actiondefs comprise of same actions. As a result, any missing bearer (such as a QCI-1 GBR bearer) is established.

At the time of "new-call" event, both QCI-1 (GBR) and QCI-5 (non-GBR) bearers are created. At the time of "restore-bearer" event, local policy will return actions to create both QCI-1 and QCI-5 bearers but since QCI-5 bearer already exists (as it was preserved), only QCI-1 bearer is established.

Show Commands and Outputs

show saegw-service statistics all

The output of this command displays the number of times SGW forwards modify bearer request to PGW due to flag enable-bearer-restore:

The output of this command includes the following fields:

MBR:— Displays the Dynamic User Plane Selection Statistics:

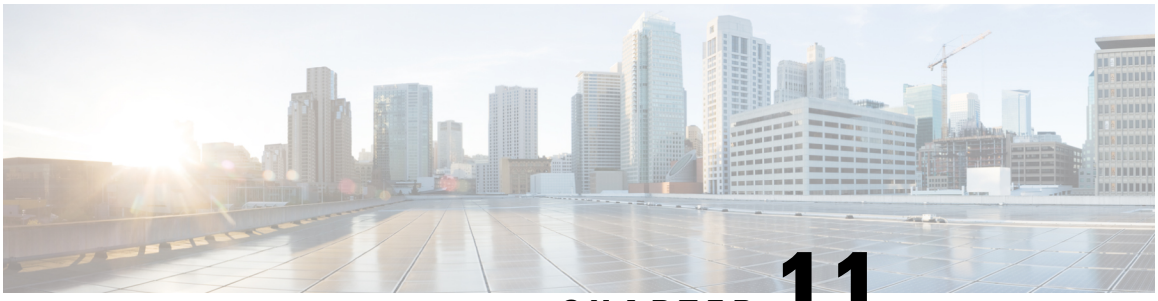
- Attempted — Displays the number of modify bearer request attempts between S-GW and P-GW due to flag enable bearers restore.
- Successful— Displays the total number of succesful modify bearer request between S-GW and P-GW due to flag enable bearers restore.
- Failure — Displays the total number of failure modify bearer request between S-GW and P-GW due to flag enable bearers restore.
- Mismatch DNS response — Displays mismatch DNS repsonse between S-GW and P-GW due to flag enable bearers restore.
- Negative DNS response — Displays negative DNS repsonse between S-GW and P-GW due to flag enable bearers restore.
- DNS timed out —Displays DNS timed out between S-GW and P-GW due to flag enable bearers restore.

show local-policy statistics all

The output of this command displays the list of events under event-base local-policy when S-GW sends modify bearer request to P-GW.

The output of this command includes the following fields:

Restore Bearers — Displays the restore-bearer enable and disable in local policy configuration.



CHAPTER 11

Bulk Statistics for Average Data Rate Per IP Pool

- Feature Summary and Revision History, on page 245
- Feature Description, on page 246
- Monitoring and Troubleshooting, on page 246

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*Statistics and Counters Reference*

Revision History

Revision Details	Release
The number of IP pool groups is increased from 2000 to 5000.	21.26
First introduced.	21.3

Feature Description

The bulk statistics support is enhanced to fetch the subscriber average data rate per IP pool (cumulative of all session managers). The average data rate consists of all the IP pools configured in the system.

The bulk statistics collection time is enhanced for the datarate-ippool schema. This schema supports up to 5000 IP pool groups when configured.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands and bulk statistics available in support of this feature.

Bulk Statistics

This feature supports the following bulk statistics:

Datarate-IPPool Schema

The following bulk statistics are added to the Datarate-IPPool schema:

- sess-datarate-ippool-name—Indicates the name of the IP pool for which average data rates are fetched.
- sess-ave-rate-fuser-bps—Indicates the average data-rate (bits/sec) from the user in uplink direction per IP pool basis.
- sess-ave-rate-tuser-bps—Indicates the average data-rate (bits/sec) to the user in downlink direction per IP pool basis.
- sess-ave-rate-fuser-pps—Indicates the average packets/second from the user in uplink direction per IP pool basis.
- sess-ave-rate-tuser-pps—Indicates the average packets/second to the user in downlink direction per IP pool basis.

Show Commands and/or Outputs

This section provides information regarding show commands and their outputs for this feature.

show bulkstats schema

Table 29: show bulkstats schema Command Output Descriptions

Field	Description
Bulk Statistics Server Configuration:	
Server State	Indicates the server state—enabled or disabled.
File Limit	Indicates the file size limit in KB.

Field	Description
Sample Interval	Indicates the sampling interval.
Transfer Interval	Indicates the transfer interval.
Receiver Mode	Indicates the receiver mode.
Local File Storage	Indicates the local file storage.
Bulk Statistics Server Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last collection time required	Indicates the last collection time required.
Last transfer time required	Indicates the last transfer time required.
Fine n	
Remote File Format	The remote file format—for example, %date%-%time%
File Header	The file's header.
File Footer	The file's footer.
File Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmissions.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.

Field	Description
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.

show bulkstats data

Table 30: show bulkstats data Command Output Descriptions

Field	Description
Bulk Statistics Server Configuration:	
Server State	Indicates the server state—enabled or disabled.
File Limit	Indicates the file size limit in KB.
Sample Interval	Indicates the sampling interval.
Transfer Interval	Indicates the transfer interval.
Receiver Mode	Indicates the receiver mode.
Local File Storage	Indicates the local file storage.
Historical Data Collection	Indicates the Historical Data Collection state—enabled or disabled.
Bulk Statistics Server Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last collection time required	Indicates the last collection time required.
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.

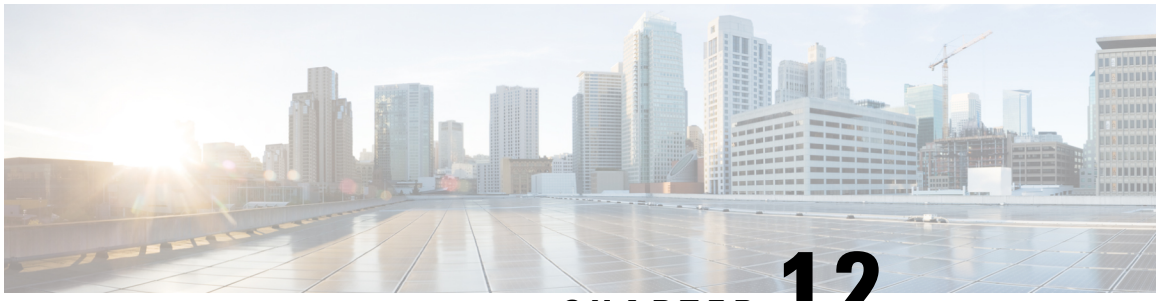
Field	Description
Fine n	
Remote File Format	The remote file format—for example, %date%-%time%
File Header	The file's header.
File Footer	The file's footer.
No bulkstats receivers	Indicates the total number of bulk statistics collection servers configured.
File Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.
Handoff Statistics	
epdg-handoff-disc	Configures LTE to Wi-Fi HO disconnect reason statistics.
show epdg-service statistics handoff-disc-reasons	Displays the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.
clear epdg-service statistics handoff-disc-reasons	Removes the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.

show subscribers data-rate ip-pool <pool_name>

Table 31: show subscribers data-rate ip-pool <pool_name> Command Output Descriptions

Field	Description
pk rate from user (bps)	The peak data rate, in bits per second, obtained for data sent from the subscriber to the network during the last sampling period.

Field	Description
peak rate to user (bps)	The peak data rate, in bits per second, obtained for data received from the network by the subscriber during the last sampling period.
ave rate from user (bps)	The average data rate, in bits per second, obtained for data sent from the subscriber to the network during the last sampling period.
ave rate to user (bps)	The average data rate, in bits per second, obtained for data received from the network by the subscriber during the last sampling period.
sust rate from user (pps)	The mean data rate, in packets per second, obtained for data sent from the subscriber to the network during the last three sampling periods.
sust rate to user(pps)	The mean data rate, in packets per second, obtained for data received from the network by the subscriber during the last three sampling periods.



CHAPTER 12

Bulkstats for GTP-C Messages by ARP Value

This chapter describes StarOS support for the Bulkstats for GTP-C Messages by ARP Value feature on the P-GW, SAE-GW, and S-GW.

- Feature Description, on page 251
- Performance Indicator Changes, on page 252

Feature Description

To comply with the "Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority" to support emergency calls over Voice over LTE (VoLTE), several Key Performance Indicators (KPIs) have been introduced with this feature. This feature is utilized to collect statistics for total number of GTP-C messages received for Enhanced Multimedia Priority Service (eMPS) session for specified interval (in minutes). The list of GTP-C messages are defined in accordance with the GIR document. As part of this feature:

- The S-GW will generate peg counts of the total number of received GTP-C messages containing an Allocation and Retention Priority (ARP), chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW level.
- The P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the specific P-GW level.
- The peg counts for GTP-C messages are broken down by message type similar to existing GTP-C message counters. The bulkstats are broken down by applicable S-GW and P-GW service and S5, S8, S11, and S4 interfaces.

Bulkstats are added for eMPS session/message.

Piggy-back Message

For piggy-back messages, if either of the messages have matching ARP or result into converting non-eMPS session to eMPS session, then both messages are counted as eMPS message and corresponding statistics for both messages are incremented.

If Modify Bearer Request is piggy-backed with Create Bearer Response on S11 interface of S-GW and Create Bearer Response result into converting non-eMPS session into eMPS session, then Modify Bearer Response statistics will not increment for this Modify Bearer Request.

Bulkstats Collection and Reset

Bulkstats are added under eGTP-C Schema and pgw-egtpc-s5s8 Schema. These eMPS bulkstats in eGTP-C Schema and pgw-egtpc-s5s8 Schema holds value only for a bulkstat interval, that is, value of these bulkstats shows number of eMPS messages exchanged during the bulkstat interval.

Limitations

This section identifies the known limitations of the feature:

- Peer level and APN level statistics are not collected.
- MPS statistics recovery is not supported.
- MPS statistics are not collected for CSReq, DDNReq, and change notification messages rejected by demux with ARP for eMPS sessions.
- MPS statistics are not collected for retried/re-transmitted messages.

Licensing



Important Bulkstats for GTP-C Messages by ARP Value feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Performance Indicator Changes

S-GW Ingress S4 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S4 interface of S-GW Ingress:

- **show egtpc statistics interface sgw-ingress interface-type s4**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s4**: Displays interface level GTP-C message statistics for S4 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s4**
  - **s4**: Interface type S4 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as

bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.

- **Create Session Request (Total RX)**: This counter will be incremented by S-GW when it receives Create session request message on S4 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create session response message on S4 interface containing an ARP value configured in MPS Profile.

S-GW Ingress S11 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S11 interface of S-GW Ingress:

- **show egtpc statistics interface sgw-ingress interface-type s11**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s11**: Displays interface level GTP-C message statistics for S11 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s11**
  - **s11**: Interface type S11 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total RX)**: This counter will be incremented by S-GW when it receives Create session request message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create session response message on S11 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Modify Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Modify Bearer response message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Create Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Create Bearer response message on S11 interface containing an ARP value configured in MPS Profile.
- **Downlink Data Notification (Total TX)**: This counter will be incremented by S-GW when it transmits Downlink Data Notification message on S11 interface containing an ARP value configured in MPS Profile.

- **Downlink Data Notification Ack (Total RX)**: This counter will be incremented by S-GW when it receives Downlink Data Notification Ack message on S11 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Update Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Update Bearer response message on S11 interface containing an ARP value configured in MPS Profile.

S-GW Egress GTP-based S5/S8 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S5/S8 interface of S-GW Egress:

- **show egtpc statistics interface sgw-egress interface-type s5s8**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s5s8**: Displays interface level GTP-C message statistics for S5/S8 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type sgw-s5s8**
  - **sgw-s5s8**: Interface type S5/S8 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total TX)**: This counter will be incremented by S-GW when it transmits Create session request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total RX)**: This counter will be incremented by S-GW when it receives Create session response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Modify Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Modify Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Create Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Update Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.

- **Update Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Update Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.

P-GW Ingress GTP-based S5/S8 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S5/S8 interface of P-GW Ingress:

- **show egtpc statistics interface pgw-ingress interface-type s5s8**
- **show egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface-type s5s8**
  - **s5s8**: Interface type S5/S8 for P-GW eGTP-C interface.

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total RX)**: This counter will be incremented by P-GW when it receives Create session request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by P-GW when it transmits Create session response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total RX)**: This counter will be incremented by P-GW when it receives Modify Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total TX)**: This counter will be incremented by P-GW when it transmits Modify Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total TX)**: This counter will be incremented by P-GW when it receives Create Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total RX)**: This counter will be incremented by P-GW when it receives Create Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total TX)**: This counter will be incremented by P-GW when it transmits Update Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Response (Total RX)**: This counter will be incremented by P-GW when it receives Update Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.

clear egtpc

The following CLI commands are modified to clear eMPS statistics at interface level and eGTP-C service level:

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**: Clears interface statistics along with eMPS statistics for all eGTP-C services of P-GW Ingress type and S5/S8 interface.
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s4 | s11 | sgw-s5s8]**: Clears interface statistics along with eMPS statistics for all eGTP-C services of S-GW Ingress type and S4 or S11 interface/S-GW Egress type and S5/S8 interface.
- **clear egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface [s5s8]**: Clears interface statistics along with eMPS statistics for all P-GW eGTP-C services and S5/S8 interface.
- **clear egtpc statistics egtp-service** *sgw_egptc_service_name* **interface [s11 | s4 | sgw-s5s8]**: Clears interface statistics along with eMPS statistics for all S-GW eGTP-C services and S4 or S11 or S5/S8 interface.

P-GW eGTP-C S5/S8 Schema

The following new bulk statistics variables are added to the P-GW eGTP-C S5/S8 schema in support of this feature:

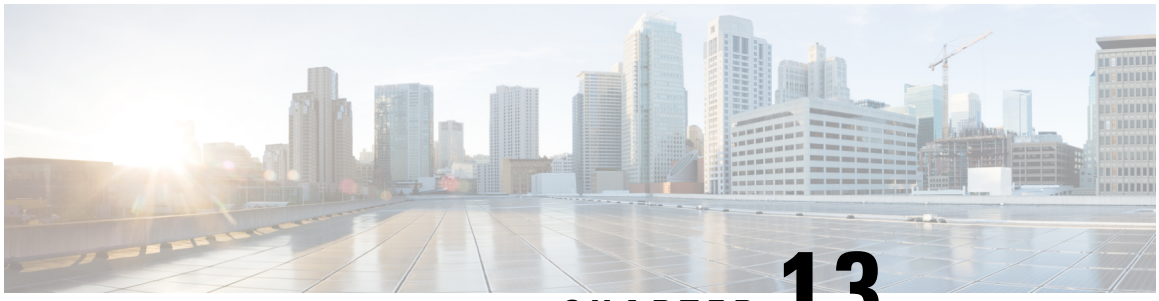
- tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-modbearerreq-emps – The total number of tunnel - modify bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-modbearerresp-emps – The total number of tunnel - modify bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-crebearerreq-emps – The total number of tunnel - create bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-crebearerresp-emps – The total number of tunnel - create bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-updbearerreq-emps – The total number of tunnel - update bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-updbearerresp-emps – The total number of tunnel - update bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.

eGTP-C Schema

The following new bulk statistics variables are added to the eGTP-C schema in support of this feature:

- s11-tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.

- s11-tun-recv-modbearerreq-emps – The total number of tunnel - modify bearer request - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-modbearerresp-emps – The total number of tunnel - modify bearer response - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-crebearerreq-emps – The total number of tunnel - create bearer request - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-crebearerresp-emps – The total number of tunnel - create bearer response - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-updbearerreq-emps – The total number of tunnel - update bearer request - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-updbearerresp-emps – The total number of tunnel - update bearer response - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-ddnreq-emps – The total number of downlink data notification - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-ddnack-emps – The total number of downlink data notificatino acknowledge - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s4-tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s4. This stat is for current bulkstat interval only.
- s4-tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s4. This stat is for current bulkstat interval only.
- tun-sent-cresessreq-emps – The total number of tunnel - create session request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-cresessresp-emps – The total number of tunnel - create session response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-modbearerreq-emps – The total number of tunnel - modify bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-modbearerresp-emps – The total number of tunnel - modify bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-crebearerreq-emps – The total number of tunnel - create bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-crebearerresp-emps – The total number of tunnel - create bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-updbearerreq-emps – The total number of tunnel - update bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-updbearerresp-emps – The total number of tunnel - update bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.



CHAPTER 13

Capability to Record and Produce Call Transactions

- Feature Summary and Revision History, on page 259
- Feature Description , on page 260
- How It Works, on page 260
- Configuring RTT, on page 302
- Monitoring and Troubleshooting, on page 303

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• ePDG • P-GW • SaMOG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *P-GW Administration Guide* • *SaMOG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
P-GW and SaMOG supports capability to record and produce historic call transactions feature. Additional RTT record schemas have been added.	21.27
Added RTT Record Schema	21.26
First introduced.	20.0

Feature Description

Regions and Network Operations Center (NOC) uses Real Time Tool (RTT) to debug network issues and to understand user behavior. All call transactions in ePDG, P-GW, and SaMOG gets generated in RTT files. ePDG, P-GW, and SaMOG transfer RTT files to the external server through SSH File Transfer Protocol (SFTP). The comma-separated values (.CSV) format RTT files get transferred either in compressed or non-compressed format. Transfer happens based on the configuration to the external servers such as servers in the customer network either directly or through the Cisco Collector server.

Note RTT Record Schema and its procedure numbers are generalized for Gateway RTT. Contact your Cisco account representative for detailed information on the specific RTT Record Schema.

How It Works

This section describes the RTT procedures and schema.

RTT Procedures

The following table lists the RTT procedures that are specific to ePDG, P-GW and SaMOG:

Procedure Number	Procedure Name	Applicability
1	S5/S8/S2b GTP Create Session	P-GW, ePDG, SaMOG
2	S5/S8/S2b GTP Create Bearer	P-GW, ePDG, SaMOG
3	S5/S8/S2b GTP Delete Session	P-GW, ePDG, SaMOG
4	S5/S8/S2b GTP Delete Bearer	P-GW, ePDG, SaMOG
5	GTP Modify Bearer	P-GW
6	S5/S8/S2b GTP Update Bearer	P-GW, ePDG, SaMOG

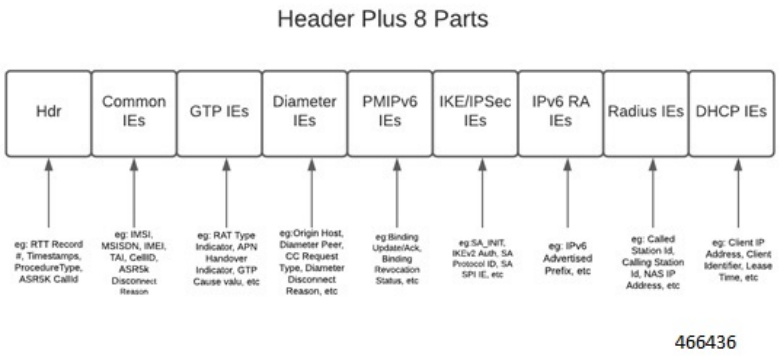
Procedure Number	Procedure Name	Applicability
7	S6b/SWm – Diameter AAR/ AAA	P-GW, ePDG, SaMOG
8	S6b/SWm – Diameter RAR/RAA	P-GW, ePDG, SaMOG
9	S6b/SWm – Diameter Session Termination	P-GW, ePDG, SaMOG
10	S6b/SWm – Abort Session	P-GW, ePDG, SaMOG
11	Diameter Gx – CCR-I/CCA-I	P-GW
12	Diameter Gx – CCR-U/CCA-U	P-GW
13	Diameter Gx – CCR-T/CCA-T	P-GW
14	Diameter Gx – RAR/RAA	P-GW
15	Diameter Gy – CCR-I/CCA-I	P-GW
16	Diameter Gy – CCR-U/CCA-U	P-GW
17	Diameter Gy – CCR-T/CCA-T	P-GW
18	Diameter Gy – RAR/RAA	P-GW
19	PMIPv6 S2a – Binding Update/Acknowledgement	P-GW
20	PMIPv6 S2a Revocation Update/Acknowledgement	P-GW
21	SWu – IKEv2 SA INIT/Resp	ePDG
22	SWu – IKEv2 Auth Req/Resp	ePDG
23	SWu – IKEv2 Information Req/Resp	ePDG
24	SWm – Diameter EAP Request/Answer	ePDG, SaMOG
25	ePDG Router Advertisement	ePDG, SaMOG
26	SWu – CREATE_CHILD_SA Req/Resp	ePDG
27	Radius – WLC-SaMOG Access Request/Challenge	SaMOG
28	Radius – WLC-SaMOG Access Request/Accept	SaMOG
29	Radius – WLC-SaMOG Disconnect Request/Response	SaMOG
30	Radius – WLC-SaMOG Accounting Request/Response	SaMOG
31	Radius – SaMOG-Radius Server Accounting Req/Res	SaMOG
32	WLC – SaMOG DHCP Discover/Offer	SaMOG
33	WLC – SaMOG DHCP Request/Ack/Nak	SaMOG

Procedure Number	Procedure Name	Applicability
34	WLC – SaMOG DHCP Release/Ack/Nak	SaMOG

RTT Record Schema

The following figure details the RTT schema for ePDG, P-GW and SaMOG. The first six IEs, Common IEs to IPv6RA IEs are common for ePDG, P-GW and SaMOG. The last two fields, Radius IEs and DHCP IEs are speicific to SaMOG.

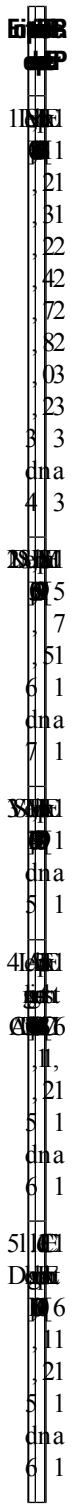
Figure 13: RTT Record Schema



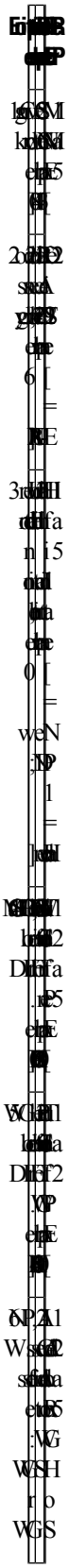
RTT schema has a Header followed by eight blocks of Information Elements (IEs). There are 220 IEs that are grouped into 8 blocks. Schemas 1 to 170 are specific to ePDG. Schemas 1 to 170 + 10 (180) CUPS schemas are specific to P-GW and schemas 171 to 220 are specific to SaMOG. For more information on CUPS schemas, refer to the *Ultra Packet Core CUPS User Plane Administration Guide*. Contact your Cisco account representative for the complete list of RTT Record Schema IEs.

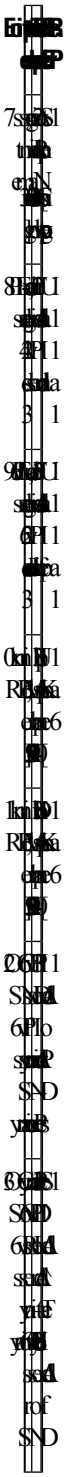
The following table lists the RTT Record schemas:













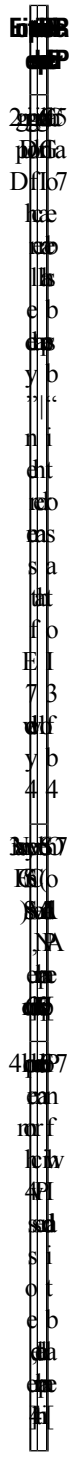










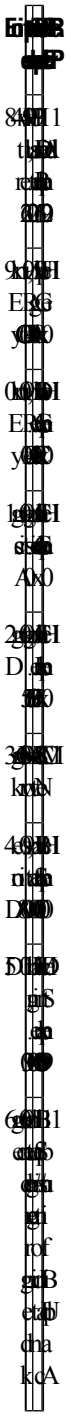


































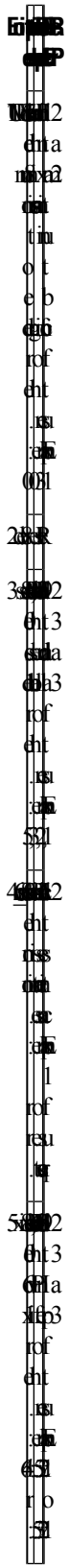


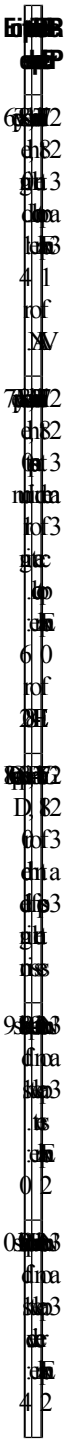




















Note Schemas 1 to 170 are speicific to ePDG. Schemas 1 to 170 + 10 Cups schemas are specific to PGW and schemas 171 to 220 are specific to SaMOG.

Configuring RTT

This section provides RTT configuration information for ePDG, P-GW and SaMOG.

Configuring RTT to Record and Produce Call Transactions

Use the following configuration to enable RTT to record and produce call transactions.

```
configure
   context context_name
      [ epdg-service | pgw-service | samog-service ] service_name
         [ no ] reporting-action event-record
end
```

NOTES:

- **reporting-action event-record**: Enables event reporting through RTT.
- **no**: Disables event reporting through RTT.

Configuring RTT under Session Event Module

Use the following configuration to configure the RTT feature in ePDG, P-GW and SaMOG.

```
configure
   context context_name
      session-event-module
         event transfer-mode push primary url URL_addressfile name file_name |
 rotation volume volume_size | rotation time rotation_time | compression
compression_type | extension extension_type
         event use-harddisk
         event remove-file-after-transfer
         event push-interval interval_time
      end
```

NOTES:

- **transfer-mode**: Enables the transfer mode in RTT.
- **push primary url***URL_address*: Specifies the external server location where the records are transferred.
- **file name** *file_name*: Specifies the RTT file name where the records are stored. *file_name* can be an alphanumeric string of size 1 to 31.
- **rotation volume** *volume_size*: The volume based on which the RTT file is generated. Enter an integer from 51200 to 62914560.
- **rotation time** *rotation_time*: The time based on which the RTT file is generated. Enter an integer from 30 to 86400 seconds.

Note RTT files are internally generated, based on the rotation volume or rotation time.

- **compression**: Specifies the file compression type. If enabled, the RTT file is generated as a Gzip file, else it is generated as a normal file.
- **extension***extension_type*: Specifies the RTT file extension (.csv).
- **event use-harddisk**: Specifies hard disk as the storage space for the RTT file generation.
- **event remove-file-after-transfer**: Specifies RTT files to be removed after pushing the files to the external server.
- **event push-interval**: Specifies the push interval time at which the RTT files are transferred to the external server.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands to support this feature.

Show Commands and Output

This section provides information regarding show commands and their outputs for this feature.

show samog-service name

Table 32: show samog-service name Command Output Descriptions

Field	Description
Reporting Action	
Event Record	Indicates if RTT feature is enabled or not.

show event-record statistics

Table 33: show event-record statistics Command Output Descriptions

Field	Description
Total Number of Event Records	The total number of event records (GTPv2 + Diameter + IKE + RA + Radius + DHCP).
GTPv2 Event Records	The total number of GTPv2 records
CSR	The total number of CSR (Create Session Request) events.
CBR	The total number of CBR (Create Bearer Request) events.

Field	Description
DSR	The total number of DSR (Delete Session Request) events.
DBR	The total number of DBR (Delete Bearer Request) events.
UBR	The total number of UBR (Update Bearer Request) events.
IPV6 RA Event Records	The total number of IPV6 RA event records.
RA Prefix	The total number of RA prefix events.
Diameter Event Records	The total number of Diameter event records (S6b + SWm + STa + Gx + Gy).
ePDG Events	
IKEv2 Event Records	The total number of IKE events.
IKE_SA_INIT	The total number of IKE_SA_INIT events.
IKE_AUTH	The total number of IKE_AUTH events.
IKE_INFORMATION	The total number of IKE_INFORMATION events.
CREATE_CHILD_SA	The total number of CREATE_CHILD_SA events.
SaMOG Events	
Radius Auth Event Records	The total number of Radius authentication event records.
Access Req/Challenge	The total number of Radius Authentication access request challenge event records.
Access Req/Accept	The total number of Radius Authentication access request accept event records.
Disconnect Req	The total number of Radius Authentication disconnect request event records.
Radius Accounting Event Records	The total number of Radius accounting event records.
Accounting Req from WLC	The total number of Radius accounting event records from WLC.
Accounting Req to Radius Server	The total number of Radius accounting event records to the Radius server.
STa Procedures	The total number of STa interface specific events.
AAR	The total number AAR (AA-Request) events.
RAR	The total number of RAR (Re-Auth-Request) events.
ASR	The total number of ASR (Abort Session Request) events.
STR	The total number of STR (Session Termination Request) events.

Field	Description
DER	The total number of DER (DE-Request) events.
DHCP Event Records	The total number of DHCP event records.
Discover/Offer	The total number of DHCPv4 discovery offer event records.
Release/Ack	The total number of DHCPv4 release ack event records.
Request/Ack	The total number of DHCPv4 request ack event records.

Bulk Statistics

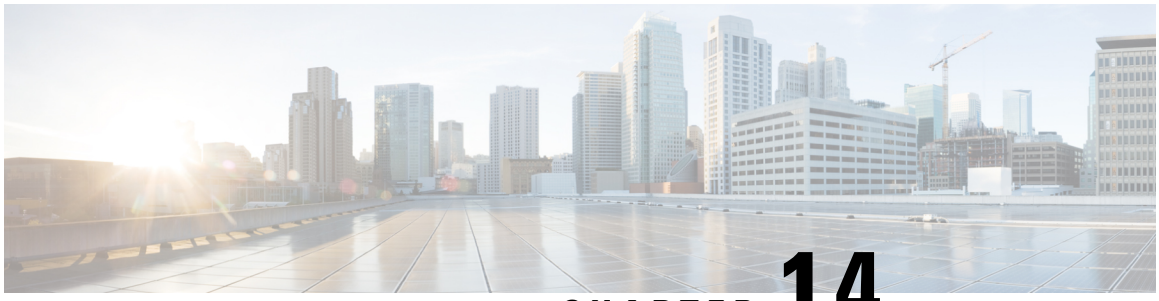
The following bulk statistics are added to the SaMOG schema as part of this feature:

SaMOG Schema

Table 34: Bulk Statistics Varibales in the SaMOG Schema

Variables	Description
sess-samog-total-number-event-records	The total number of SaMOG session event records.
sess-samog-total-s2a-event-records	The total number of SaMOG S2a event records.
sess-samog-total-csr-event-records	The total number of SaMOG CSR event records.
sess-samog-total-cbr-event-records	The total number of SaMOG CBR event records.
sess-samog-total-dsr-event-records	The total number of SaMOG DSR event records.
sess-samog-total-dbr-event-records	The total number of SaMOG DBR event records.
sess-samog-total-ubr-event-records	The total number of SaMOG UBR event records.
sess-samog-total-ipv6-ra-event-records	The total number of SaMOG IPv6 RA event records.
sess-samog-total-ra-prefix-event-records	The total number of SaMOG RA prefix event records.
sess-samog-total-dhcpv4-event-records	The total number of SaMOG DHCPv4 event records.
sess-samog-total-dhcpv4-disc-offer-event-records	The total number of SaMOG DHCPv4 discovery offer event records.
sess-samog-total-dhcpv4-req-ack-event-records	The total number of SaMOG DHCPv4 request acknowledgement event records.
sess-samog-total-dhcpv4-rel-ack-event-records	The total number of SaMOG DHCPv4 release acknowledgement event records.
sess-samog-total-rad-auth-event-records	The total number of SaMOG Radius Authentication event records.

Variables	Description
sess-samog-total-rad-auth-acc-req-chal-event-records	The total number of SaMOG Radius Authentication access request challenge event records.
sess-samog-total-rad-auth-acc-req-acpt-event-records	The total number of SaMOG Radius Authentication access request accepted event records.
sess-samog-total-rad-auth-disc-req-event-records	The total of number SaMOG Radius Authentication disconnect request event records.
sess-samog-total-rad-acct-event-records	The total number of SaMOG Radius Accounting event records.
sess-samog-total-rad-acct-wlc-event-records	The total number of SaMOG Radius Accounting event records from Wireless LAN Controller.
aaa-samog-total-rad-acct-aaa-event-records	The total number of SaMOG Radius Accounting event records to AAA.
aaa-samog-total-sta-event-records	The total number of SaMOG STa event records.
aaa-samog-total-sta-aar-event-records	The total number of SaMOG STa AAR event records.
aaa-samog-total-sta-der-event-records	The total number of SaMOG STa DER event records.
aaa-samog-total-sta-asr-event-records	The total number of SaMOG STa ASR event records.
aaa-samog-total-sta-rar-event-records	The total number of SaMOG STa RAR event records.
aaa-samog-total-sta-str-event-records	The total number of SaMOG STa STR event records.



CHAPTER 14

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

- Feature Summary and Revision History, on page 307
- Overview, on page 309
- How Cisco Ultra Traffic Optimization Works, on page 309
- Configuring Cisco Ultra Traffic Optimization, on page 339
- Monitoring and Troubleshooting, on page 344

Feature Summary and Revision History

Summary Data

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

Revision History



Important Revision history details are not provided for features introduced before release 21.2 and N5.1.

Revision Details	Release
In this release, P-GW supports Cisco Ultra Traffic Optimization show commands and outputs are enhanced to show Rx/Tx packets statistics for Uplink and Downlink for UDP and TCP split.	21.23
In this release, Cisco Ultra Traffic Optimization P-GW supports high throughput (4G or 5G) optimization of the traffic.	21.22
In this release, P-GW supports MBR/GBR handling in optimization library.	21.21
In this release, ranges of configurable policy parameters for Cisco Ultra Traffic Optimization are modified.	21.20.4
In this release the following three new parameters are added in Large TODR: **1.** International Mobile Subscriber Identity (IMSI) **2.** Flow-ID and Flow-ID list **3.** User Location Information (ULI) For more information, refer the *Large TODR Enhancement* section.	21.19.1
The Cisco Ultra Traffic Optimization library version has been upgraded from 3.0.9 to 3.0.11.	21.14.2
With this release, new keywords **large-flows-only** and **managed-large-flows-only** are implemented as part of the **data-record** command to enable the CUTO library to stream respective statistics to the external server. New bulk statistics are added in support of this enhancement	21.14
With this release, Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.3.17
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.3.x
Multi-Policy support for Cisco Ultra Traffic Optimization solution.	21.6
Cisco Ultra Traffic Optimization solution is supported in Ultra Gateway Platform (UGP).	21.6
Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.5
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.5
First introduced.	21.2

Overview

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

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

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

How Cisco Ultra Traffic Optimization Works

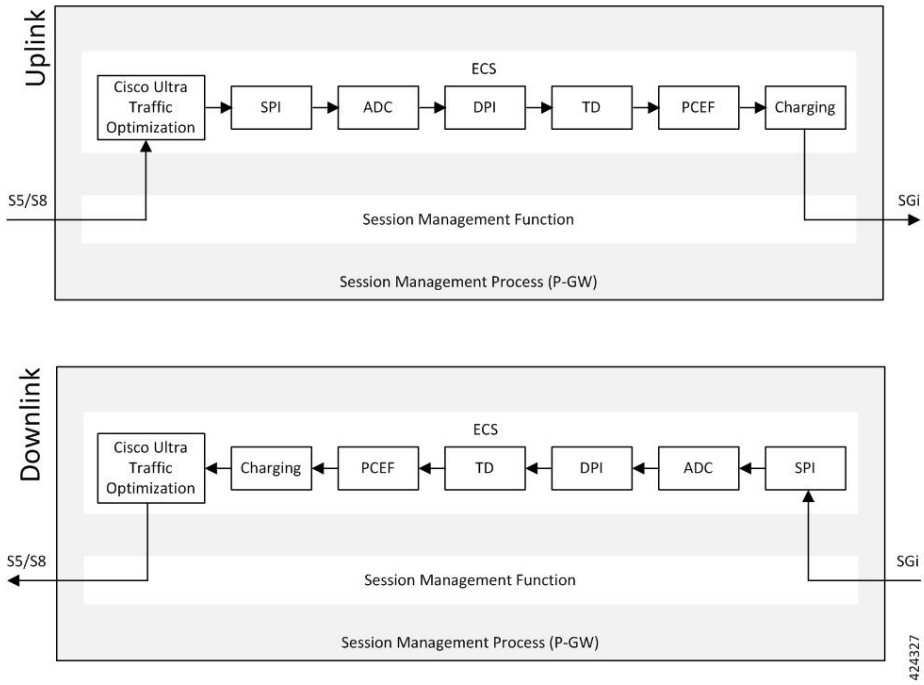
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested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

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

Architecture

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

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



Licensing

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

Limitations and Restrictions

- The values which the P-GW chooses to send to the Cisco Ultra Traffic Optimization engine are the values associated from the bearer GBR and bearer MBR.
- In the current implementation, only downlink GBR and MBR are sent to the engine for traffic optimization.
- UDP/QUIC based Traffic Optimization is supported only on PORT 443.
- The traffic-optimization data-records are generated in the same folder as that of EDRs. Also, the file rotation criteria will be similar to that of EDRs.
- A povision to dynamically load the library without statically linking it is restricted.
- OP works on ‘per flow’ level GBR/MBR to optimize the flows However, P-GW supports only sending bearer level GBR/MBR.
- The sending GBR and MBR values to Optimation library functionality is applicable only for P-GW product.

Handling of Traffic Optimization Data Record

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

Large TODR Enhancement

In 21.19.1 and later releases, the following three new parameters are added in large TODR:

1. International Mobile Subscriber Identity (IMSI)
2. Flow-ID and Flow-ID list
3. User Location Information (ULI)

   The Flow-ID is used to correlate the ACS Flow ID that is visible in End Point Detection and Response ("sn-flow-id" attribute) and then the ULI is correlated with RAN counters.

Note These new fields are only available in Large TODRs generated on non-VPP based P-GW and SAEGW.

Enhancing Large TODR

Use the following configuration to enable enhanced large TODR.

```
configure
  active-charging service service_name
    traffic-optimization-profile
      data-record
        enhanced-large-todr [ imsi | acs-flow-id | uli ]
        end
```

Example 1: When all fields are to be displayed:

```
enhanced-large-todr
```

Example 2: When IMSI and ULI are to be displayed:

```
enhanced-large-todr imsi
enhanced-large-todr uli
```

Show Commands and Outputs

```
show active-charging traffic-optimization info
```

Output Example 1:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
```

```
                Enhanced Large TODR: DISABLED
[local]laas-setup#
```

Output Example 2 for IMSI and ULI:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: ENABLED, Fields: imsi uli
[local]laas-setup#
```

The output of this command includes the following fields:

- Enhanced Large TODR

Enhancement to the Existing Large TODRs

1. **Large TODRs with IMSI**

   IMSI: Indicates the International Mobile Subscriber Identity.

   IMSI value is 0 if it is a trusted build.

2. **ACS Flow ID**

   ACS Flow ID is a newly introduced field. As there could be a lot of flow, it is limited to a maximum of 20 flows as a part of TODR.

   acs_flow_id_count: Number of ACS Flow Ids present in this TODR. A Maximum of 20 ACS Flow IDs is present.

   acs_flow_id_list: List of individual ACS Flow Ids. For examples, acs_flow_id1, acs_flow_id2 and so on.

   a. **EDR ACS Flow ID**

      In EDR, each ACS flow ID is printed by enabling the attribute ‘sn-flow-id’ in EDR config as given below :

      ```
      config
      active-charging service ACS
          edr-format EDR_SN
          delimiter comma
            attribute sn-flow-id priority 10
            rule-variable bearer 3gpp imsi priority 15
            rule-variable bearer qci priority 20
      ```

      It is printed out in EDR in the following format **92:30278:14786055** where:

      - 92 is the Session Manager instance
      - 30278 is the Session Handle orsession number
      - 14786055 is the ACS flow identifier

   b. **TODR ACS Flow ID**

      TODR ACS flow idshould follow the same format as in EDR so customers can correlate TODRs with EDRs. Therefore, each flow ID in the list acs_flow_id_list that is acs_flow_id1, acs_flow_id2, and so on should get printed out in TODR as `smgr instance:session handle: flow id`.

An example is **92:30278:14786055** where:

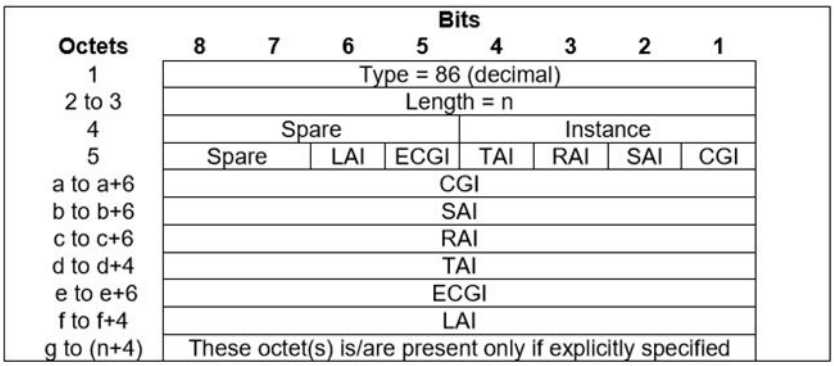
- 92 is the Session Manager instance
- 30278 is the Session Handle orsession number
- 14786055 is the ACS flow identifier

3. **ULI**

Even though the original requirment was to print ECGI, it does not cover all the scenarios. For example, when PGW is the anchor for a call that moves from 4G to 3G, ECGI does not make sense as the ULI (User Location Information) indicates CGI rather than ECGI as the user is now in 3G. Normally, MME informs PGW through SGW of the changes happened in ULI. This feature supports ULI that is s superset of ECGI.

The new field is called ULI. However, ULI is a complex IE composed of multiple identifiers and of variable length. For more details, refer the 3GPP TS 29.274.

Figure 14: User Location Information (ULI)



An ULI can be composed of one or more identifiers For example, there could be TAI and ECGI both in the ULI. Supporting such identifiers is problematic since the total length of ULI goes beyond 8 bytes and on per packet level, and have to pass an byte array and that has performance implications. In order, to overcome this issuse, ULI is formed as a combined type (for example, TAI AND ECGI together), then alone the ECGI part is shown in TODRs. This is done to ensure that identifier portion of ULI is accommodated in `uint64_t` (8 bytes). Specifically,

a. If TAI and ECGI both are present as a combined type, then only ECGI is shown.

b. If CGI and RAI both are present as a combined type, then only CGI is shown.

c. If both SAI and RAI both are present as a combined type, then only RAI is shown .

Every TODR can have multiple phases with a granularity of 2 seconds. ULI is added to the list of Phase attributes:

a. *ULI*: Newly introduced field.

ULI Details

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULI Type: ULI Value

ULI Type can be any one of these:

- 1–CGI
- 2–SAI
- 4–RAI
- 8–TAI
- 16–ECGI

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULIType:ULIValue

An example is given below when ULI Type is ECGI:

16:0x21635401234567

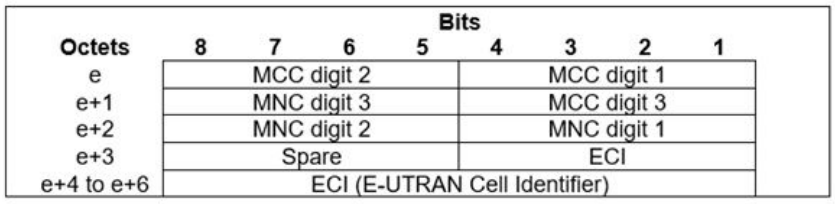
Here 16 represents that ULI Type is ECGI

0x21635401234567 is the hexadecimal representation of ECGI

MCC is '123' i.e. the three digits of MCC are '1', '2' and '3' MNC is '456', that is. the three digits of MNC are '4', '5' and '6'

ECI is '19088743' in decimal ('1234567' in hexadecimal)

Figure 15: ECGI Field



List of Attributes and File Format

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

Standard TODR

The following is the format of a Standard TODR:

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

Example:

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

Where:

- *instance_id*: Instance ID.

- *flow_type*: Standard flow (0)
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.

Large TODR

The following is a sample output of a Large TODR.

```
19,1,404005123456789,22.22.0.1,209.165.200.225.8,custom1,2,0,1588858362158,1588858952986,16420806,1588858364162,419,351,7000,0,0,1,
19:2:15,2,0,0,2,1,1,16:0x12546300012345,
1588858364162,80396,1472,0,0,0,2,1,16:0x12546300012345,1588858366171,146942,1937,7000,0,0,2
```

Where:

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

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

Sending GBR and MBR Values to Optimization Library

P-GW sends:

- GBR and MBR values based on the classification of traffic optimization selection
- Flow level GBR and MBR values to the optimization library
- Only downlink GBR and MBR to the optimization library

P-GW passes Zero GBR value for flows on a non-GBR bearer towards optimization library.

Optimatization library maintains logical flow based on Source IP, Destination IP, and Protocol IP (3-tuple). Whereas, P-GW provides GBR and MBR values based on Source IP, Destination IP, Source Port, Destination Port, and Protocol IP (5-tuple) to the optimization library. Because of these, multiple StarOS 5-tuple entries can belong to same 3-tuple entry in optimization library. Optimization library uses:

- Minimum of all MBR values that belong to the same 3-tuple entry as upper-limit.
- Maximum of all GBR values that belong to same 3-tuple entry as lower-limit.

High Throughput Traffic Optimization Support

Cisco Ultra Traffic Optimization feature is enhanced to support the subscribers through the optimization of traffic. With High Throughput Traffic Optimization Support feature, support is added for optimization of traffic for 5G subscribers (high throughput). The feature also allows automatic switching of traffic optimization parameters depending on throughput characteristics (which is in turn based on 4G or 5G).



Note This is a licensed feature. Contact your Cisco Account representative for detailed information on specific licensing requirements.

The existing Cisco Ultra Traffic Optimization single flow logic is enhanced to dynamically toggle between algorithms depending on the profile packet pattern real time (for example, 4G LTE vs 5G mm and wave traffic pattern).

Cisco Ultra Traffic Optimization library is updated to introduce two separate sets of policy parameters under a traffic optimization policy:

- Base policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects normal throughput (for example, 4G throughput). They are called 'Base' policy parameters. These parameters are the same as the parameters that existed before the High Throughput Traffic Optimization Support feature was introduced.
- Extended policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects high throughput for a flow (for example, 5G throughput). They are called ‘Extended’ policy parameters.

The two separate policy parameters under the same policy quickly switch from one set to the other without requiring any intervention from session managers when there is a change in throughput.

Hence, having two separate sets of policy parameters in the same policy helps meet the requirement that the Cisco Ultra Traffic Optimization algorithm automatically, dynamically, and immediately adjusts to the change in throughput. This change in throughput could be due to a change in RAN characteristics, for example, when UE enters a 5G or high speed 4G coverage area.

How High Throughput Optimization Support Works

Cisco Ultra Traffic Optimization algorithm monitors the traffic and automatically transitions between Base and Extended policy parameters based on the following logic:

1. Start with base policy.
2. If measurement phase burst rate > extended link profile initial-rate then move to the extended policy.

3. If measurement phase burst rate < base link profile max-rate then move to the base policy.
4. Repeat steps 2,3 for every measurement phase.

.

Multi-Policy Support for Traffic Optimization

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

This feature includes the following functionalities:

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

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

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

Important Location Change Trigger is not supported with IPSG.

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

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

How Multi-Policy Support Works

Policy Selection

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

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

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

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

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

Deleting a Policy

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

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

Configuring Multi-Policy Support

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

Configuring a Traffic Optimization Profile

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

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

NOTES:

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

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

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

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

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

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

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

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

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

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

Configuring a Traffic Optimization Policy

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

```
configure
   require active-charging
   active-charging service service_name[extended]
      [ no ] traffic-optimization-policy policy_name[extended]
        bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
```

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

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

[no] bandwidth-mgmt

[no] extended-bandwidth-mgmt

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

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

[no] curbing-control

[no] extended-curbing-control

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

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

[no] heavy-session

[no] extended-heavy-session

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

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

[no] link-profile

[no] extended-link-profile

session-params { tcp-ramp-up *tcp_rampup_duration* **[udp-ramp-up** *udp_rampup_duration* **] | udp-ramp-up** *udp_rampup_duration* **[tcp-ramp-up** *tcp_rampup_duration* **] }**

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

NOTES:

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

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

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

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

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

- **heavy-session**: Configures parameters for Base heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows.
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed..
- **extended-heavy-session**: Configures parameters for Extended heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows. .
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed.
- **link-profile**: Configures Base link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.
- **extended-link-profile**: Configures Extended link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.
- **session-params**: Configures Base session parameters.
  - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
  - **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..
- **extended-session-params**: Configures Extended session parameters.
  - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.

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



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

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

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

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

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

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

Traffic Optimization Policy - Default Values

```
Bandwidth-Mgmt:

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

Curbing-Control:

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

Heavy-Session:

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

Link-Profile:

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

Session-Params:

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

Associating a Trigger Action to a Traffic Optimization Policy

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

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

NOTES:

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

Enabling TCP and UDP

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

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

NOTES:

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



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

Service-Scheme Configuration for Multi-Policy Support

The service-schema framework enables traffic optimization at APN, rule base, QCI, and Rule level. In 21.6, with the Multi-Policy Support feature, traffic optimization in a service-schema framework allows the operator to configure multiple policies and to configure traffic optimization based on a desirable location.

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

Session Setup Trigger

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

Use the following configuration to setup a Session Trigger:

```
configure
    active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
trigger-action trigger_action_name
```

```
            exit
        subs-class sub_class_name
            apn = apn_name
            exit
        subscriber-base subscriber_base_name
           priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
            end
```

Sample Configuration

Following is a sample configuration for Session Setup Trigger:

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

Bearer Creation Trigger

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

Use the following configuration to configure a Bearer Creation Trigger:

```
configure
  active-charging service service_name
    service-scheme service_scheme_name
      trigger bearer-creation
        priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
        exit
      trigger-condition trigger_condition_name2
        qci = qci_value
        exit
      trigger-action bearer-creation
        traffic-optimization policy bearer-creation
        exit
```

Sample Configuration

The following is a sample configuration for Bearer Creation Trigger:

```
service-scheme SS1
     trigger bearer-creation
       priority 1 trigger-condition bearer-creation trigger-action bearer-creation
     #exit
   trigger-condition bearer-creation
     qci = 1 to 2
   #exit
   trigger-action bearer-creation
```

```
    traffic-optimization policy bearer-creation
  #exit
```

Flow Creation Trigger

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

Use the following configuration to configure a flow creation trigger:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
            ip-protocol = protocol_type
            rule-name = rule_name
               **Multi-line or All-lines**
            exit
```

Sample Configuration

The following is a sample configuration for Flow Creation Trigger using the default Cisco Ultra Traffic Optimization policy:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC5 trigger-action TA4
    #exit
    trigger-condition TC5
      ip protocol = tcp
      ip protocol = udp
      multi-line-or all-lines
    #exit
    trigger-action TA4
      traffic-optimization
    #exit
```

Configuring: ecgi-change

The following demonstrates ecgi-change sample configuration:

Trigger Condition and Trigger Action in ACS Configuration

```
configure
active-charging-service ACS
   trigger-action TA1
      traffic-optimization policy flow-create-ecgi-change
    #exit
    trigger-condition TC4
      local-policy-rule = ruledef-ecgi
    #exit
 end
```

Service Schema Configuration

```
configure
active-charging-service ACS
```

```
    service-scheme SS1
      trigger flow-create
        priority 2 trigger-condition TC4 trigger-action TA1
      #exit
    subs-class SC1
      any-match = TRUE
    #exit
    subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
    #exit
end
```

Local Policy Configuration

```
local-policy-service LP
    ruledef anymatch
      condition priority 1 imsi match *
    #exit
    ruledef ecgi-1
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AE7F0A 1AE7F0B 1AE7F28 1AE7F29
1AE7F46 1AE7F47 1AEAC00 1AEAC01 1AEAC02 1AEAC0A 1AEAC0B 1AEAC0C 1AEAC14 1AEAC15 1AEAC16
1AEAC28 1AEAC29 1AEAC2A 1AEAC46 1AEAC47 1AEAC48 1AEAC50 1AEAC51 1AEAC52 1AEAC6E 1AEAC6F
1AEAC70 1AEAC78 1AEAC79 1AEAC7A
    #exit
    ruledef ecgi-10
      condition priority 1 ecgi mcc 300 mnc 235 eci match 1F36C52 1F36C6E 1F36C6F 1F36C70
1F36C78 1F36C79 1F36C7A
    #exit
    ruledef ecgi-2
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBE01 1AEBE02 1AEBE0B 1AEBE0C
1AEBE15 1AEBE16 1AEBE29 1AEBE2A 1AEBE47 1AEBE48 1AEBF00 1AEBF01 1AEBF02 1AEBF0A 1AEBF0B
1AEBF0C 1AEBF14 1AEBF15 1AEBF16 1AEBF1E 1AEBF1F 1AEBF20 1AEBF28 1AEBF29 1AEBF2A 1AEBF46
    #exit
    ruledef ecgi-3
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBF47 1AEBF48 1AEBF50 1AEBF51
1AEBF52 1AEBF6E 1AEBF6F 1AEBF70 1AEBF78 1AEBF79 1AEBF7A 1AF0E00 1AF0E01 1AF0E02 1AF0E0A
1AF0E0B 1AF0E0C 1AF0E14 1AF0E15 1AF0E16 1AF0E28 1AF0E29 1AF0E2A 1AF0E46
    #exit
    ruledef ecgi-4
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF0E47 1AF0E48 1AF4A0A 1AF4A0B
1AF4A14 1AF4A15 1AF4A28 1AF4A29 1AF4A46 1AF4A47 1AF4D00 1AF4D01 1AF4D0A 1AF4D0B 1AF4D14
1AF4D15 1AF4D28 1AF4D29 1AF4D46 1AF4D47 1AF4D50 1AF4D51 1AF4D6E 1AF4D6F
    #exit
    ruledef ecgi-5
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF4D78 1AF4D79 1AF7200 1AF7201
1AF7202 1AF720A 1AF720B 1AF720C 1AF7214 1AF7215 1AF7216 1AF721E 1AF721F 1AF7444 1AF7228
1AF7229 1AF722A 1AF7246 1AF7247 1AF7248 1AF7250 1AF7251 1AF7252 1AF726E
    #exit
    ruledef ecgi-6
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF726F 1AF7270 1B04C00 1B04C01
1B04C02 1B04C03 1B04C0A 1B04C0B 1B04C0C 1B04C0D 1B04C14 1B04C15 1B04C16 1B04C17 1B04C1E
1B04C1F 1B04C20 1B04C21 1B04C28 1B04C29 1B04C2A 1B04C2B 1B04C46 1B04C47
    #exit
    ruledef ecgi-7
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B04C48 1B04C49 1B04C50 1B04C51
1B04C52 1B04C53 1B04C6E 1B04C6F 1B04C70 1B04C71 1B04C78 1B04C79 1B04C7A 1B04C7B 1B05300
1B05301 1B05302 1B0530A 1B0530B 1B0530C 1B05314 1B05315 1B05316 1B05328 1B05329
    #exit
    ruledef ecgi-8
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B0532A 1B05346 1B05347 1B05348
1B32F00 1B32F01 1B32F02 1B32F0A 1B32F0B 1B32F0C 1B32F14 1B32F15 1B32F16 1B32F28 1B32F29
1B32F2A 1B32F46 1B32F47 1B32F48 1B76400 1B76401 1B76402 1B7640A 1B7640B 1B7640C 1B76428
    #exit
    ruledef ecgi-9
```

```
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B76429 1B7642A 1B76446 1B76447
1B76448 1F36C00 1F36C01 1F36C02 1F36C0A 1F36C0B 1F36C0C 1F36C14 1F36C15 1F36C16 1F36C1E
1F36C1F 1F36C20 1F36C28 1F36C29 1F36C2A 1F36C46 1F36C47 1F36C48 1F36C50 1F36C51
    #exit
    actiondef activate_lp_action
      action priority 1 activate-lp-rule name ruledef-tai
    #exit
    actiondef activate_lp_action1
      action priority 3 event-triggers ecgi-change
    #exit
    actiondef ecgi_change
      action priority 1 activate-lp-rule name ruledef-ecgi
    #exit
    eventbase default
     rule priority 1 event new-call ruledef anymatch actiondef activate_lp_action1 continue

      rule priority 11 event new-call ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 12 event new-call ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 13 event new-call ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 14 event new-call ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 15 event new-call ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 16 event new-call ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 17 event new-call ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 18 event new-call ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 19 event new-call ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 20 event new-call ruledef ecgi-10 actiondef ecgi_change continue
      rule priority 21 event ecgi-change ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 22 event ecgi-change ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 23 event ecgi-change ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 24 event ecgi-change ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 25 event ecgi-change ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 26 event ecgi-change ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 27 event ecgi-change ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 28 event ecgi-change ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 29 event ecgi-change ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 30 event ecgi-change ruledef ecgi-10 actiondef ecgi_change continue
    #exit
  #exit
end
```

Traffic Optimization Policy Configuration

```
configure
active-charging-service ACS
traffic-optimization-policy Config:
    traffic-optimization-policy flow-create-ecgi-change
      heavy-session threshold 400000
    #exit
end
```

Local Policy Configuration



Important Configuring Local Policy needs a Local Policy Decision Engine License. Contact your Cisco account representative for information on specific licensing requirements.

This section describes the traffic optimization policy configuration that is based on location.

Use the following sample configuration to enable a eCGI change rule:

```
configure
   active-charging service service_name
      local-policy-service service_name
         ruledef ruledef_name
            condition priority priority_value ecgi mccmcc_value mnc mnc_value eq
eq_value
            exit
         actiondef actiondef_name1
            action priority priority_value event-triggers actiondef_name2
            exit
         actiondef actiondef_name2
            action priority priority_value activate-lp-ruleruledef_name
            exit
         eventbase eventbase_name
            rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
            rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
            exit
```

Service-Scheme Configuration

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger flow-create
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger condition trigger_condition_name
            local-policy-rule = rule_name
            exit
         trigger action trigger_action_name
            traffic-optimization policy policy_name
            exit
```

Configuring L7 Rule

Important Configuring L7 Rule needs an Application Detection Control License. Contact your Cisco account representative for detailed information on specific licensing requirements.

Use the following CLI to configure an L7 rule:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
```

```
        rule-name = rule_name
        rule-name = rule_name
          **Multi-line or All-lines**
    trigger-action trigger_action_name
        traffic-optimization policy policy_name
        exit
```

Sample Configuration

The following is a sample configuration for L7 Rules:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC6 trigger-action TA6
    #exit
    trigger-condition TC6
      rule-name = whatsapp
      rule-name = http
      multi-line-or all-lines
    #exit
    trigger-action TA6
      traffic-optimization policy flow-create-L7-Rules
    #exit
```

Ookla Speedtest

Use the configuration information discussed in the section Configuring L7 Rule, on page 333.

Sample Configuration

The following is a sample configuration for Ookla Speedtest:

```
service-scheme SS1
     trigger flow-create
       priority 1 trigger-condition ookla trigger-action ookla
     #exit
   trigger-condition ookla
     rule-name = speedtest
   #exit
   trigger-action ookla
     no traffic-optimization
   #exit
```

Location and App-based Configuration

Sample Configuration

```
service-scheme SS1
   trigger flow-create
     priority 1 trigger-condition TC3 trigger-action TA2
   #exit
   trigger-condition TC3
     local-policy-rule = ruledef-ecgi
     rule-name = youtube
     rule-name = whatsapp
     multi-line-or all-lines
   #exit
   trigger-action TA2
     traffic-optimization policy flow-create-ecgi-change
   #exi
```

Selective Configuration by Disabling TCP and UDP

Sample Configuration

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition tcponly trigger-action tcponly
      priority 2 trigger-condition udponly trigger-action udponly
    #exit
    trigger-condition tcponly
      ip protocol = tcp
    #exit
    trigger-condition udponly
      ip protocol = udp
    #exit
    trigger-action tcponly
      no traffic-optimization
    #exit
    trigger-action udponly
      no traffic-optimization
    #exit
```

L7/ADC and Location Trigger based Configuration

Sample Configuration

This sample configuration describes a scenario where an operator wants to always disable Traffic Optimization for Speedtest. The configuration disables traffic optimization regardless of the location. It applies a specific policy for a specific location (ECGI) (except for Speedtest) and overrides any other policy set by any trigger condition.

Also, for a specific policy optimization, for example: YouTube, the policy selection is prioritized as follows:

```
Service Scheme Configuration:
service-scheme SS1
trigger flow-create
  priority 1 trigger-condition speedtest-tc trigger-action speedtest-ta
  priority 2 trigger-condition location-tc trigger-action location-ta
  priority 3 trigger-condition youtube-tc trigger-action youtube-ta
  #exit
  trigger-condition location-tc
    local-policy-rule = ruledef-ecgi
  #exit
  trigger-action location-ta
    traffic-optimization policy flow-create-ecgi-change
  #exit
  trigger-condition speedtest-tc
    *rule-name = speedtest
  #exit
  trigger-action speedtest-ta
    no traffic-optimization
  #exit
  trigger-condition youtube-tc
    rule-name = youtube
  #exit
  trigger-action youtube-ta
    traffic-optimization policy youtube-policy
  #exit
* Provided rule-name = speedtest, is configured such that it always detects this traffic.
```

Cisco Ultra Traffic Optimization Bulk Statistics Enhancements

Feature Description

In this StarOS 21.23 release, the following show commands and bulk statistics schema counters are enhanced to show Rx/Tx packet statistics for Uplink and Downlink for UDP and TCP split in Cisco Ultra Traffic Optimization solution.

- show active-charging traffic-optimization counters sessmgr all
- show active-charging traffic-optimization counters tcp sessmgr all
- show active-charging traffic-optimization counters udp sessmgr all

Monitoring and Troubleshooting

Show Commands and Outputs

show active-charging traffic-optimization counters sessmgr all

You can view CUTO Control Plane statistics for the following show command.

Table 35: show active-charging traffic-optimization counters sessmgr all

Field	Description
CUTO Control Plane Stats:	
Total Active Streams	Displays total number of active streams.
Active TCP Streams	Displays total number of active TCP uplink and downlink streams received.
Active UDP(QUIC) Streams	Displays total number of active UDP uplink nd downlink streams transmitted.

You can also view similar outputs for the folowing show commands:

- **show active-charging traffic-optimization counters tcp sessmgr all**
- **show active-charging traffic-optimization counters udp sessmgr all**

show bulkstats variables ecs

The following ECS level statistic variables are added for the Cisco Ultra Traffic Optimization feature.

Table 36: Bulk Statistic Variables in the ECS Schema

Variables	Description	Data Type
cuto-tcp-uplink-rx	**Description:** Displays the total number of TCP packets received from the UE for Cisco Ultra Traffic Optimization **Type:** Counter **Triggers**: Increments whenever a TCP packet is received from the UE for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-tcp-uplink-tx	**Description:** Displays the total number of TCP packets sent towards the UE for Cisco Ultra Traffic Optimization. **Type:** Counter **Triggers**: Increments whenever a TCP packet is sent towards the UE for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-tcp-dnlink-rx	**Description:** Displays the total number of TCP packets received from the internet for Cisco Ultra Traffic Optimization. **Type:** Counter **Triggers**: Increments whenever a TCP packet is received from the internet for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-tcp-dnlink-tx	**Description:** Displays the total number of TCP packets sent towards the internet for Cisco Ultra Traffic Optimization **Type:** Counter **Triggers**: Increments whenever a TCP packet is sent towards the internet for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64

Variables	Description	Data Type
cuto-udp-uplink-rx	**Description:** Displays the total number of UDP packets received from the UE for Cisco Ultra Traffic Optimization. **Type:** Counter **Triggers**: Increments whenever a UDP packets is received from the UE for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-udp-uplink-tx	**Description:** Displays the total number of UDP packets sent towards the UE for Cisco Ultra Traffic Optimization **Type:** Counter **Triggers**: Increments whenever a UDP packet is sent towards the UE for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-udp-dnlink-rx	**Description:** Displays the total number of UDP packets received from the internet for Cisco Ultra Traffic Optimization. **Type:** Counter **Triggers**: Increments whenever a UDP packets is received from the internet for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64
cuto-udp-dnlink-tx	**Description:** Displays the total number of UDP packets sent towards the internet for Cisco Ultra Traffic Optimization. **Type:** Counter **Triggers**: Increments whenever a UDP packet is sent towards the internet for Cisco Ultra Traffic Optimization. **Availability**: Per Active Charging Service.	Int64

Bulk Statistics

The following bulk statistics are added in the ECS schema.

ECS Schema

Table 37: Bulk Statistics Variables in the ECS Schema

Variables	Description
cuto-tcp-uplink-rx	Indicates that the total number of TCP packets received from the UE for Cisco Ultra Traffic Optimization.
cuto-tcp-uplink-tx	Indicates that the total number of TCP packets sent towards the UE for Cisco Ultra Traffic Optimization.
cuto-tcp-dnlink-rx	Indicates that the total number of TCP packets received from the internet for Cisco Ultra Traffic Optimization.
cuto-tcp-dnlink-tx	Indicates that the total number of TCP packets sent towards the internet for Cisco Ultra Traffic Optimization.
cuto-udp-uplink-rx	Indicates that the total number of UDP packets received from the UE for Cisco Ultra Traffic Optimization.
cuto-udp-uplink-tx	Indicates that the total number of UDP packets sent towards the UE for Cisco Ultra Traffic Optimization.
cuto-udp-dnlink-rx	Indicates that the total number of UDP downlink packets received from the internet for Cisco Ultra Traffic Optimization.
cuto-dnlink-forward	Indicates that thee total number of data packets that are forwarded by Cisco Ultra Traffic Optimization library in the downlink direction.
cuto-dnlink-tx	Indicates that the total number of downlink packets sent by Cisco Ultra Traffic Optimization library.
cuto-dnlink-rx	Indicates that the total number of downlink packets received by Cisco Ultra Traffic Optimization library.
cuto-dnlink-hold	Indicates that the total number of data packets that are held by Cisco Ultra Traffic Optimization library in the downlink direction.

Configuring Cisco Ultra Traffic Optimization

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

Loading Traffic Optimization

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

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



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



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



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



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

Enabling Cisco Ultra Traffic Optimization Configuration Profile

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

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

NOTES:

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

Configuring the Operating Mode

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

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

Notes:

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

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

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

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

Session Setup Trigger

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

Following is a sample configuration:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
          trigger sess-setup
             priority priority_value trigger-condition trigger_condition_name1
trigger-action trigger_action_name
             exit
          trigger-condition trigger_condition_name1
             any-match = TRUE
             exit
          trigger-action sess-setup
          traffic-optimization policy sess-setup
             exit
```

Bearer Creation Trigger

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

The following is a sample configuration:

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

Flow Creation Trigger

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

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      trigger-condition trigger_condition_name3
         rule-name = rule_name
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
```

```
            priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
            exit
          exit
       subs-class sub_class_name
          apn = apn_name
          exit
       subscriber-base subscriber_base_name
          priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
          end
```

Notes:

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

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

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



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

Generating TODR

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

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

NOTES:

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

Monitoring and Troubleshooting

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

Cisco Ultra Traffic Optimization Show Commands and/or Outputs

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

show active-charging traffic-optimization counters

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

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



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

Following are the new field/counters:

- Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count

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

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



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

- TCP Traffic Optimization Flows:
  - Active Normal Flow Count

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

- UDP Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count

- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Base Policy:
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
- Extended Policy:
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count

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

show active-charging traffic-optimization info

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

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

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

Following are the new fields/counters:

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

show active-charging traffic-optimization policy

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

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Extended-Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Curbing-Control
  - Time
  - Rate
  - Max-phases
  - Threshold-Rate
- Extended-Curbing-Control
  - Time
  - Rate
  - Max-phases

    - Threshold-Rate
- Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Extended-Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Extended-Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Session-Params
    - Tcp-Ramp-Up
    - Udp-Ramp-Up
- Extended-Session-Params
    - Tcp-Ramp-Up
    - Udp-Ramp-Up

Bulk Statistics

The following bulk statistics are added in the ECS schema to support Large and Managed flows:

Bulk Statistics	Description
tcp-active-base-large-flow-count	Indicates the number of TCP active-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-managed-large-flow-count	Indicates the number of TCP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-active-base-unmanaged-large-flow-count	Indicates the number of TCP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-large-flow-count	Indicates the number of TCP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-managed-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-unmanaged-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-large-flow-count	Indicates the number of TCP total-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-managed-large-flow-count	Indicates the number of TCP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-unmanaged-large-flow-count	Indicates the number of TCP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-managed-large-flow-count	Indicates the number of TCP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-unmanaged-large-flow-count	Indicates the number of TCP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-large-flow-count	Indicates the number of UDP active-base-large-flow-count count for Cisco Ultra Traffic Optimization.
udp-active-base-managed-large-flow-count	Indicates the number of UDP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-unmanaged-large-flow-count	Indicates the number of UDP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-large-flow-count	Indicates the number of UDP active-ext-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-active-ext-managed-large-flow-count	Indicates the number of UDP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-unmanaged-large-flow-count	Indicates the number of UDP active-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-large-flow-count	Indicates the number of UDP total-base-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-managed-large-flow-count	Indicates the number of UDP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-unmanaged-large-flow-count	Indicates the number of UDP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-large-flow-count	Indicates the number of UDP total-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-managed-large-flow-count	Indicates the number of UDP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-unmanaged-large-flow-count	Indicates the number of UDP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-normal-flow-count	Indicates the number of TCP active-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-active-large-flow-count	Indicates the number of TCP active-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-managed-large-flow-count	Indicates the number of TCP active-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-unmanaged-large-flow-count	Indicates the number of TCP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-normal-flow-count	Indicates the number of TCP total-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-count	Indicates the number of TCP total-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-managed-large-flow-count	Indicates the number of TCP total-managed-large-flow count for Cisco Ultra Traffic Optimization.

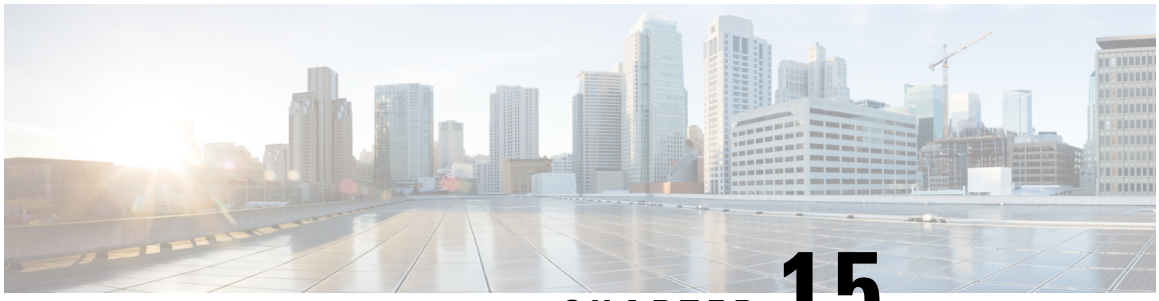
Bulk Statistics	Description
tcp-total-unmanaged-large-flow-count	Indicates the number of TCP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-io-bytes	Indicates the number of TCP total-IO bytes for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-bytes	Indicates the number of TCP total-large-flow bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-bytes	Indicates the number of TCP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-ms	Indicates the number of TCP total-recovered capacity ms for Cisco Ultra Traffic Optimization.
udp-active-normal-flow-count	Indicates the number of UDP active-normal-flow count for Cisco Ultra Traffic Optimization.
udp-active-large-flow-count	Indicates the number of UDP active-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-managed-large-flow-count	Indicates the number of UDP active-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-unmanaged-large-flow-count	Indicates the number of UDP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-normal-flow-count	Indicates the number of UDP total-normal-flow count for Cisco Ultra Traffic Optimization.
udp-total-large-flow-count	Indicates the number of UDP total-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-managed-large-flow-count	Indicates the number of UDP total-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-unmanaged-large-flow-count	Indicates the number of UDP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-io-bytes	Indicates the number of UDP total-IO bytes for Cisco Ultra Traffic Optimization.
udp-total-large-flow-bytes	Indicates the number of UDP total-large-flow bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-bytes	Indicates the number of UDP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-ms	Indicates the number of UDP total-recovered capacity ms for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-uplink-drop	Indicates the number of TCP uplink-drop for Cisco Ultra Traffic Optimization.
tcp-uplink-hold	Indicates the number of TCP uplink-hold for Cisco Ultra Traffic Optimization.
tcp-uplink-forward	Indicates the number of TCP uplink-forward for Cisco Ultra Traffic Optimization.
tcp-uplink-forward-and-hold	Indicates the number of TCP uplink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-uplink-hold-failed	Indicates the number of TCP uplink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-uplink-bw-limit-flow-sent	Indicates the number of TCP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-drop	Indicates the number of TCP downlink-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold	Indicates the number of TCP downlink-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward	Indicates the number of TCP downlink-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward-and-hold	Indicates the number of TCP downlink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold-failed	Indicates the number of TCP downlink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-dnlink-bw-limit-flow-sent	Indicates the number of TCP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-drop	Indicates the number of TCP downlink-async-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold	Indicates the number of TCP downlink-async-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward	Indicates the number of TCP downlink-async-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward-and-hold	Indicates the number of TCP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold-failed	Indicates the number of TCP downlink-async-hold-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-drop	Indicates the number of TCP process-packet-drop for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-process-packet-hold	Indicates the number of TCP process-packet-hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward	Indicates the number of TCP process-packet-forward for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-failed	Indicates the number of TCP process-packet-forward-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold	Indicates the number of TCP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold-failed	Indicates the number of TCP process-packet-forward and hold-failed for Cisco Ultra Traffic Optimization.
tcp-pkt-copy	Indicates the number of TCP packet-copy for Cisco Ultra Traffic Optimization.
tcp-pkt-Copy-failed	Indicates the number of TCP packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy	Indicates the number of TCP process-packet-copy for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy-failed	Indicates the number of TCP process-packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-action-forward	Indicates the number of TCP process packet, no packet found, and action forward for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of TCP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-action-drop	Indicates the number of TCP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
tcp-todrs-generated	Indicates the number of TCP TODRs generated for Cisco Ultra Traffic Optimization.
udp-uplink-drop	Indicates the number of UDP uplink-drop for Cisco Ultra Traffic Optimization.
udp-uplink-hold	Indicates the number of UDP uplink-hold for Cisco Ultra Traffic Optimization.
udp-uplink-forward	Indicates the number of UDP uplink-forward for Cisco Ultra Traffic Optimization.
udp-uplink-forward-and-hold	Indicates the number of UDP uplink-forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-uplink-hold-failed	Indicates the number of UDP uplink-hold failed for Cisco Ultra Traffic Optimization.
udp-uplink-bw-limit-flow-sent	Indicates the number of UDP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-drop	Indicates the number of UDP downlink-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-hold	Indicates the number of UDP downlink-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-forward	Indicates the number of UDP downlink-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-forward-and-hold	Indicates the number of UDP downlink-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-hold-failed	Indicates the number of UDP downlink-hold failed for Cisco Ultra Traffic Optimization.
udp-dnlink-bw-limit-flow-sent	Indicates the number of UDP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-async-drop	Indicates the number of UDP downlink-async-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold	Indicates the number of UDP downlink-async-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward	Indicates the number of UDP downlink-async-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward-and-hold	Indicates the number of UDP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold-failed	Indicates the number of UDP downlink-async-hold failed for Cisco Ultra Traffic Optimization.
udp-process-packet-drop	Indicates the number of UDP process-packet-drop for Cisco Ultra Traffic Optimization.
udp-process-packet-hold	Indicates the number of UDP process-packet-hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward	Indicates the number of UDP process-packet-forward for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-failed	Indicates the number of UDP process-packet-forward failed for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold	Indicates the number of UDP process-packet-forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-process-packet-forward-and-hold-failed	Indicates the number of UDP process-packet-forward and hold failed for Cisco Ultra Traffic Optimization.
udp-pkt-copy	Indicates the number of UDP packet-copy for Cisco Ultra Traffic Optimization.
udp-pkt-Copy-failed	Indicates the number of UDP packet-copy-failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy	Indicates the number of UDP process-packet-copy for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy-failed	Indicates the number of UDP process-packet-copy failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-forward	Indicates the number of UDP process packet, no packet found, action forward for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of UDP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-drop	Indicates the number of UDP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
udp-todrs-generated	Indicates the number of UDP TODRs generated for Cisco Ultra Traffic Optimization.



CHAPTER 15

Enable Cinder Volume Multi-attach to Multiple VNFs

- Feature Summary and Revision History, on page 357
- Feature Description, on page 358
- Configure Multi-attach Cinder Volume , on page 358
- Monitoring and Troubleshooting, on page 359

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• VPC-DI
Feature Default	Disabled - Configuration Required to Enable
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

Cinder is the OpenStack Block Storage service for providing volumes to the VNFs. Volumes are block storage devices that is attached to instances to enable persistent storage.

In P-GW, prior to OSP 16.0, operational issues developed when working with Virtual Customer Premises Equipment (VCPE) and RedHat. The Recover VM functionality brings down the VM Control Function (CF) of QvPC-DI and tries to bring it back up on a different compute host due to compute host failures. When a new CF instance comes up and redundant array of independent disks (RAID1) is formed, the active CF instance performs disk synchronization over the internet Small Computer System Interface (iSCSI) channel. This process is done block by block and iterates over the entire disk. Disk synchronization takes place over DI-LAN. When disk sizes are larger than 250GB, it takes time depending on how storage is configured, and DI-LAN network bandwidth, and traffic.

To overcome this issue, OSP16.1 is used to support the Cinder volume multi-attach . You can use this Cinder multi-attach capability to simultaneously attach volumes to multiple VNF instances.

- CF1 (Active) and CF2 (Standby) of QvPC-DI connects to the same multi-attach volume when bringing up the orchestrator.
- StarOS detects if CF1 and CF2 are connected to the same disk volume over the iSCSI channel.
- If a cinder volume multi-attach case is detected, the HD-RAID gets formed using the HD-local disk alone (disk connected to active CF). This process avoids the HD-RAID mirroring to solve the operational issues.

Disk Failures in Multi-attach

For disk failure in multi-attach, CF switchover is not possible as both CFs point to the same volume. If a disk failure is detected for Cinder volume multi-attach, it initiates an automatic ICSR switchover. The Interchassis Session Recovery (ICSR) setup is used to handle disk failure scenarios for Cinder volume multi-attach.

Monitor System Volume Status

When multi-attach cinder volume fails on the active CF card of vPGW, the monitor system volume functionality under the Service Redundancy Protocol (SRP) global configuration mode allows:

- Monitoring the system volume during volume attach and detach using a CLI command.
- Modification of switchover reason when the multi-attach cinder volume detaches from the active CF card and the SRP switch over happens.
- SNMP traps notification when the standby CF card from the active VNF detects volume detach.

Configure Multi-attach Cinder Volume

Use the following CLI command to enable the system to monitor multi-attach cinder volume status from the active CF.

```
configure
  context context_name
    service-redundancy-protocol
```

```
    [ no ] monitor system volume
  end
```

NOTES:

- **monitor system volume**: Enables Service Redundancy Protocol (SRP) to monitor volumes.
- **no**: Disables the volume monitoring.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot this feature using show commands.

Show Commands and Outputs

This section provides information about show commands and their outputs for this feature.

show hd raid verbose

The following new field is added to the output of this command:

- HD Raid
  - Degraded—No (Multiattach)

The following is the sample output:

Verify SRP Switchover Reasons through SNMP Traps Notification

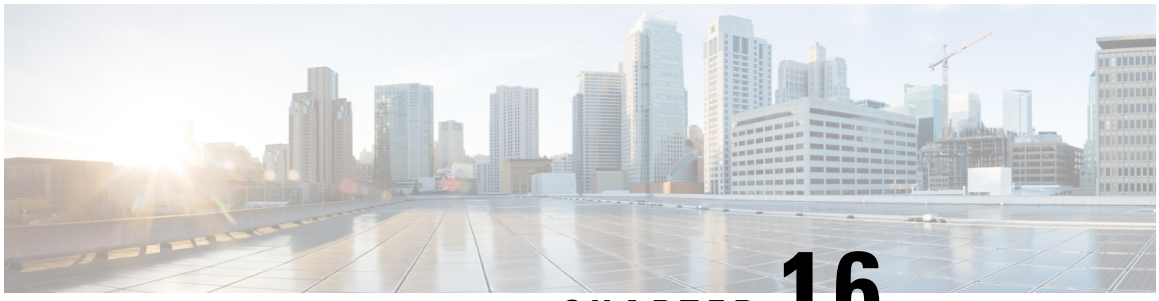
The standby CF card raises the following SNMP traps:

- **StorageNotFound**—volume detach
- **StorageFound**—volume attach

When the switchover occurs due to multi-attach volume detach from an active CF card, the SRPSwitchoverOccurred trap displays the reason as **Cinder Volume Failure**.

```
Internal trap notification 1278
 (SRPSwitchoverOccured)  vpn SRP ipaddr 2002:4888:34:13:386:200:0:11 rtmod
 18 Switchover Reason: (18) Cinder Volume Failure
```

Note When cinder volume is re-attached to the active card, it is not automatically detected by the system unless a soft reload is done.



CHAPTER 16

Cloud Initialization Support for Elastic Services Controller

- Feature Summary and Revision History, on page 361
- Feature Description, on page 361

Feature Summary and Revision History

Summary Data

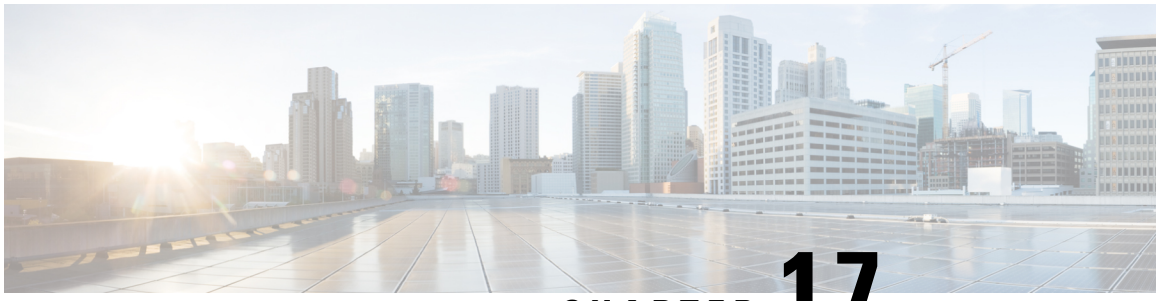
Applicable Product(s) or Functional Area	StarOS
Applicable Platform(s)	VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Openstack 16 and above
Related Documentation	*ASR 5500 System Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

When Elastic Services Controller (ESC) uses Cinder Multi-Attach volume on Control Function (CF), Active and Standby for QvPC-DI, the invoked Openstack API version for virtual machine (VM) Orchestration is 2.60 or higher. In this API version, ESC encodes and injects the configuration files into the VM for security reasons. Since, the VM is unable to read the encoded configuration files, ESC uses the **`user_data`** compressed file. This **`user_data`** file contains the configuration files that are required to boot VM.



CHAPTER 17

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, on page 363
- Session Redirection (Hotlining), on page 368

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:

Procedure

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 364.

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 367.

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, refer to the *AAA Interface Administration and Reference*.

- A number of optional keywords and variables are available for the **radius change-authorize-nas-ip** command. For more information regarding this command please refer to the *Command Line Interface Reference*.

CoA and DM Attributes

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

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

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

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

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

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

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

The following attributes are also supported:

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

CoA and DM Error-Cause Attribute

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

The value classes of error causes are as follows:

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

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

- 201- Residual Session Context Removed

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

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

Viewing CoA and DM Statistics

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

show session subsystem facility aaamgr

The following is a sample output of this command.

```
1 AAA Managers
807 Total aaa requests                                  0 Current aaa requests
379 Total aaa auth requests                             0 Current aaa auth requests
    0 Total aaa auth probes                             0 Current aaa auth probes
    0 Total aaa auth keepalive                          0 Current aaa auth keepalive
426 Total aaa acct requests                             0 Current aaa acct requests
    0 Total aaa acct keepalive                          0 Current aaa acct keepalive
379 Total aaa auth success                              0 Total aaa auth failure
    0 Total aaa auth purged                             0 Total aaa auth cancelled
    0 Total auth keepalive success                      0 Total auth keepalive failure
    0 Total auth keepalive purged
    0 Total aaa auth DMU challenged
367 Total radius auth requests                          0 Current radius auth requests
    2 Total radius auth requests retried
    0 Total radius auth responses dropped
    0 Total local auth requests                         0 Current local auth requests
  12 Total pseudo auth requests                         0 Current pseudo auth requests
    0 Total null-username auth requests (rejected)
    0 Total aaa acct completed                          0 Total aaa acct purged
    0 Total acct keepalive success                      0 Total acct keepalive timeout
    0 Total acct keepalive purged
    0 Total aaa acct cancelled
426 Total radius acct requests                          0 Current radius acct requests
    0 Total radius acct requests retried
    0 Total radius acct responses dropped
    0 Total gtpp acct requests                          0 Current gtpp acct requests
    0 Total gtpp acct cancelled                         0 Total gtpp acct purged
    0 Total null acct requests                          0 Current null acct requests
  54 Total aaa acct sessions                            5 Current aaa acct sessions
    3 Total aaa acct archived                           0 Current aaa acct archived
    0 Current recovery archives                       0 Current valid recovery records

    2 Total aaa sockets opened                          2 Current aaa sockets open
    0 Total aaa requests pend socket open
    0 Current aaa requests pend socket open
    0 Total radius requests pend server max-outstanding
    0 Current radius requests pend server max-outstanding
    0 Total aaa radius coa requests                     0 Total aaa radius dm requests
    0 Total aaa radius coa acks                         0 Total aaa radius dm acks
    0 Total aaa radius coa naks                         0 Total aaa radius dm naks
    2 Total radius charg auth                           0 Current radius charg auth
    0 Total radius charg auth succ                      0 Total radius charg auth fail
    0 Total radius charg auth purg                    0 Total radius charg auth cancel

    0 Total radius charg acct                           0 Current radius charg acct
    0 Total radius charg acct succ                      0 Total radius charg acct purg
    0 Total radius charg acct cancel
357 Total gtpp charg                                    0 Current gtpp charg
357 Total gtpp charg success                            0 Total gtpp charg failure
    0 Total gtpp charg cancel                           0 Total gtpp charg purg
    0 Total prepaid online requests                   0 Current prepaid online requests

    0 Total prepaid online success                    0 Current prepaid online failure

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

```
0 Current prepaid online purged
0 Total aaamgr purged requests
0 SGSN: Total db records
0 SGSN: Total sub db records
0 SGSN: Total mm records
0 SGSN: Total pdp records
0 SGSN: Total auth records
```

Session Redirection (Hotlining)



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

Overview

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

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

License Requirements

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

Operation

ACL Rule

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

Redirecting Subscriber Sessions

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

For information on CoA messages and how they are implemented in the system, refer to RADIUS Change of Authorization and Disconnect Message, on page 363.



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

Session Limits On Redirection

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

Stopping Redirection

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

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

Handling IP Fragments

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

Recovery

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

AAA Accounting

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

Viewing the Redirected Session Entries for a Subscriber

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

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

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

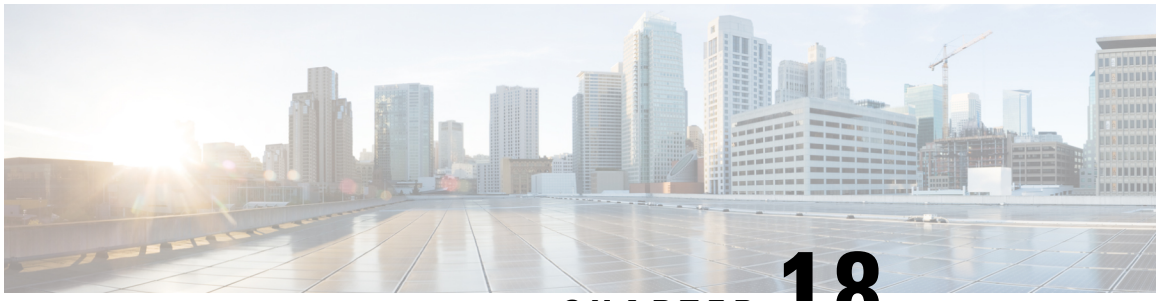
show subscribers debug-info msid 0000012345

The following is a sample output of this command:

```
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED      SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                  Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
         Failure (other reasons):  0
Redirected Session Entries:
         Allowed:                  2000      Current:                   0
         Added:                    0         Deleted:                   0
         Revoked for use by different subscriber: 0
  Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:             0          0             0ms            0ms
     Micro:            0          0             0ms            0ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_MAKECALL
            SMGR_STATE_MAKECALL_PENDING     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_REQ
```

```
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED             SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_RSP_SUB_SESSION
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                            Event
            SMGR_STATE_OPEN                  SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED       SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED      SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                  Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
         Failure (other reasons):  0
Redirected Session Entries:
         Allowed:                  2000      Current:                   0
         Added:                    0         Deleted:                   0
         Revoked for use by different subscriber: 0
Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:             0          0             0ms            0ms
     Micro:            0          0             0ms            0ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                            Event
            SMGR_STATE_OPEN                  SMGR_EVT_MAKECALL
            SMGR_STATE_MAKECALL_PENDING      SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED             SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_RSP_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_ADD_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
  Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
         Total out-of-seq arrived: 0
  IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
```

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



CHAPTER 18

Collision Handling on the P-GW/SAEGW/S-GW

- Feature Description, on page 373
- How It Works, on page 373
- Configuring Collision Handling, on page 376
- Monitoring the Collision Handling Feature, on page 377

Feature Description

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. GTP procedure collisions are quite common in the network; especially with dynamic Policy and Charging Control, the chances of collisions happening in the network are very high.

These collisions are tracked by statistics and processed based on a pre-defined action for each message collision type. These statistics assist operators in debugging network issues.

Important If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will see the respective collision statistics if they occur.

Relationships to Other Features

- This feature is a part of the base software license for the P-GW/SAEGW/S-GW. No additional license is required.
- A P-GW, S-GW, or SAEGW service must be configured to view GTPv2 collision statistics.

How It Works

Collision Handling

As GTPv2 message collisions occur, they are processed by the P-GW, SAEGW, and S-GW. They are also tracked by statistics and with information on how the collision was handled.

Specifically, the output of the **show egtpc statistics** verbose command has been enhanced to provide information on GTPv2 message collision tracking and handling at the S-GW and P-GW ingress interfaces, The information available includes:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5) and P-GW (S8).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure. Note that the Old Proc are per 3GPP TS 23.401.
- **New Proc (Msg Type)**: The new procedure and message type. Note that the New Proc are per 3GPP TS 23.401.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old**: Abort the original message handling and processes the new message.
  - **Reject New**: Reject the new message, and process the original (old) message.
  - **Silent Drop New**: Drop the new incoming message, and the process the old message.
  - **Parallel Hndl**: Handle both the original (old) and new messages in parallel.
  - **Buffer New**: Buffer the new message and process it once the original (old) message has been processed.
- **Counter**: The number of times each collision type has occurred.



Important The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

Sample output:

```
Message Collision Statistics
   Interface      Old Proc (Msg Type)       New Proc (Msg Type)    Action    Counter
    SGW(S5)   NW Init Bearer Create (95)  NW Init PDN Delete (99)  Abort Old    1
```

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.

The action that is carried out due to this collision at the eGTP-C layer is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the Initiate PDN Delete procedure. The Counter total of 1 indicates that this collision happened once.

Example Collision Handling Scenarios

This section describes several collision handling scenarios for the S-GW and P-GW.

The S-GW processes additional collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification (DDN) message with Create Bearer Request or Update Bearer Request.

The S-GW behavior to handle these collision scenarios are as follows:

1. A CBReq and MBReq [(Inter MME/Inter RAT (with or without ULI change)] collision at the S-GW ingress interface results in the messages being handled in parallel. The CBReq will wait for a Create Bearer Response (CBRsp) from the peer. Additionally, an MBReq is sent in parallel to the P-GW.
2. An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change)] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.
3. Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

As a result, no S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.

The following GTP-C example collision handling scenarios may also be seen on the P-GW:

DBCmd/MBreq Collision Handling:

The P-GW enables operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW.

There are three CLI-controlled options to handle the collision between the DBCmd and MBReq messages:

- Queue the DBcmd message when the MBreq message is pending. The advantage of this option is that the DBCmd message is not lost for most of the collisions. It will remain on the P-GW until the MBRsp is sent out.
- Drop the DBCmd message when the MBreq message is pending. Note that with this option the S-GW must retry the DBCmd.
- Use pre-StarOS 19.0 behavior: abort the MBreq message and handle the DBcmd message. The advantage of this option is that it provides backward compatibility if the operator wants to retain pre-StarOS 19.0 functionality.

The CLI command **collision handling** provides more flexibility in configuring the handling of the DBCmd message and MBReq message collision scenario. Also refer to Configuring DBcmd Message Behavior, on page 376 in this document for instructions on how to configure the behavior for this collision handling scenario.

MBReq/CBreq Parallel Processing; Handling CBRsp:

The P-GW/S-GW handles the following example collision scenario:

The node queues the CBRsp message and feeds the CBRsp message to the P-GW/S-GW session manager when the MBRsp is sent out. As a result, operators will see no retransmission of CBRsp messages from the MME.

Handling UBrsp when Transaction is Suspended:

The P-GW/S-GW handles the following example collision scenario:

When the P-GW/S-GW receives an UBRsp message, then the P-GW/S-GW handles the UBRsp message for the suspended transaction. As a result, The UBRsp message will be buffered until the MBRsp message is sent out.

Collision Handling of MBR over MBR for Drop and Retry

To avoid collision over Modify bearer request (mbreq) message over mbreq, the MME supports collision of MBR over MBR Drop and Retry functionality through a `mbreq-over-mbreq drop` CLI configuration under the egtp-service. The following functions occur:

- MME sends modify bearer request when service request modify bearer request is in pending state
- S-GW drops the E-RAB procedure modify bearer request message
- MME retries the dropped MBR until first MBR response.

Limitations

There are no known limitations to the collision handling feature on the P-GW/SAEGW/S-GW.

Standards Compliance

Specifications and standards do not specify any hard rules for collision handling cases.

Configuring Collision Handling

Operators can use the Command Line Interface (CLI) to configure the behavior of the P-GW for handling the following GTPv2 message collision:

- DBcmd Message when the MBreq Message for the Default Bearer is pending at the P-GW



Important Configuration via the CLI is **not** required for all other P-GW and S-GW collision handling scenarios.

Configuring DBcmd Message Behavior

Use the following example to configure the collision handling behavior for the Delete Bearer command message when the Modify Bearer Request message for the Default Bearer is pending at the P-GW.

```
configure
   context  context_name
      egtp-service  egtp_service_name
         collision-handling dbcmd-over-mbreq  { drop | queue }
         { default | no } collision-handling dbcmd-over-mbreq
         end
```

NOTES:

- **collision-handling dbcmd-over-mbreq** : Configures collision handling of DBcmd when MBreq is pending.
- **drop**: Drop the DBcmd message when the MBreq message is pending.
- **queue**: Queue the DBcmd message when the MBreq is message is pending.

  The default behavior is to abort the MBReq message and handle the DBcmd message.

Verifying the Configuration

To verify the DBcmd Message when the MBreq Message for the Default Bearer is pending at the P-GW configuration, use the following command in Exec Mode:

```
show egtpc service all
     Collision handling: DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort
 MBreq and handle Dbcmd>
```

Monitoring the Collision Handling Feature

This section describes how to monitor the collision handling feature.

Collision Handling Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the collision handling on the P-GW/SAEGW/S-GW feature.

show configuration

The output of this command indicates if collision handling for the DBcmd message when the MBreq message is pending is enabled or disabled or for the mbreq over mbreq drop messages:

- collision-handling dbcmd-over-mbreq queue
- no collision-handling dbcmd-over-mbreq queue
- collision-handling mbreq-over-mbreq drop

show egtp-service all | name

The output of this command indicates how the P-GW is configured to handle the DBcmd Message when the MBreq message for the Default Bearer is pending at due to Drop MBreq or Abort MBreq and handle MBreq scenarios:

- Collision handling:
  - MBreq when MBreq pending

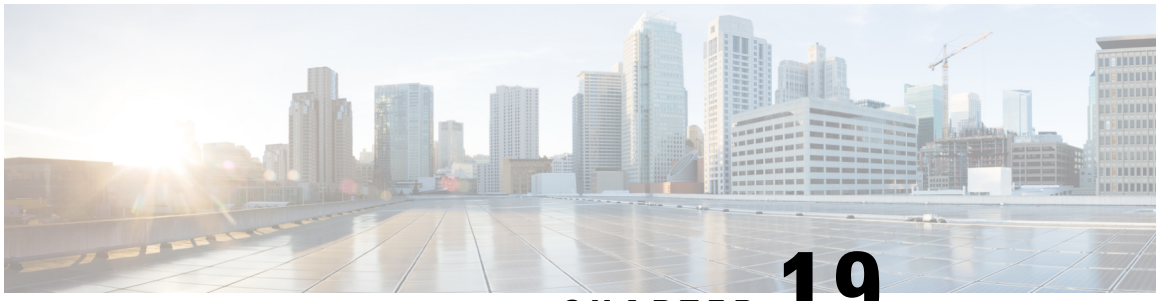
show egtp statistics verbose

The output of this command has been enhanced to provide detailed information for all supported GTPv2 message collisions at the P-GW/S-GW ingress interface, including:

- The interface on which the collision occurred.
- The ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- The new procedure and message type.
- The pre-defined action taken to handle the collision.
- The number of times each collision type has occurred.



Important The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.



CHAPTER 19

Closed Subscriber Group Mobility Event Support on P-GW and GGSN

- Feature Summary and Revision History, on page 379
- Feature Description, on page 380
- Access Control, on page 380
- How it Works, on page 383
- Behavior Matrix, on page 384
- Monitoring and Troubleshooting, on page 384

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • GGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	• *Statistics and Counters Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, support for Closed Subscriber Groups mobility event for P-GW and GGSN is added.	21.23

Feature Description

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the Public Land Mobile Network (PLMN) as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN, which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG information change reporting for a subscriber session requested by GGSN, the Serving GPRS Support Node (SGSN) includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

When users enter or exit the CSG Cells or Hybrid Cells, if there are no event notifications sent back to the P-GW and Gateway GPRS Support (GGS), the capability to provide different policy and charging characteristic to the users becomes limited. In this StarOS 21.23 and later releases, CSG mobility event support is available in multiple network elements, namely eNodeB, MME, SGW, PGW, PCRF, SGSN, GGSN, HSS, and so on. This CSG mobility event feature provides full support of CSG capability on P-GW and GGSN based on 3GPP standards. This CSG mobility event feature includes capability to:

- Enable and trigger the CSG notification event.
- Apply appropriate policy and charging rules.

Access Control

The CSG Mobility Event feature functions on S5/S8, Gn/Gp, Gx, and Rf interfaces:

S5 and S8 Interfaces

The message types that processes CSG information shows the message initiated from MME and the messages initiated from PGW. S-GW passes the information from and to MME.and to and from P-GW:

- **Create Session Request**: In the Create Session Request (CSR) message, it contains a CSG Change Reporting Support Indication(CCRSI) flag when MME is configured to support CSG information change reporting to the S-GW and P-GW. If the UE is attached through a CSG or hybrid cell, the User CSG information (UCI) IE is included in the CSR. The User CSG Information IE contains the PLMN and CSG ID of the CSG or hybrid cell, the access mode (closed or hybrid), and if the access mode is hybrid, the membership status of the UE in the CSG.
- **Create Session Response**: If CSG information reporting is started or stopped, the P-GW/S-GW sends the CSG Information Reporting Action (CIRA) IE in the Create Session Response . This IE includes three bits that indicate whether the MME should report when the UE enters or leaves a CSG (non-hybrid) cell, a subscribed hybrid cell, or an unsubscribed hybrid cell. If all three bits are set to zero, all CSG information reporting to the S-GW and P-GW is stopped. The MME stores the CSG reporting information as part of the PDN context,.
- **Create Bearer Request**: If CSG reporting from the MME changes, the Create Bearer Request message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.
- **Modify Bearer Request**: The CCRSI flag in the Indication IE is set in a Modify Bearer Request when the MME is configured to support CSG information change reporting to the S-GW and P-GW. If the

P-GW and S-GW has requested CSG information reporting and a TAU, Handover, or UE-initiated Service Request is taking place, the MME includes the UCI IE in the Modify Bearer Request message.

- **Update Bearer Request**: If CSG reporting from the MME changes, the Create Bearer Request message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.
- **Change Notification Request**: If there is a change to the CSG connection information without a Create Bearer Request or Modify Bearer Request, the MME sends a Change Notification Request to the S-GW P-GW for each PDN where it is requested. The Change Notification Request contains a UCI IE. Since Location Reporting also uses the Change Notification Request message, the MME minimizes the number of Change Notification Request messages sent by bundling the reporting of a location change with a CSG change into the same message whenever possible.
- **Change Notification Response**: If CSG reporting from the MME changes, the Change Notification Response message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.

Gn and Gp Interfaces

The message types that processes CSG information shows the message initiated from SGSN and the messages initiated from GGSN:

- **Create PDP Context Request (CPC Request)**: The CPC Request message contains a CSG Change Reporting Support Indication (CCRSI) flag when SGSN is configured to support CSG information change reporting to the GGSN. If the UE is attached through a CSG or hybrid cell, the User CSG information (UCI) IE is included in the CPC. The User CSG Information IE contains the PLMN and CSG ID of the CSG or hybrid cell, the access mode (closed or hybrid), and if the access mode is hybrid, the membership status of the UE in the CSG.



Note Ignores UCI value on GGSN/P-GW when access mode value is reserved (2 or 3).

- **Create PDP Context Response (CPC Response)**: If CSG information reporting is to be started or stopped, the GGSN sends the CSG Information Reporting Action (CIRA) IE in the CPC Response. This IE includes three bits that indicate whether the SGSN should report when the UE enters or leaves a CSG (non-hybrid) cell, a subscribed hybrid cell, or an unsubscribed hybrid cell. If all three bits are set to zero, all CSG information reporting to the GGSN is stopped.
- **Update PDP Context Request (UPC Request)**: The CCRSI flag in the Extended Common Flags IE is set in UPC Request when the SGSN supports CSG Information Change Reporting and if CSG Change Reporting is requested by the GGSN through the CSG Information Reporting Action. If the UE is accessed through CSG cell or Hybrid cell, the SGSN includes the User CSG Information IE.
- .**Network Requested Update PDP Context Request (NRUPC Request)**: If CSG reporting from the SGSN changes, the NRUPC Request message from the GGSN includes a CIRA IE. The SGSN stores the CSG reporting information as part of the PDN context.
- **MS Info Change Notification Request**: The MS Info Change Notification Request contains a UCI IE and CCRSI flag in the Extended Common Flags IE. Since Location Reporting also uses the MS Info Change Notification Request message, the SGSN minimizes the number of MS Info Change Notification

Request messages sent by bundling the reporting of a location change with a CSG change into the same message whenever possible.

- **MS Info Change Notification Response**: If CSG reporting from the SGSN changes Notification Response message from the GGSN includes a CIRA IE . The SGSN stores the CSG reporting information as part of the PDN context.

Gx Interface

During CSG handling related messages over Gx interface the following functions happen:

- **Internet Protocol**: During an Internet Protocol connectivity Access Network (IP-CAN) session, the PCRF determines whether the reports for change of CSG cell or Hybrid cell is required for an IP-CAN session.
- When the UE enters or leaves the CSG or Hybrid cell, Policy and Charging Enforcement Function (PCEF) reports either USER_CSG_INFORMATION_CHANGE, USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE, or USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE event. PCEF also reports the CSG change within the User-CSG-Information AVP.
- If CSG-Information-Reporting AVP is not received in subsequent CCA-U messages, existing CSG-Information-Reporting values are reused.
- CSG-Information-Reporting AVP is used by PCRF to inform PCEF to report the user CSG information change to the Charging Data Function (CDF)/ Offline Charging Server (OFCS) over RF interface. If this AVP is not received during IPCAN session, PCEF does not report the user CSG information change to the CDF/OFCS.

Rf Interface

The ACR messages in the CSG information handling involve:

- User CSG Information (UCI) at PS level (Ps-Information AVP) to send information only during ACR start message. Sends UCI information SDC level (Service-Data-Container AVP) in subsequent messages



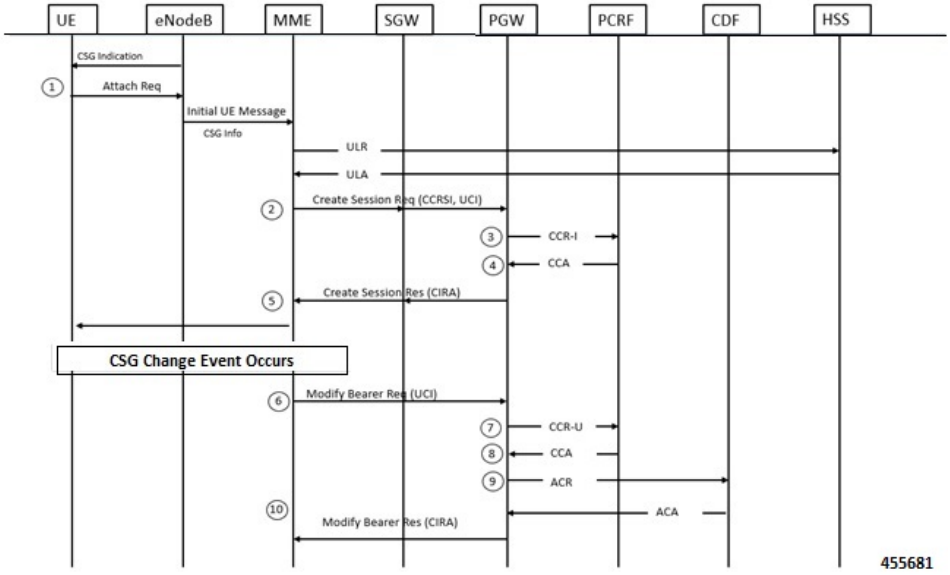
Important Configuration **attribute csg** in the Rf profile enables UCI information at PS level when transmitted in the ACR start message.

- User CSG Information (UCI) change value gets added in the Change-Condition AVP at SDC level every time when change of User CSG Information is received from access side and CSG change reporting to OFCS in CSG Information is enabled in the Reporting AVP from PCRF.
- If CSG Information Reporting is not received during IP-CAN session, P-GW does not send User CSG Information AVP to OFCS over Rf interface.

How it Works

The following diagram shows the messaging between the EPC elements in a Closed Subscriber Group implementation.

Figure 16: Closed Subscriber Groups Message Call Flow



The following steps describes the workflow:

1. The eNodeB broadcasts the CSG Information to UEs. When an Attach Request event happens, the eNodeB sends its own CSG-related Information in Initial UE message to the MME. The MME sends an Update Location Request (ULR) to the HSS to get subscriber's profile. The HSS responds with an update Location Answer including subscription-data which includes CSG-subscription-data.
2. The MME proceeds with the call according to the user profile from the HSS. The MME sets the CSG membership Indication and passes it to the S-GW including Access Mode and CSG-ID. The S-GW transparently passes the information to the P-GW.
3. The P-GW requests policy and charging rule from the PCRF.
4. The PCRF sends Event-Trigger:=USER_CSG_INFORMATION_CHANGE, USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE and USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE and CSG-Information-Reporting AVP based on the user subscription profile.
5. The P-GW sets CSG-Information-Reporting-Action in Create Session Response when the P-GW receives Event-Trigger:=USER_CSG_INFO_CHG.
6. The MME sends CSG-Membership-Status to eNodeB. This is only occurs when the Access mode is set to Hybrid.
7. The eNodeB/MME reports the event when a CSG change event happens. The MME updates CSG change event using a Change Notification Request or Modify Bearer Request.

8. The P-GW reports CSG change event using Event-Reporting-Indication AVP to the PCRF.
9. The PCRF updates the policy and charging rule with Charging-Rule-Base-Name or install new Charging-Rule-Base-Name.
10. The P-GW reports charging record to CDF over Rf interface and includes User-CSG-Information AVP, if PCRF reports CSG-Information-Reporting AVP with CHANGE_CSG_CELL flags.
11. If the policy and charging rule changes cause bearer modification or creation, the P-GW sends a CSG Information Reporting Action IE as part of the Modify Bearer Response, a Change Notification Response, or it can initiate a change through an Update Bearer Request.

Behavior Matrix

Following Message types and the CSG AVP are available in the Gx and Rf interfaces.

Table 38: Message Type behaviour (E-UTRAN/UTRAN)

Message Type	User-CSG-Information AVP (Gx)	User-CSG-Information AVP (Rx)
Create-Session-Request/ Create PDP Context Request	CCR - I	ACR-Start
Modify-Bearer-Request/Update PDP Context Request	CCR-U	ACR-Interim
Change -Notification -Request/MS Info Change Notification Request	CCR-U	ACR-Interim
Delete-Session-Request/ Delete PDP Context Request	-	ACR-Stop
Delete-bearer-Request	-	ACR-Interim/Stop

Note Only 3G and E-UTRAN RAT Type is supported for CSG -information on Gx and Rf Interface.

Handoff Expected Behavior: If there are UE handover from E-UTRAN or 3G to other RAT types (for example. WI-FI) , then the User-CSG-Information AVP will not be sent on Gx and Rf interface.

Monitoring and Troubleshooting

This section provides information regarding show command outputs available for the Closed Subscriber Groups mobility event feature.

Show Commands and Outputs

show subscribers pgw-only full all

The output of **show subscribers pgw-only full all** command has been enhanced to include the following output fields in support of the Closed Subscriber Groups Mobility Event feature on P-GW and GGSN.

Similarly, the output of **show subscribers ggsn-only full all** and **show subscribers saegw-only full** CLI commands has been enhanced to include the following output fields:

Field	Description
UCI	
MCC	Displays a Mobile Country Code (MCC) for User CSG Information.
MNC	Displays a Mobile Network Code (MNC) for the User CSG Information.
CSG-ID	Displays the Closed Subscriber Group identifier.
Access Mode	Displays a matching access mode.
LCSG	Displays Leave Closed Subscribers Group (LCSG) value. The default value is 0.
CMI	Displays CSG Membeship Information (CMI). The CMI displayed is either Member or Non-Member of hybrid cell.

show ims-authorization sessions full all

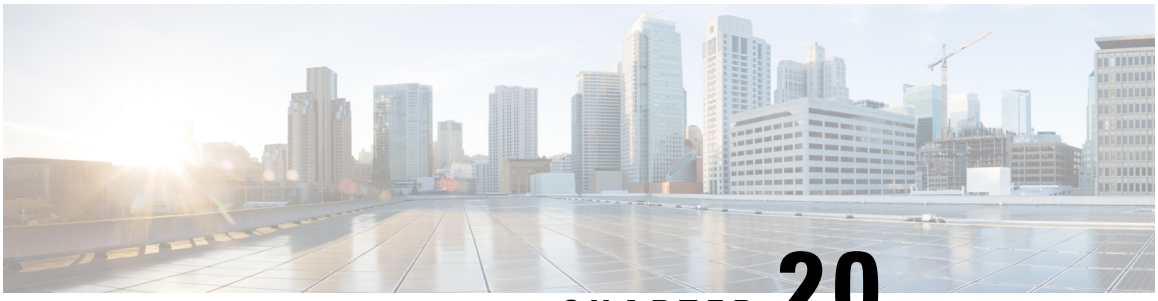
The output of this command has been enhanced to include the following output fields in support of the Closed Subscriber Groups Mobility Event feature on P-GW and GGSN.

Field	Description
Auth Decision:	
Event Triggers:	
User-CSG-Information-Change	Displays total number of User CSG Information change request event triggers.
User- CSG -Hybrid-Subscribed -Information -Change	Displays total number of User CSG Hybrid Subscribed Information.change request event triggers.
User-CSG-Hybrid- Unsubscribed -Information -Change	Displays total number of User CSG Hybrid Unsubscribed Information.change request event triggers..

show ims-authorization service statistics

The output of this command displays the the CSG feature statistics.

Field	Description
Re-Authorization Triggers	
User CSG Info Chg	Displays total number of User CSG Information.change counters.
User CSG Hybrid Sub Info Chg	Displays total number of User CSG Hybrid Subscribed Information change counters.
User CSG Hybrid Unsub Info Chg	Displays total number of User CSG Hybrid Unsubscribed Information change counters.



CHAPTER 20

Crowd Sourcing Optimization

- Feature Summary and Revision History, on page 387
- Feature Description, on page 388
- How it Works, on page 388
- **Configuring Detection Mode for Elephant Detection Mechanism**, on page 390
- Configuring Crowd Source Optimization in trial-mode, on page 390
- Monitoring and Troubleshooting, on page 391

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in this Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First Introduced.	21.23

Feature Description

The Crowd Sourcing Optimization feature uses historical data sessions to provide an increase in recovered capacity from active elephants through seeding profiles and more rapid learning of cell conditions and capabilities.

Crowd Sourcing Optimization feature allows

- Reporting of real-time and historical cell characteristics that capture performances of traffic flows.
- Handling of traffic from the same subscriber by the same session manager.
- Location update enablement.
- Reporting to Cisco Ultra Traffic Optimization library based on the ECGI change instead of ULI change.
- Crowd Sourcing information on each VPP instance.



Note The Crowd Sourcing Optimization feature works only if P-GW learns about user location (for example, from MME). Hence, you should enable the User Location Information update.

Relationship to Other Feature

The Crowd Sourcing Optimization feature is related to Cisco Ultra Traffic Optimization functionality. For details, see the *Cisco Ultra Traffic Optimation* chapter in the *P-GW Administration Guide*.

Licensing

The Crowd Sourcing Optimization feature requires Feature Pack1 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*.

How it Works

The Crowd sourcing optimization procedure describes:

- Handling ECGI Information
- Enhanced elephant detection mechanism
- Trial Mode mechanism

Handling ECGI Information

Following is the workflow for processing ECGI data:

- When P-GW records the ULI information it receives the session creation request.
- P-GW experiences the traffic, recorded ULI information is reported to CUTO during flow creation.
- During the location update, new ULI information is received in bearer modification request during mid flows. All the flows of respective subscribers gets onloaded and new ULI information is reported through CUTO stream modification and streams get offloaded again once rule is matched.

  Under the “CUTO Upgrade Pack 1” license:

  - Reporting of the ULI information is generated based on CUTO algorithm.
  - ULI type and ECGI information gets captured in TODR after the end of flow in multiple phases. It helps for analysis of flows in scale scenario.

Enhanced Elephant Detection Mechanism

Detection of elephant logic, which is based on byte-based, time-based, or bytes-and-time-based thresholds, are added in the configuration CLI as follows.

- Detection mechanism is grouped under the following two modes:
  - **Base Mode**: In Base mode, threshold bytes parameter value is considered.
  - **Enhanced Mode**: In Enhanced mode, combinations of threshold bytes and seed-time values are considered.

  Flows become elephant when either of them crosses first.



Note Seed time is applicable in enhanced mode of detection. Ensure to activate Seed Time and Detection Mode CLI options under the CUTO Upgrade Pack1 license to view all parameters in the CLI.

- Detections of the elephant flows are based on the cuto base policy configuration parameters (seed-time, detection-mode) and CUTO does not consider extended based policy parameters in detection algorithm. CLI throws warning as:

```
Seed-time configured will not take effect for detection. Please configure
under heavy-session” when it’s getting configured.
```

- Detection-cause (time or bytes) and cuto mode (Active/Passive) are recorded in TODR, which helps in the analysis of flows in scale. Detection-cause is recorded under “CUTO Upgrade Pack 1” license and cuto-mode is recorded without any license and applicable for the base CUTO license as well.

Trial Mode

Trail Mode allows the feature to schedule a A/B test campaign from within the P-GW that alternates active and passive modes at regular intervals to demonstrate CUTO’s network efficacy.The Trial Mode operates under the traffic-optimization license or Cisco Ultra Traffic Optimization suppression license, but does not

need the“CUTO feature pack 1” license to turn it on. Service Request (SR) is supported as Trial Mode is applicable only on the Active chassis, however, ICSR is not supported.



Important Make sure to disable Trial Mode before making any changes in the **cuto-profile** because no changes are allowed in the **cuto-profile** during Trial Mode.

Configuring Detection Mode for Elephant Detection Mechanism

Detection of elephant logic that is based on byte-based, time-based or bytes-and-time-based thresholds are added in the configuration CLI as follows.

```
configure
   active-charging service service_name
      [ no ] traffic-optimization-policy policy_name[extended]
         default detection-mode
         detection-mode
        [ no ] heavy-session { standard-flow-timeout  standard_flow-timeout_value
  threshold threshold_value  seed-time seed_time_value }
         end
```

NOTES:

- **default**: Default configuration for detection-mode.
- **detection-mode**: Configures heavy-session detection mode. The default value for detection mode is "enhanced".
- **heavy-session**: Configures heavy-session detection related parameters.
- **seed-time**: Configures time in ms for detection of elephant flow. Use this parameter in the enhanced detection mode.

Configuring Crowd Source Optimization in trial-mode

Use the following CLI commands to enable the Crowd Sourcing Optimization feature in trial-mode.

```
configure
   require active-charging
   active-charging service service_name
      traffic-optimization-profile
         trial-mode  start-time YYYYMMDDHHMM end-time YYYYMMDDHHMM
mode-toggle-interval mode_toggle_interval initial-mode initial_active |
initial_passive
         end
```

NOTES:

- **trial-mode**: Enables the Crowd Sourcing Optimation feature in the Trial Mode.
- **start-time** : Local time begins trial in YYYY:MM:DD:HH:MM.

- **end-time** : Local time ends trial in YYYY:MM:DD:HH:MM.
- **toggle-mode-interval** : Provides interval in minutes to toggle the CUTO mode toggling between Active and Passive at interval. Interval can be at 15, 30, 60 minutes. Starting interval is at 15 minutes.
- **initial-mode** : Set the initial mode with Active or Passive when trial starts.
  - active: Start the trial mode with CUTO mode as active.
  - passive: Start the trial mode with CUTO mode as passive

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Crowd Sourcing Optimization solution on the P-GW.

Show Commands and Outputs

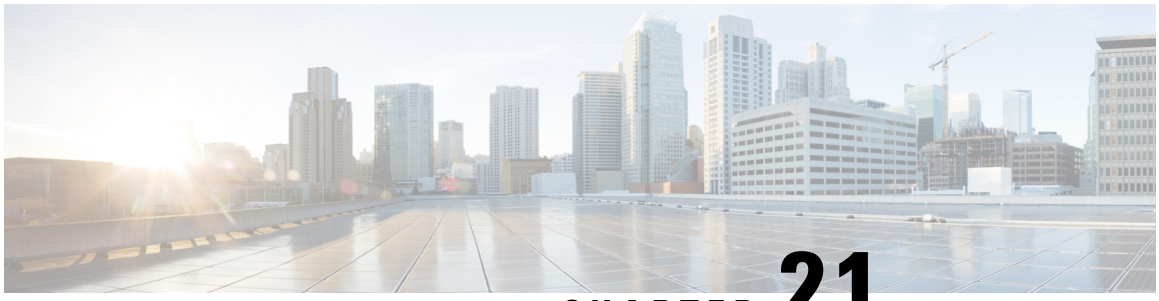
This section provides information about show commands and the fields that are introduced in support Crowd Sourcing Optimization solution.

show active-charging traffic-optimization policy all

Shows configured values of heavy-sessions, extended-heavy-session at active charging service level and traffic optimization policy.

Table 39:

Field	Description
Heavy-Session: Shows heavy-session detection related parameters.	
Seed-Time	Displays time in milliseconds for detection of elephant flow.
Detection-Mode: Shows heavy-session detection mode (Default: enhanced).	
Extended Heavy-Session: Shows heavy-session detection related parameters for extended policy	
Seed-Time	Displays time in milliseconds for detection of elephant flow.



CHAPTER 21

Customizing Access-Link IP Fragmentation

- Feature Summary and Revision History, on page 393
- Feature Description, on page 394
- Configuring Access-Link IP Fragmentation, on page 394
- Monitoring and Troubleshooting, on page 396

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Support is added for access-link fastpath to enforce APN MTU for IPv4 traffic.	21.27
First introduced.	21.26

Feature Description

The P-GW APN level configuration controls the IP fragmentation, if the forward or drop logic for IP packets that are larger than MTU, becomes higher due to GTPU encapsulation overheads. To override multiple configurations at the APN level, the global-level CLI reduces deployment time, configuration size, and minimizes errors.

Note If the CLI is not configured at the APN level, the Global level configuration is applied by default. If the CLI is not configured at the Global level, then the default value is applied.

Configuring Access-Link IP Fragmentation

Configuring access-link IP fragmentation involves the following steps:

- Configuring Global Level Access-Link IP Fragmentation
- Configuring APN Level Access-Link IP Fragmentation
- Configuring Access-Link Fastpath to Enforce APN MTU

Configuring Global Level Access-Link IP Fragmentation

Use the following configuration to configure the access-link IP fragmentation in the Global configuration mode:

```
configure
  [ default ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
  end
```

NOTES:

- **access-link ip-fragmentation**: Configures the access-link IP fragmentation to the mobile node if the link MTU is smaller than the packet length.
- **df-fragment-and-icmp-notify**: Partially ignores the DF bit setting when the packet is fragmented. It also sends ICMP unreachable error to the source, even if DF bit is set for the packet.

- **df-ignore**: Ignores the DF bit setting when the packet is fragmented. This is the default value.
- **normal**: Configures the normal fragmentation process.
- **default**: The default value is set to **df-ignore**.

Configuring APN Level Access-Link IP Fragmentation

Use the following configuration to configure the access-link IP fragmentation in the APN configuration mode:

```
configure
   context context_name
      apn apn_name
         [ no ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
         end
```



Note The **no** option is introduced in the APN configuration and the **default** option is deprecated.

NOTES:

- **access-link ip-fragmentation**: Configures the access-link IP fragmentation to the mobile node if the link MTU is smaller than the packet length.
- **df-fragment-and-icmp-notify**: Partially ignores the DF bit setting when the packet is fragmented. It also sends ICMP unreachable error to the source, even if DF bit is set for the packet.
- **df-ignore**: Ignores the DF bit setting when the packet is fragmented.
- **normal**: Configures the normal fragmentation process.

Configuring Access-Link Fastpath to Enforce APN MTU

The downlink SGi IP packet may get fragmented before it is sent out through the GTP tunnel. The packet is not fragmented, if the packet size and GTP tunnel encapsulation is smaller than or equal to the APN MTU size. If the packet size and GTP tunnel encapsulation are bigger than the APN MTU size, then the packet is fragmented before it is sent through the GTP tunnel. The packet is fragmented either in the inner or outer packet. The global-level configuration enforces the VPP enabled platform to perform outer packet fragmentation upon receiving the nonfragmented packets.

Use the following configuration to access-link fastpath to enforce APN MTU for IPv4 traffic:

```
configure
   [ no ] access-link fastpath apn-ppp-mtu-enforce
   end
```

NOTES:

- **access-link fastpath apn-ppp-mtu-enforce**: Enforces the APN MTU to VPP-based fastpath IPv4 data streams.

Note After configuration, the newly created bearers are set to the newly configured value. However, the ongoing bearer traffic does not get affected due to this configuration. The **access-link fastpath apn-ppp-mtu-enforce** is disabled by default and is not supported in the VPC-DI platform.

Monitoring and Troubleshooting

This section provides information regarding show commands and their outputs.

Show Commands and Output

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

show configuration access-link

The output of this command displays the following field.

Field	Description
access-link ip-fragmentation normal	Displays the respective value, if configured at Global level. If the configuration is set to **default** or **df-ignore** then, no output is displayed.

show configuration access-link verbose

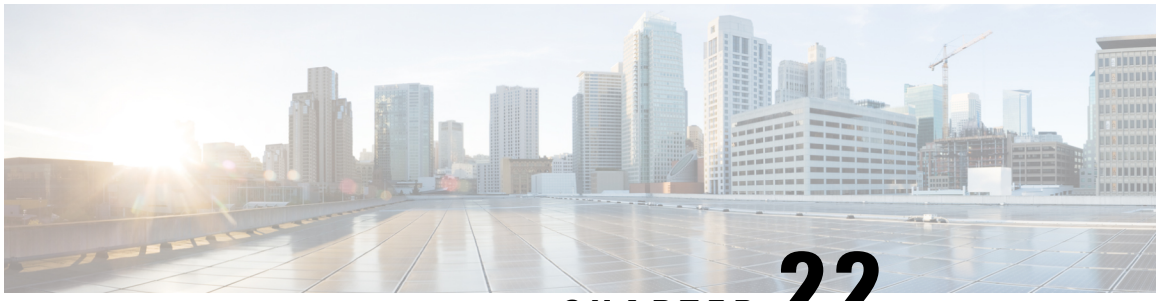
The output of this command displays the following field.

Field	Description
access-link ip-fragmentation df-ignore	Displays the respective value, if configured at Global level. If the configuration is set to **default** or **df-ignore** then, df-ignore is displayed.

show config apn <apn_name>

The output of this command displays the following field.

Field	Description
access-link ip-frag: df-ignore (APN-Configured: False)	Displays the application logic applied to the APN. APN-Configured confirms if the application logic is derived from the APN (True) or from the Global level (False).



CHAPTER 22

Diamproxy Peer Connection Status Audit

- Feature Summary and Revision History, on page 397
- Feature Description, on page 397
- How It Works, on page 398
- Configuring Diamproxy Peer Connection Status Audit, on page 398

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

The TCP connections between the Diameter proxy (Diamproxy) and the configured peers for different endpoints can either be in Open or Closed state. The state of these TCP connections for every peer (or endpoints) is maintained at the Diamproxy and the clients (sessmgrs/aaamgrs), for enabling communication with these peers through the Diamproxy. If the connection status of sessmgrs/aaamgrs is IDLE and the Diamproxy is in

OPEN state, then the Diameter messaging failures, resulting in call failures, can be seen. This is the primary reason an audit mechanism and auto-correction is required and useful.

Due to network conditions, the connection state can change randomly. If this change is not communicated appropriately, it can result in discrepancies regarding connection state at the clients. Similarly, when a new peer is configured, the clients initiates PIN Peer messages to Diamproxy to notify the new peer configuration. Due to the throttling done at the Diamproxy, some of the PIN Peer messages get dropped. This can also result in discrepancies in connection state at the clients.

This feature helps in auto-detecting, and correcting these discrepancies by Peer Connection Status Audit mechanism between the Diamproxy and Diabase clients. The Diamproxy periodically publishes current connection status of Diameter peers across all endpoints to the registered Diabase clients (sessmgr/aaamgr tasks). The Diabase client audits the current connection status and takes corrective action if there is any discrepancy in connection status.

How It Works

Following is a brief overview of how this feature works:

1. The Diamproxy initiates endpoint peer connection status audit process with sessmgr and aaamgr.
2. If there is any discrepancy in peer connection status, then the sessmgr and aaamgr initiate an auto-corrective action.
3. Any discrepancy in peer connection status between Diamproxy and sessmgr/aaamgr gets corrected within pre-defined time interval.
4. After any type of recovery event and peer connection status audit process, there is no race condition between peer connection status reconciliation during startup.

The Audit is delayed by 3 minutes for connection stabilization when any of the following events occur:

1. Diamproxy tasks starts.
2. Diamproxy task restarts.
3. ICSR switchover -> Chassis state moves from Standby to Active.
4. Planned card migration -> Start AUDIT 3 minutes from migration end time.
5. Unplanned card migration -> Same as Diamproxy task restart.

Configuring Diamproxy Peer Connection Status Audit

This section provides information about CLI commands available in support of the feature.

Enabling Connection Status Audit Interval

Use the following CLI commands under Global Configuration Mode to enable the connection status audit interval:

```
configure
  diameter-proxy conn-audit interval audit_interval
  exit
```

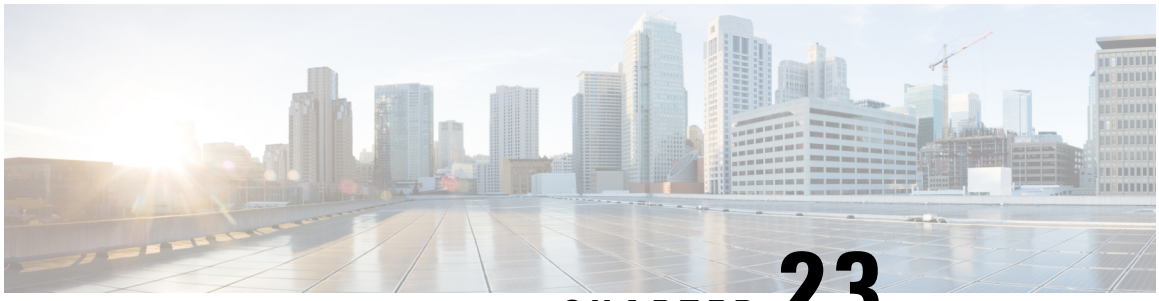
Notes:

- **diameter-proxy**: Specifies the Diamproxy related configurations.
- **conn-audit**: Specifies the periodic connection status audit processes. Disabled by default.
- **interval** *audit_interval*: Specifies the connection status audit interval in minutes in the range of 1 through 10. Recommended value is 2 minutes.
- If previously configured, use the **default diameter-proxy conn-audit** CLI command to disable Diamproxy Peer Connection Status Audit with Diabase clients.
- Enabling Diamproxy Peer Connection Status Audit with Diabase clients might affect performance of the services using Diameter interface.

Verifying the Diamproxy Peer Connection Status Audit

Use the following CLI command to verify if the connection status is in SYNC at all Diameter peers.

- **show diameter peers full debug**



CHAPTER 23

Direct Tunnel for 4G (LTE) Networks

This chapter briefly describes support for direct tunnel (DT) functionality over an S12 interface for a 4G (LTE) network to optimize packet data traffic.

Cisco LTE devices (per 3GPP TS 23.401 v8.3.0) supporting direct tunnel include:

- Serving GPRS Support Node (S4-SGSN)
- Serving Gateway (S-GW)
- PDN Gateway (P-GW)

Important Direct Tunnel is a licensed Cisco feature. A separate feature license is required for configuration. 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 sections are included in this chapter:

- Direct Tunnel for 4G Networks - Feature Description , on page 401
- How It Works, on page 404
- Configuring Support for Direct Tunnel, on page 428
- Monitoring and Troubleshooting Direct Tunnel, on page 431

Direct Tunnel for 4G Networks - Feature Description

The amount of user plane data will increase significantly during the next few years because of High Speed Packet Access (HSPA) and IP Multimedia Subsystem technologies. Direct tunneling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates.

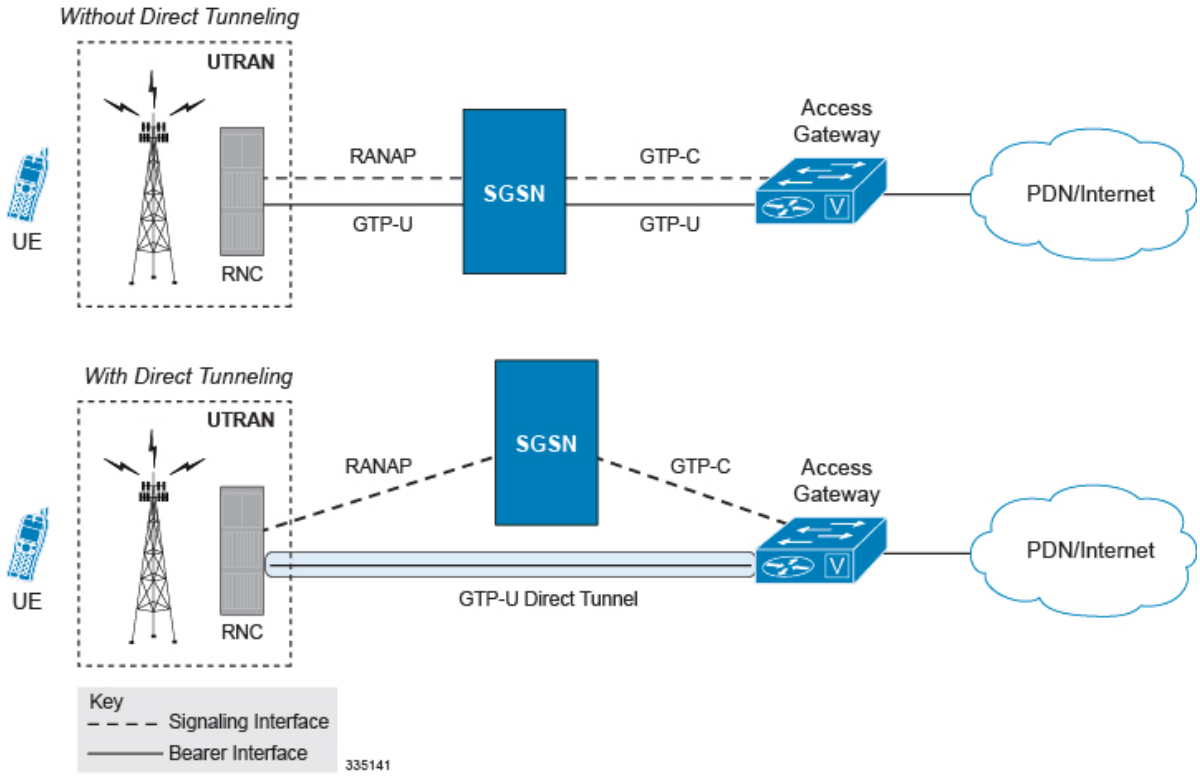
Direct Tunnel (DT) offers a solution that optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

Important Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. 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 Establishment of a direct tunnel is controlled by the SGSN; for 4G networks this requires an S4 license-enabled SGSN setup and configured as an S4-SGSN.

Once a direct tunnel is established, the S4-SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

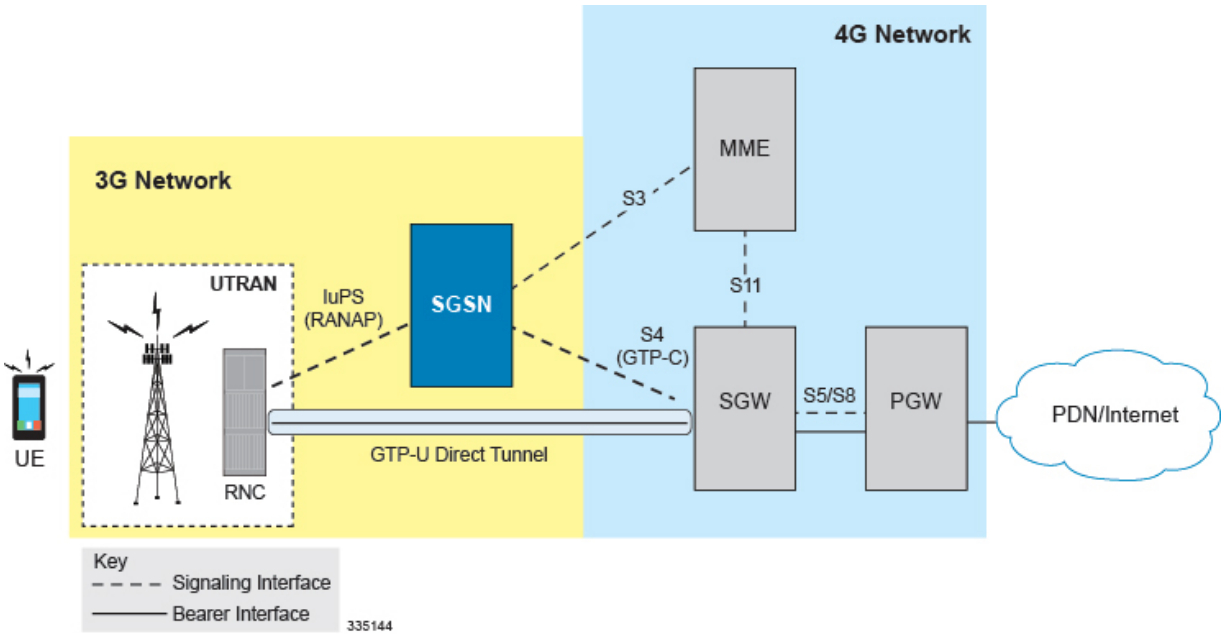
Figure 17: GTP-U Direct Tunneling



A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the S4-SGSN/S-GW to handle the user plane processing.

A direct tunnel is achieved upon PDP context activation when the S4-SGSN establishes a user plane tunnel (GTP-U tunnel) directly between the RNC and the S-GW over an S12 interface, using a Create Bearer Response or Modify Bearer Request towards the S-GW.

Figure 18: Direct Tunneling - LTE Network, S12 Interface



A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

S4-SGSN supports establishment of a GTP-U direct tunnel between an RNC and the S-GW under the scenarios listed below:

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without S-GW change
- Intra SGSN Routing Area Update with S-GW change
- Intra SGSN SRNS relocation without S-GW change
- Intra SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation without S-GW relocation
- E-UTRAN-to-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- UTRAN-to-E-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- Network Initiated PDP Activation

Scenarios that vary at S4-SGSN when direct tunneling is enabled, as compared to DT on a 2G or 3G SGSN using the Gn interface, include:

- RAB Release
- Iu Release
- Error Indication from RNC

- Downlink Data Notification from S-GW
- Downlink Data Error Indication from S-GW
- MS Initiated PDP Modification
- P-GW Initiated PDP Modification while the UE is IDLE
- HLR/HSS Initiated PDP Modification
- Session Recovery with Direct Tunnel

The above scenarios exhibit procedural differences in S4-SGSN when a direct tunnel is established.

How It Works

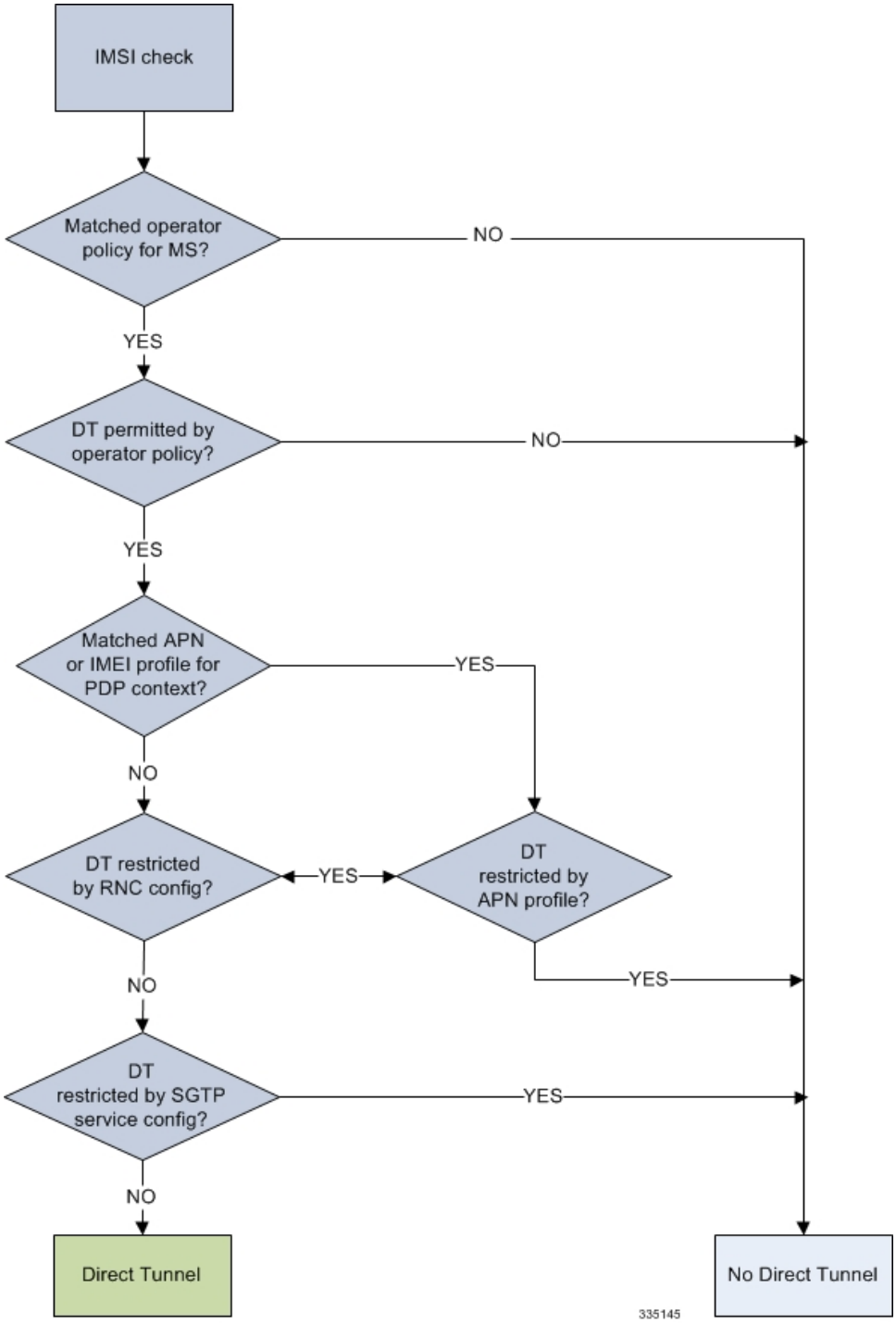
DT functionality enables direct user plane tunnel between RNC and SGW within the PS domain. With direct tunneling the S4-SGSN provides the RNC with the TEID and user plane address of the S-GW, and also provides the S-GW with the TEID and user plane address of the RNC.

The SGSN handles the control plane signaling and makes the decision when to establish the direct tunnel between RNC and S-GW, or use two tunnels for this purpose (based on configuration).

DT Establishment Logic

The following figure illustrates the logic used within the S4-SGSN/S-GW to determine if a direct tunnel will be setup.

Figure 19: Direct Tunneling - Establishment Logic



Establishment of Direct Tunnel

The S4-SGSN uses the S12 interface for DT.

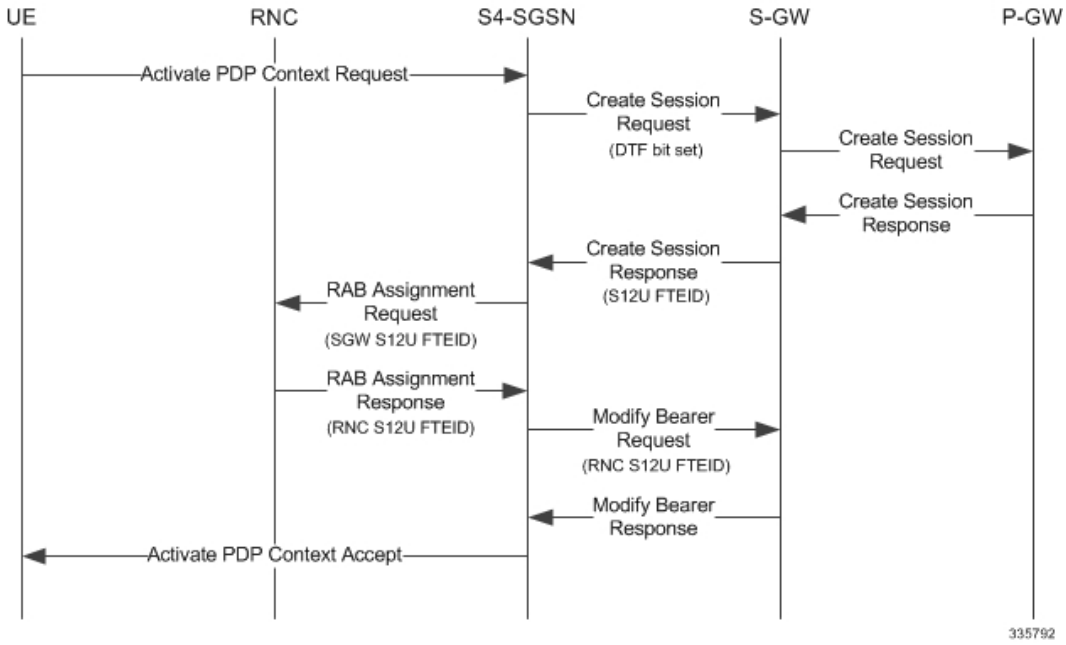
Direct Tunnel Activation for Primary PDP Context

For the PDP Context Activation procedure this solution uses new information elements (IEs) for the GPRS Tunnelling Protocol v2 (GTPv2) as defined in TS 29.274. SGSN provides the user plane addresses for RNC and S-GW as S12U FTEIDs as illustrated in the figure below.

The sequence for establishing a direct tunnel between the RNC and S-GW during PDP activation is as follows:

- SGSN sends a Create Session Request to the S-GW with the indication flag DTF (direct tunnel flag) bit set
- In its Create Session Response, the S-GW sends the SGSN an S12U FTEID (Fully Qualified Tunnel Endpoint Identifier).
- The SGSN forwards the S-GW S12U to the RNC during the RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends the SGSN its transport address and Tunnel Endpoint ID (TEID).
- The SGSN forward the RNC S12 U FTEID o the S-GW via a Modify Bearer Request.

Figure 20: Primary PDP Activation with Direct Tunnel

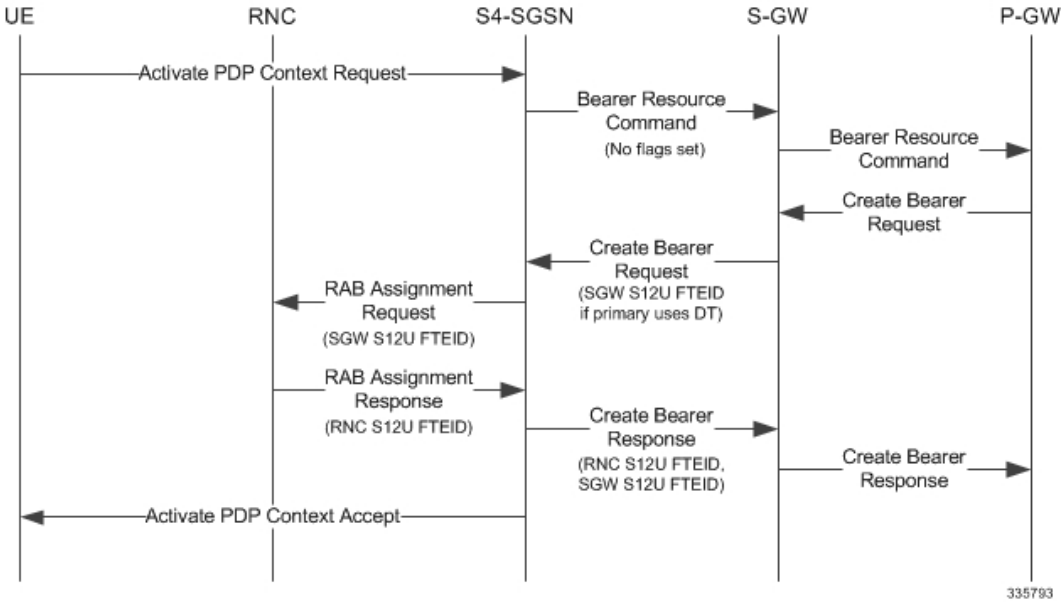


Direct Tunnel Activation for UE Initiated Secondary PDP Context

The following is the general sequence for establishing a direct tunnel for a Secondary PDP Context Activation:

- The SGSN sends a Bearer Resource Command to the S-GW with no flags set. (S-GW already knows Direct Tunnel is enabled for primary.)
- The S-GW sends a Create Bearer Response that includes the S12U FTEID to the SGSN.
- The SGSN forwards the S-GW S12U to RNC via a RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends its transport address and TEID to the SGSN.
- The SGSN forwards the S12U TEID received from the RNC to the S-GW via a Create Bearer Response.

Figure 21: Secondary PDP Activation with Direct Tunnel



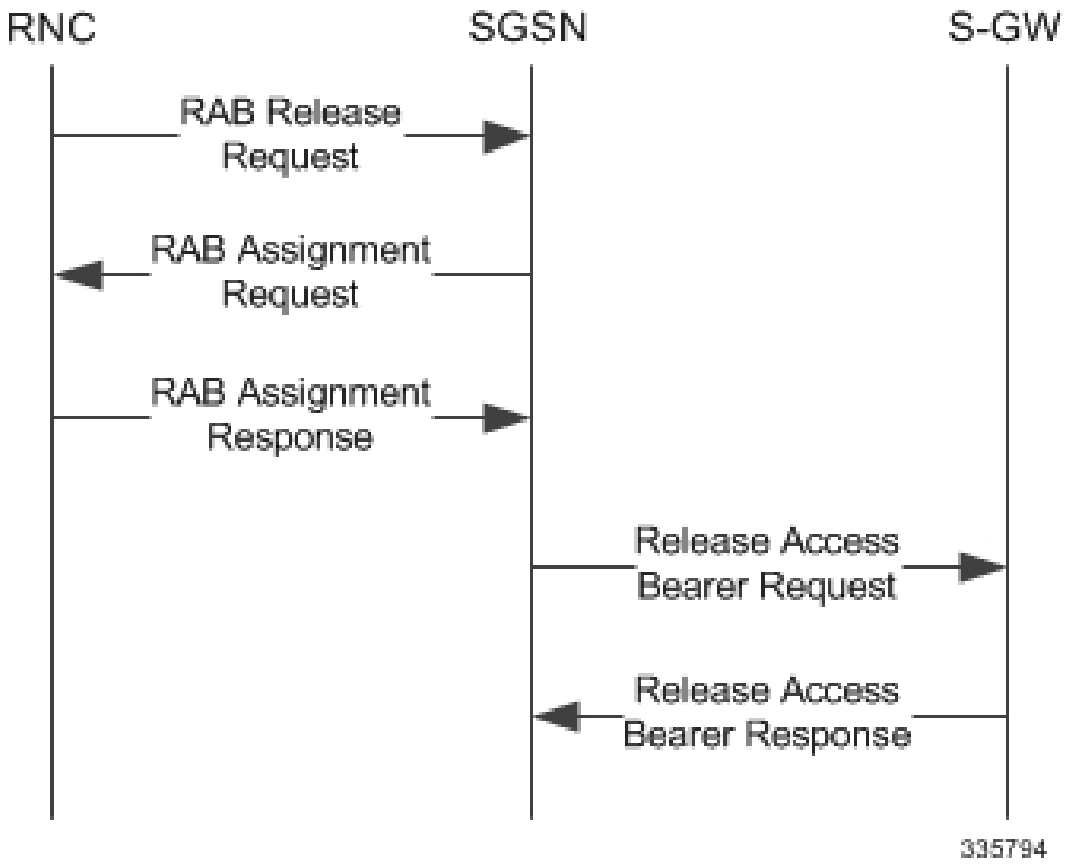
RAB Release with Direct Tunnel

If the SGSN receives a RAB Release Request from the RNC for bearer contexts activated with Direct Tunnel, it sends a Release Access Bearer Request to the S-GW.

Upon receiving the Release Access Bearer Request, the S-GW removes the S12 U RNC FTEID. If any downlink data appears, the S-GW sends a Downlink Data Notification because it does not have a user plane FTEID with which to forward data.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming/conversational bearers upon RAB release.

Figure 22: RAB Release Procedure with Direct Tunnel



Important Operators should not use conversational or streaming class bearers in S4-SGSN.

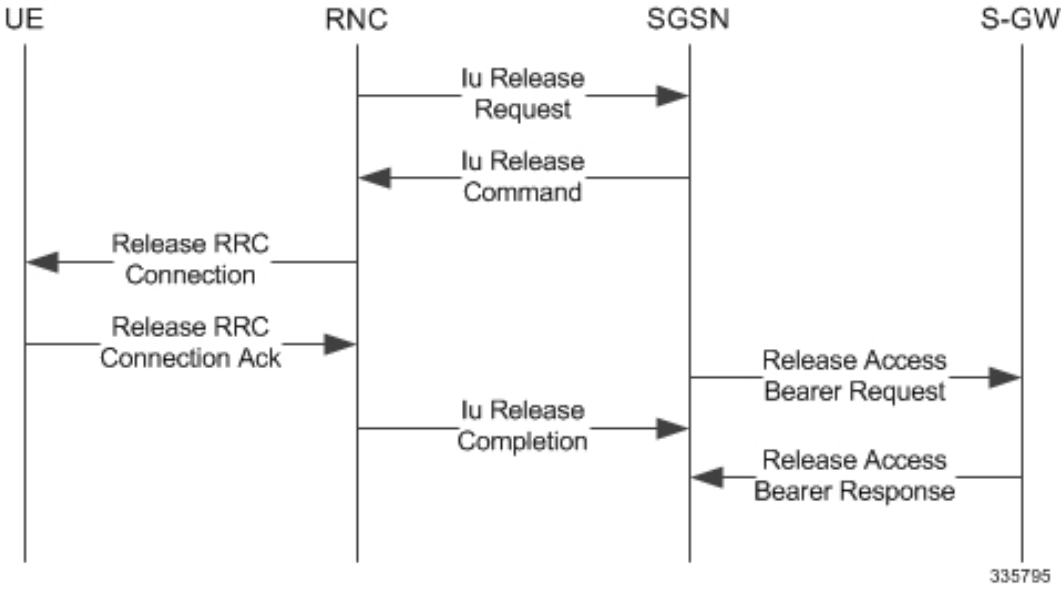
Iu Release with Direct Tunnel

If the SGSN receives an Iu Release and bearers are activated with direct tunneling, it sends a Release Access Bearer Request to the S-GW.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming or conversational bearers upon Iu release.

Important Operators should not use conversational or streaming class bearers in S4-SGSN.

Figure 23: Iu Release Procedure with Direct Tunnel

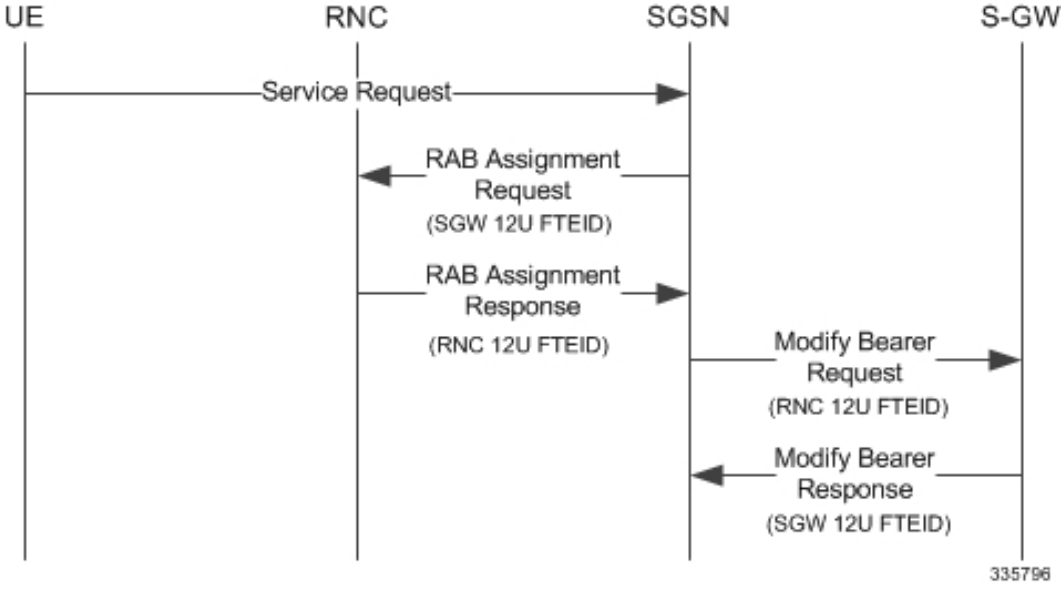


Service Request with Direct Tunnel

When a UE is Idle and wants to establish a data or signaling connection, it sends a Service Request for data. Alternatively a UE can also send a Service Request to the SGSN when it is paged by the SGSN.

Upon receiving a Service Request for data, the SGSN establishes RABs and sends a Modify Bearer Request to the S-GW with the 12U FTEID received from the RNC.

Figure 24: Service Request Procedure with Direct Tunnel



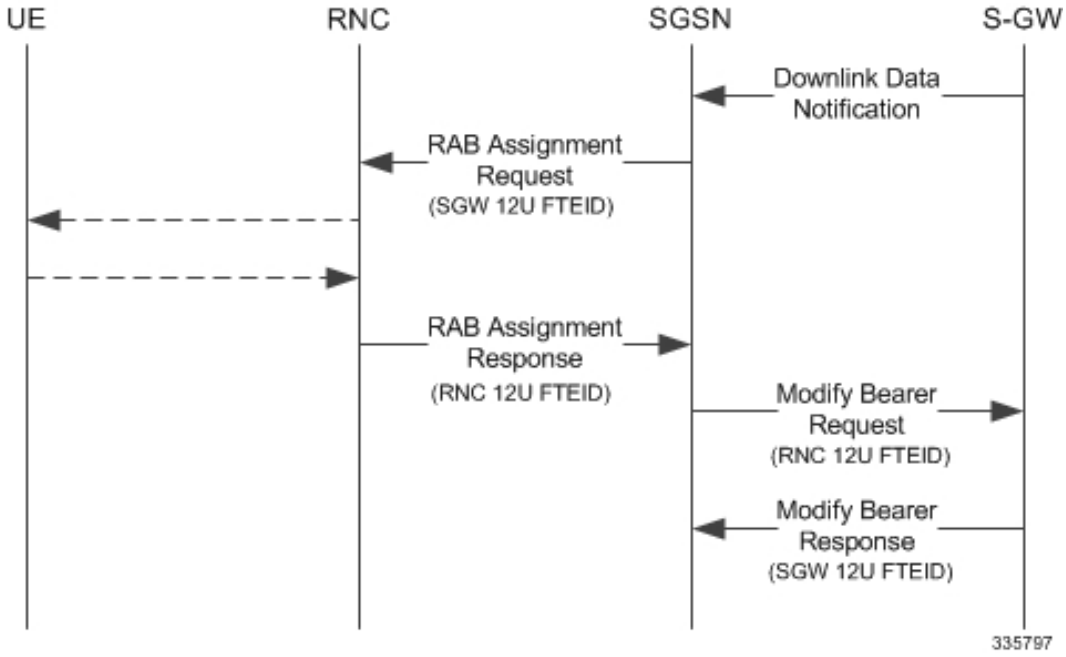
Downlink Data Notification with Direct Tunnel when UE in Connected State

When RABs are released (but UE retains an Iu connection with the SGSN), the SGSN notifies the S-GW to release the RNC side TEIDs via a Release Access Bearer Request.

If the S-GW receives any downlink GTPU data from the P-GW after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification message from the S-GW.

If the Downlink Data Notification is received from the S-GW, all of the missing RABs are established and a Modify Bearer Request is sent to the S-GW with the RNC S12U FTEID

Figure 25: Downlink Data Notification with Direct Tunnel

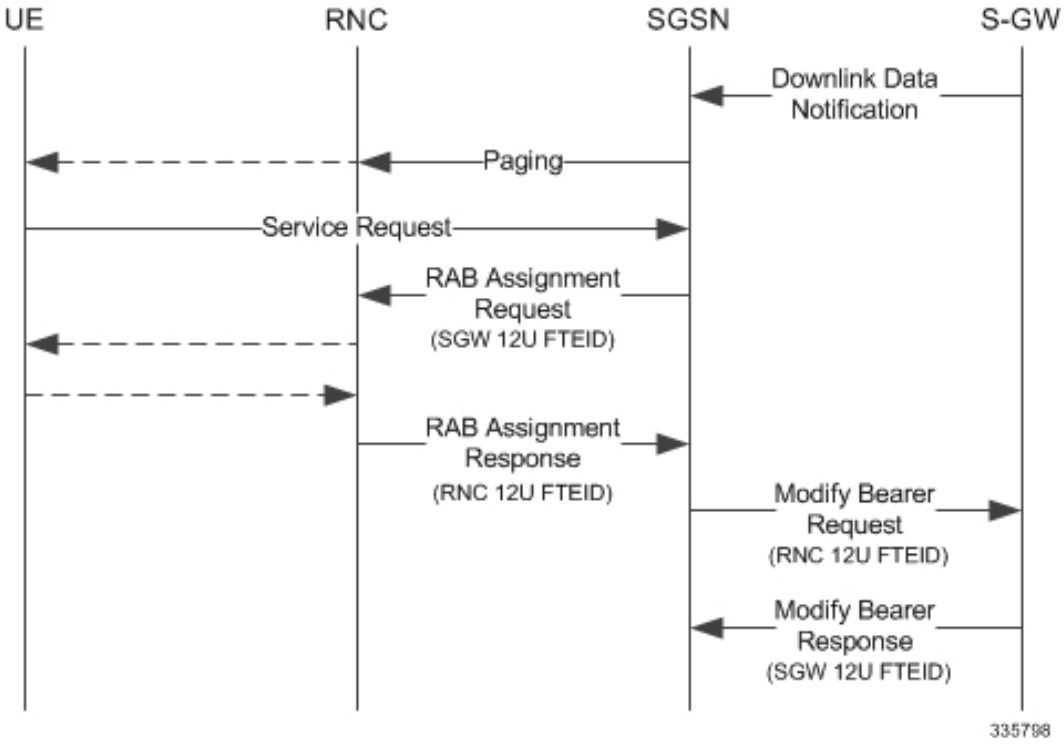


Downlink Data Notification with Direct Tunnel when UE in Idle State

When an Iu is released the UE goes IDLE. The SGSN informs the S-GW to release the RNC side TEIDs by sending a Release Access Bearer Request. After this point if the S-GW receives any downlink GTPU data from the P-GW, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data.

If the S-GW receives any downlink GTPU data after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification from the S-GW. If a Downlink Data Notification is received from S-GW when the UE is idle, the SGSN pages the UE before establishing the RABs. The SGSN sends a Modify Bearer Request to the S-GW with the RNC S12U FTEID.

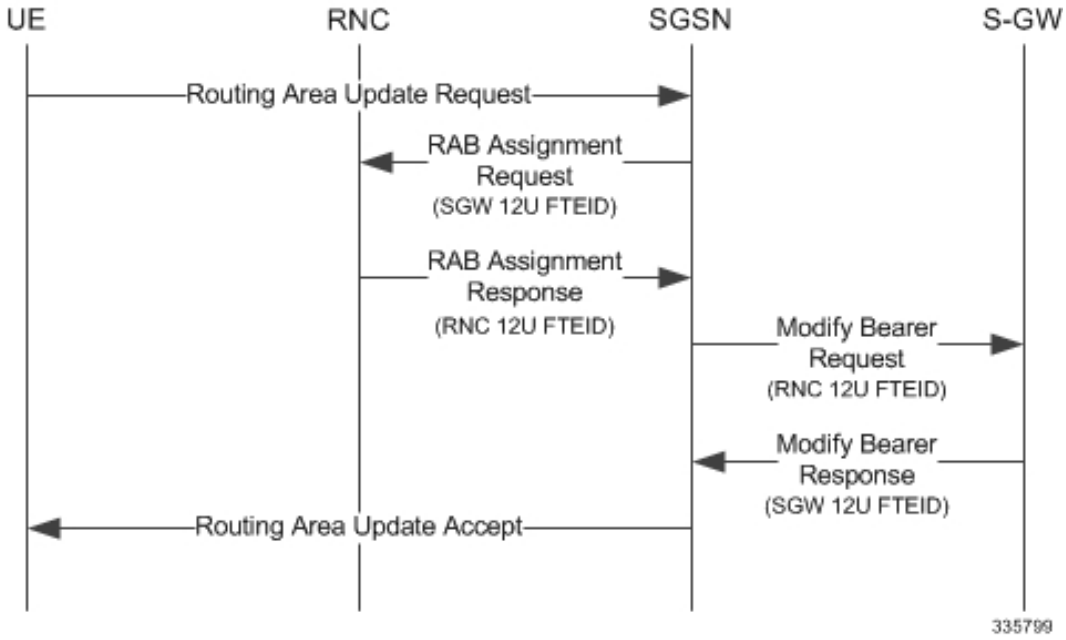
Figure 26: Downlink Data Notification when UE in Idle State



Intra SGSN Routing Area Update without SGW Change

For a Routing Area Update without an S-GW change with Direct Tunnel, the SGSN sends a Modify Bearer Request to the S-GW with the RNC FTEID. The SGSN will establish RABs with the target RNC only if the RABs were present with the source RNC.

Figure 27: Routing Area Update Procedure without SGW Change



The table below includes detailed behaviors for a Routing Area Update without S-GW change.

Table 40: Routing Area Update without S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs that are be modified and the rest released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	Yes	Supported	No	No RAB establishmen with new RNC. MBR is sent with only PLMN change. Beare Context will not carry any TEID.
Intra RAU	Present	No RAB	Supported	Yes	Supported	No	Same as above.
Intra RAU	Not Present	No RAB	Not Supported	No	Supported	No	No RAB establishmen with new RNC. Modify Bearer Request to S-GW witl DTF set and no user FTEID.
Intra RAU	Present	No RAB	Not Supported	No	Supported	No	Same as above.
Intra RAU	Present	Some RABs	Not Supported	Do not care	Supported	No	Only the present RAB are established. MBR sent to S-GW with the bearers with RABs to be modified and the rest to be released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.Modify Bearer.
Intra RAU	Not Present	No RAB	Not Supported	Yes	Supported	No	No RAB establishmen with new RNC. MBR is sent with only PLMN change. SGSN will page / Service rec / establish RABs when a downlink data notification is received.
Intra RAU	Present	No RAB	Not Supported	Yes	Supported	No	Same as above.
Intra RAU: New RNC does not support Direct Tunnel. No SGW relocation							

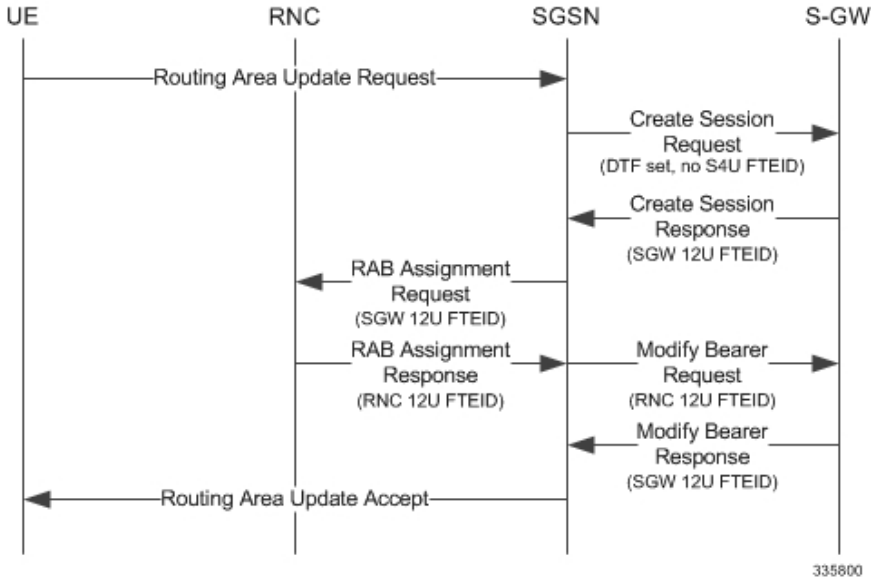
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	No	No RAB establishment with new RNC. SGSN sends Modify Bearer Request to S-GW with S4U TEID. If there is change in PLMN ID, then new PLMN ID will be carried.
Intra RAU	Present	No RAB	Supported	Do not care	No Supported	No	Same as above.
Intra RAU	Present	Some RABs	Supported	Do not care	Not supported	No	Only the present RABs are established. MBR sent to S-GW with all bearers having S4U TEID. If there is change in PLMN ID, the new PLMN ID will be carried.

Routing Area Update with S-GW Change

In a Routing Area Update with an S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. In its Create Session Response,. the S-GW sends an S12U FTEID which is forwarded to the RNC via a RAB Assignment Request.

The SGSN sends the RNC FTEID received in the RAB Assignment Response to the S-GW in a Modify Bearer Request. There are many scenarios to consider during Intra SGSN RAU.

Figure 28: Routing Area Update Procedure with SGW Change



The table below includes detailed behaviors for a Routing Area Update with S-GW change.

Table 41: Routing Area Update with S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU: Both RNCs support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW will send its S12U TEID that SGSN stores as part of DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN will get DDN and establish RABs and send MBR.
Intra RAU	Present	No RAB	Supported	Do not care	Supported	Yes	Same as above.
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC. MBR will be initiated only with those RABs that are present rest of bearers to be removed
Intra RAU: Old RNC does not support Direct Tunnel. SGW relocation							

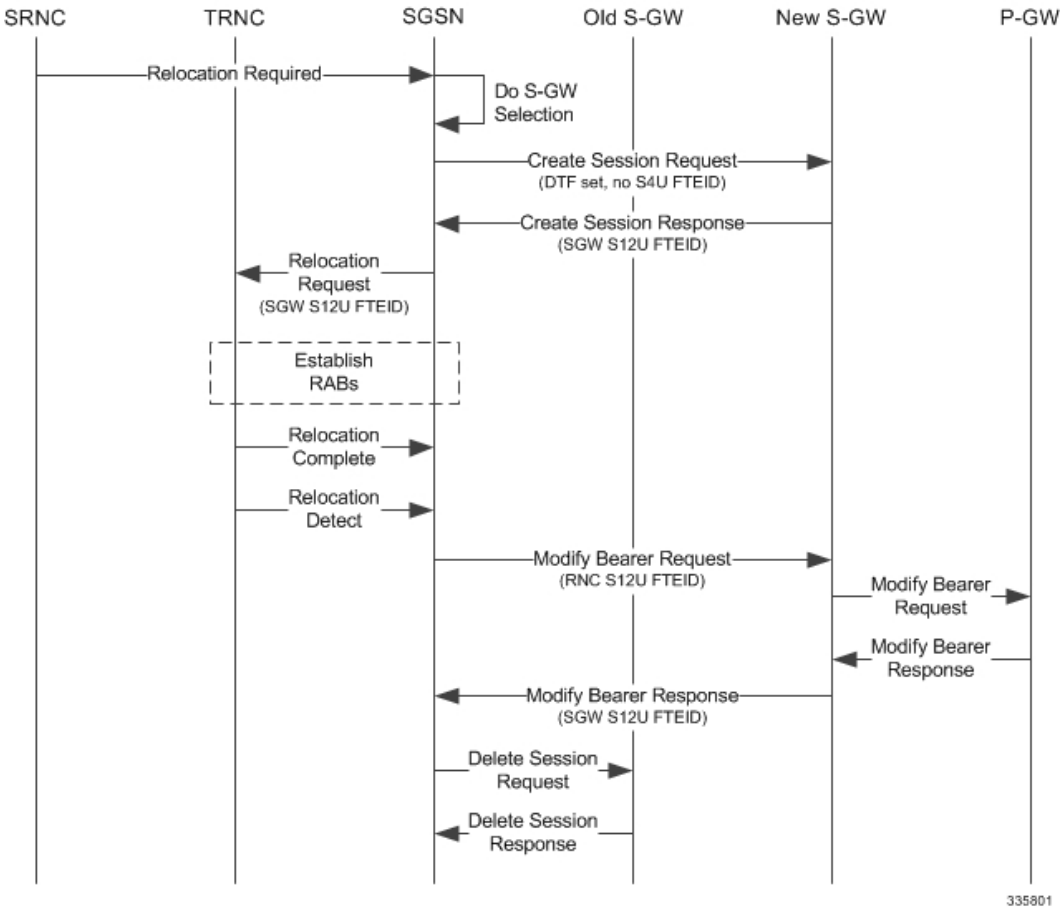
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID that SGSN stores as part of our DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN gets DDN and establishes RABs and sends MBR.
Intra RAU	present	No RAB	Not Supported	Do not care	Supported	Yes	Same as above.
Intra RAU	Present	Some RABs	Not SUpported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC and MBR will be initiated only with those RABs that are present and the rest as bearers to be removed.
Intra RAU: New RNC does not support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	Some rABs	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID. No deactivation of PDPs.

Intra SRNS with S-GW Change

In Intra SRNS (Serving Radio Network Subsystem) with S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. The Create Session Response from the new S-GW contains the SGW S12U FTEID which the SGSN forwards to the Target RNC in a Relocation Request.

The SGSN sends the RNC S12U FTEID to the new S-GW in a Modify Bearer Request.

Figure 29: Intra SRNS with S-GW Change

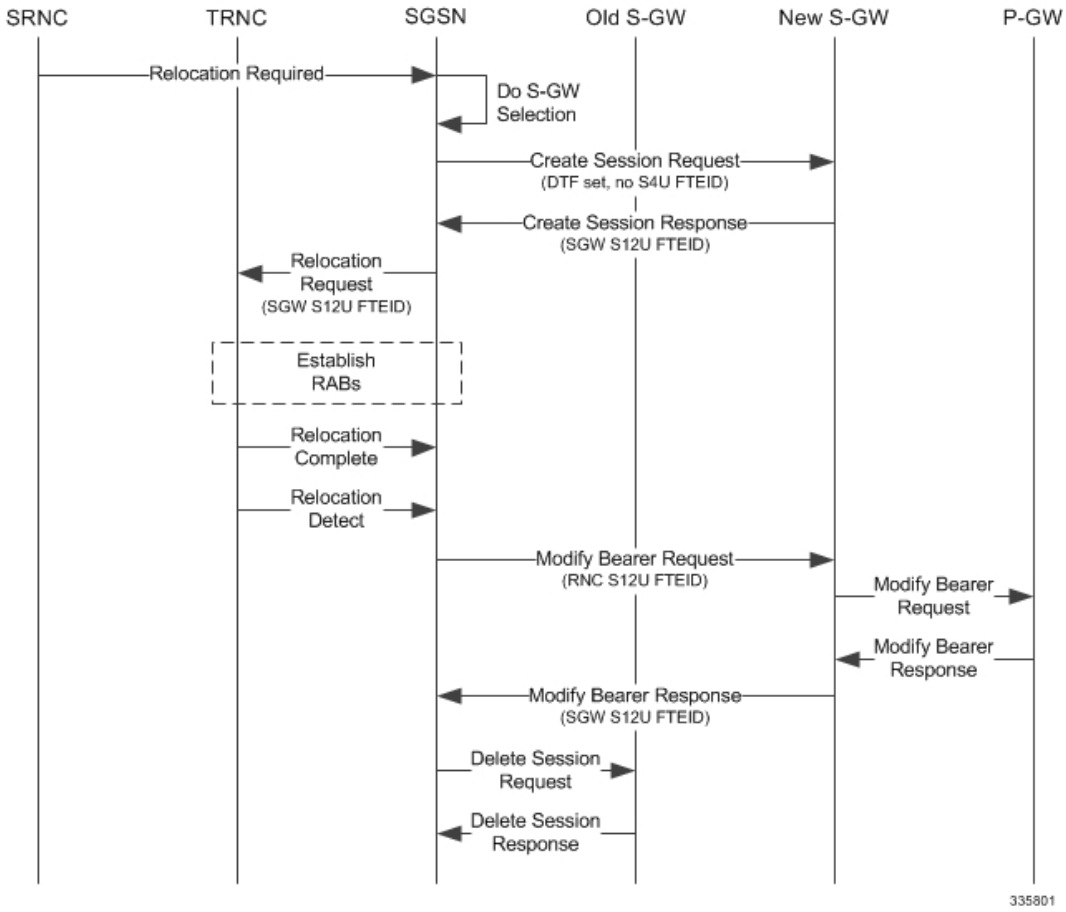


The table below includes detailed behaviors for intra SRNS scenarios.

Intra SRNS without S-GW Change

In Intra SRNS without S-GW change, a Relocation Request is sent with SGW S12U FTEID. The RNC S12U FTEID received is forwarded to the S-GW in a Modify Bearer Request.

Figure 30: Intra SRNS without S-GW Change



The table below includes detailed behaviors for intra SRNS scenarios.

Table 42: Intra SRNS Behaviors

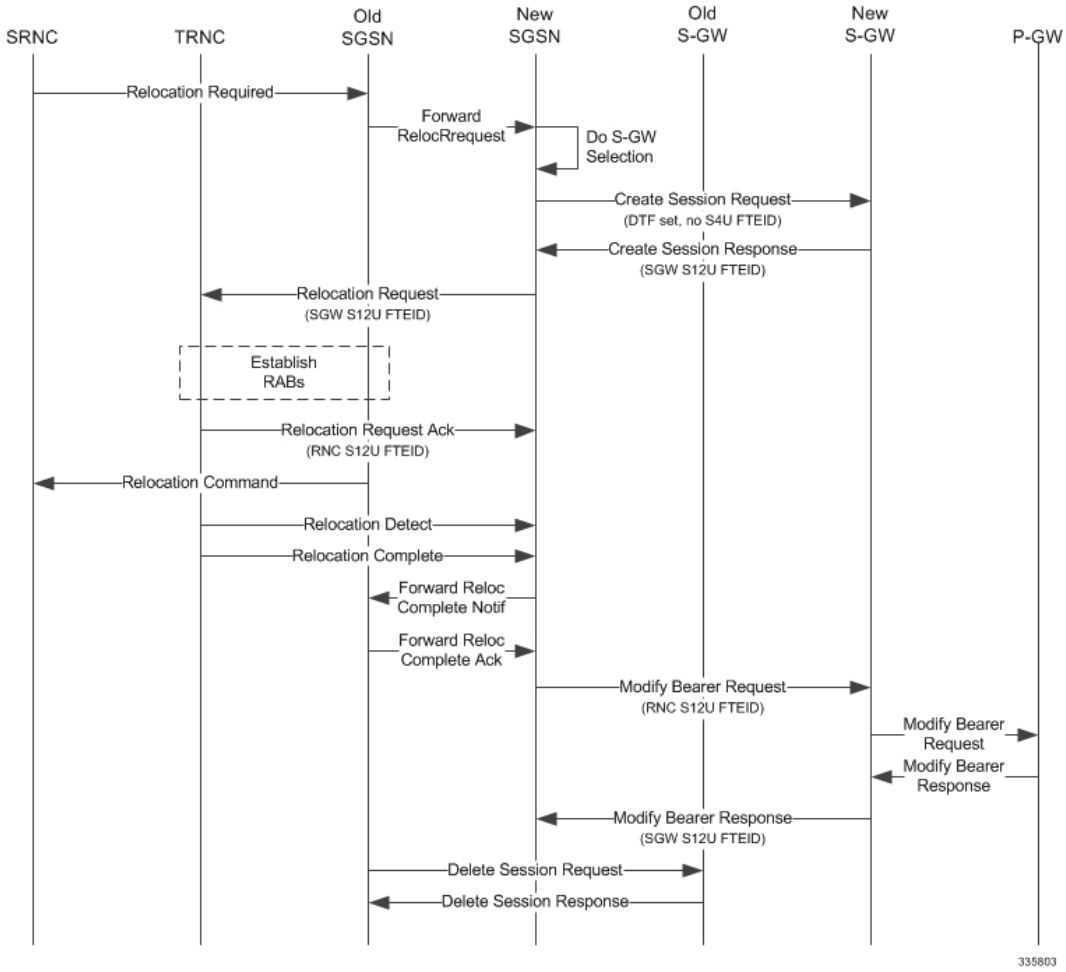
Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12 U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Supported	Not Supported	No	Relocation Request to Target RNC is sent with SGSN S4 U FTEID. Modify Bearer Request to S-GW is sent with SGSN S4 U FTEID
Not Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.

Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Not Supported	Supported	Yes	Create Session Request to new S-GW is sent with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response SGSN internally treats that as an S12U FTEID and continues the relocation. Relocation Request to Target RNC is sent with S12 U FTEID received in Create Session Response. Modify Bearer Request to new S-GW is sent with RNC S12U FTEID
Supported	Not Supported	Yes	Create Session Request to new SGW is sent with S4 U FTEID. Relocation Request to Target RNC is sent with SGSN U FTEID.Modify Bearer Request is sent with SGSN S4U FTEID.
Supported	Supported	Yes	SGSN sends a Create Session Request to new SGW with DTF flag set and no user plane FTEID.Even if S-GW sent S4U FTEID in CSR Response, SGSN will internally treat that as S12U FTEID and continue the relocation. Relocation Request to the Target RNC is sent with the S12 U FTEID received in the Create Session Response. Modify Bearer Request to new S-GW is sent with RNC U FTEID.

New SRNS with S-GW Change and Direct Data Transfer

The new SGSN sends a Create Session Request with DTF flag set and no user plane FTEID to the new S-GW. The new SGSN sends the SGW S12U FTEID received in the Create Session Response in Relocation Request to the Target RNC. The new SGSN sends the RNC S12U FTEID received in a Relocation Request Ack to the new S-GW in a Modify Bearer Request.

Figure 31: New SRNS with S-GW Change with Data Transfer

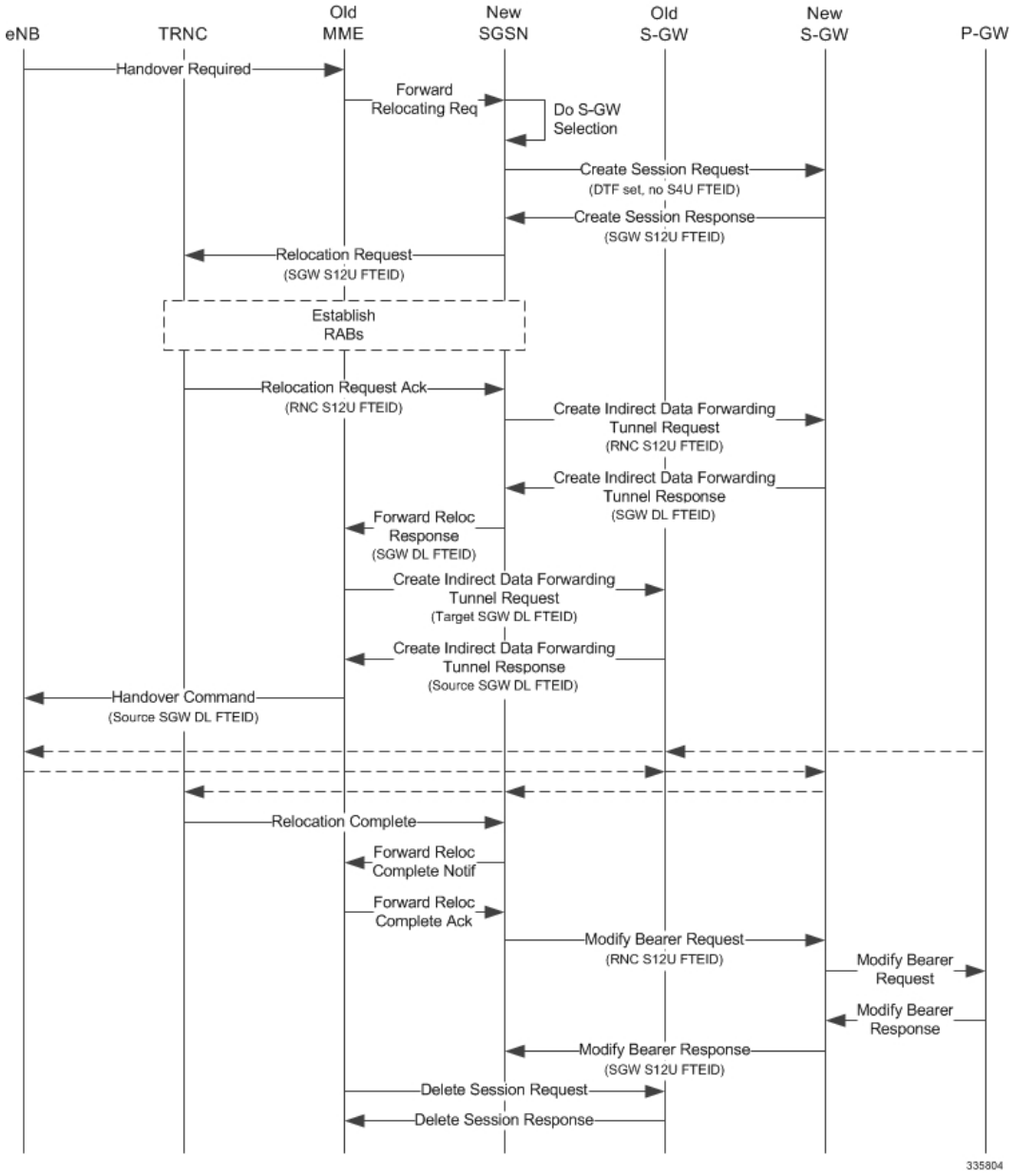


The table below includes detailed behaviors for New SRNS scenarios.

New SRNS with S-GW Change and Indirect Data Transfer

Indirect Data Transfer (IDFT) during a new SGSN SRNS happens during E-UTRAN-to-UTRAN connected mode IRAT handover. See the figure below for a detailed call flow.

Figure 32: New SRNS with S-GW Change and Indirect Data Transfer



The table below includes detailed behaviors for New SRNS scenarios.

Table 43: New SRNS Behaviors

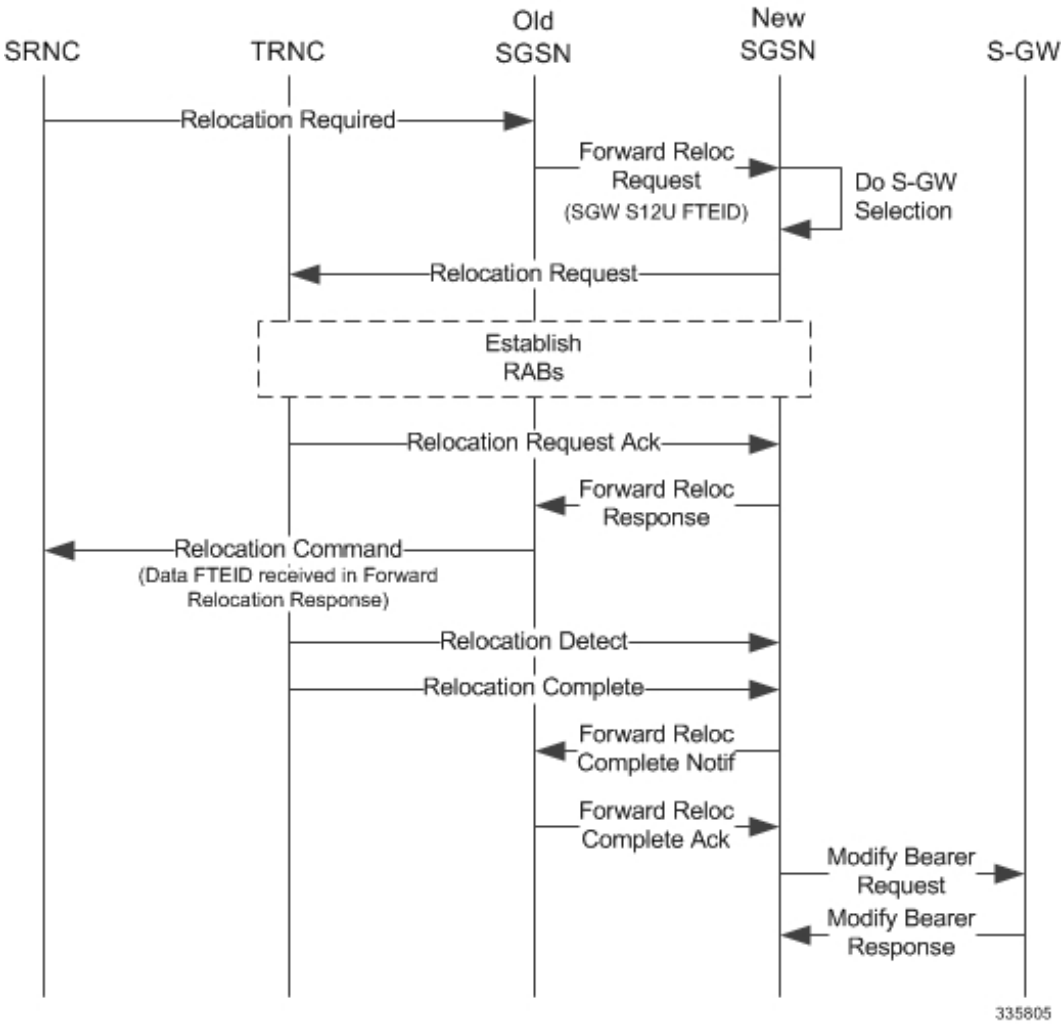
Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. SGSN includes RNC U FTEID in Forward Relocation Response. RNC U FTEID is also sen in Modify Bearer Request with DTF flag set.

Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	Yes	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. In Forward Relocation Response RNC U FTEID is included. And in Modify Bearer Request RNC U FTEID is sent and DTF flag is set.
Supported	No	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent is SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. Create Indirect Data Forwarding Tunnel Request is sent with RNC FTEID received in Relocation Request Acknowledge.In Forward Relocation Response SGW DL U FTEID received in Create IDFT response is sent. Modify Bearer Request is send with DTF set and RNC U FTEID.
Supported	Yes	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. In Forward Relocation Response RNC FTEID is sent and Modify Bearer Request is sent with DTF flag set and RNC U FTEID

Old SRNS with Direct Data Transfer

This scenario includes SRNS relocation between two SGSNs and hence IDFT is not applicable. Data will be forwarded between the source and target RNCs directly. Forward Relocation Request is sent with S12U FTEID.

Figure 33: Old SRNS with Direct Data Transfer



The table below includes detailed behaviors for Old SRNS.

Old SRNS with Indirect Data Transfer

Indirect Data Transfer (IDFT) during Old SGSN SRNS happens during UTRAN-to-E-UTRAN connected mode IRAT handover. A Forward Relocation Request is sent with SGW S12U FTEID.

Figure 34: Old SRNS with Indirect Data Transfer 4

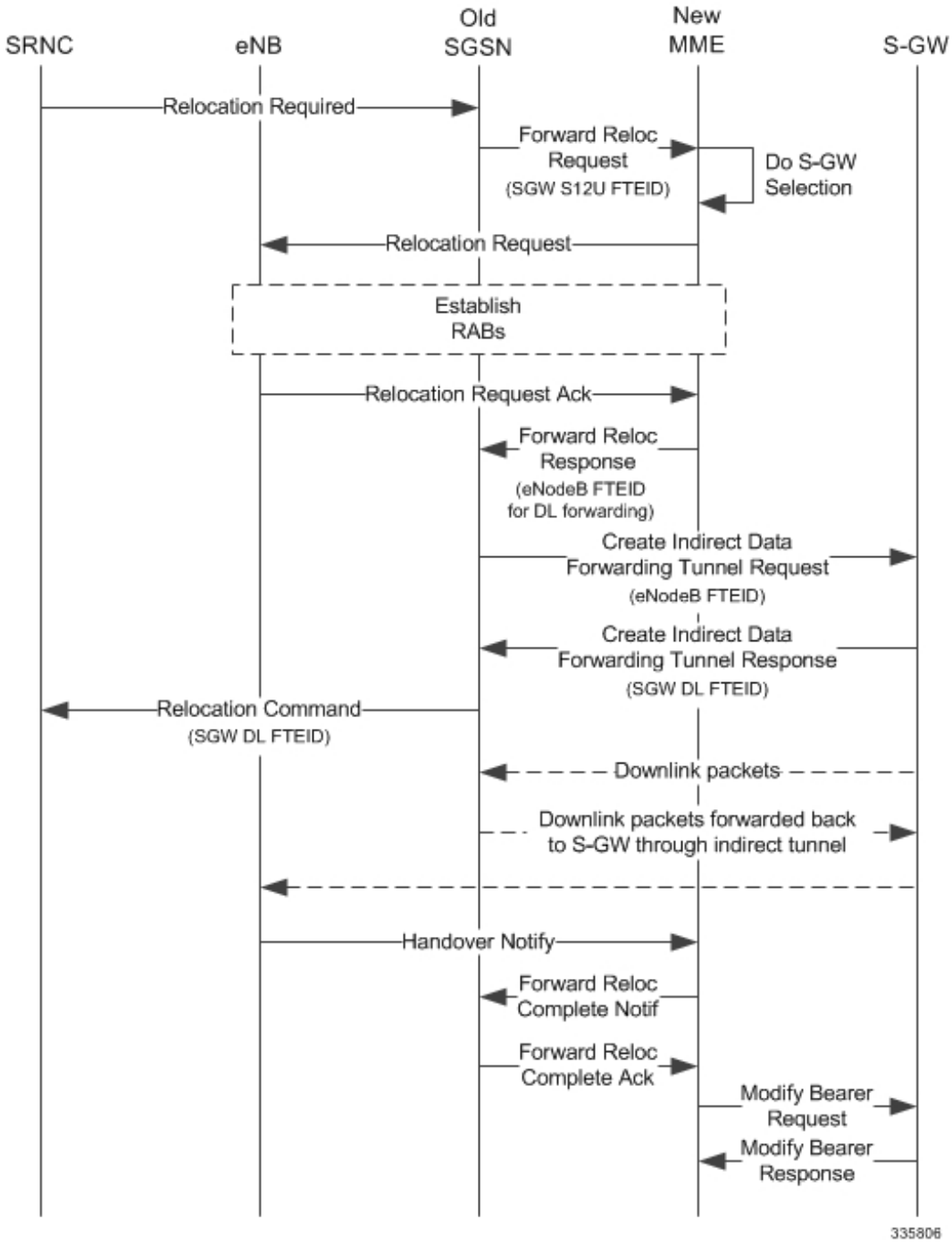


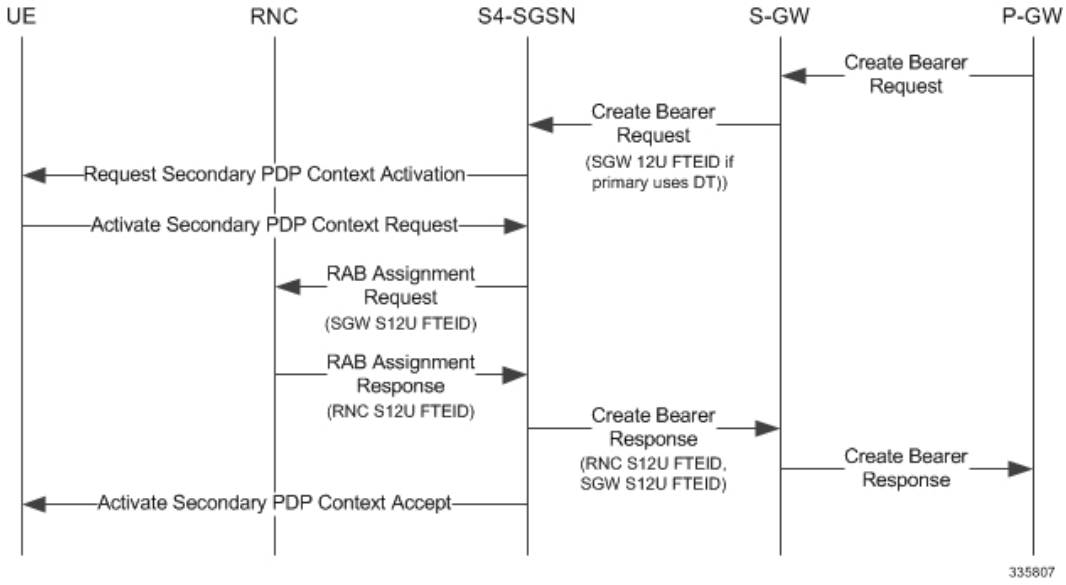
Table 44: Old SRNS Behaviors

Source RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Forward Relocation Request is send with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then a Create Indirect Data Forwarding Tunnel Request is sent with Use plane FTEID received in the Forward Relocation Response This will be the eNB user plane FTEID. The SGW DL forwarding user plane FTEID received in the Create Indirec Data Forwarding Tunnel Response is sent in the Relocatio Command.
Supported	Yes	No	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC user plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.
Supported	No	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then Create Indirect Data Forwarding Tunnel Request is sent with eNE User plane FTEID received in the Forward Relocation Response. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.
Supported	Yes	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC use plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.

Network Initiated Secondary PDP Context Activation

The S-GW sends a Create Bearer Request for Network Initiated Secondary PDP Context Activation with the SGW S12U FTEID. This FTEID is sent in a RAB Assignment Request to the RNC. The RNC S12U FTEID received in the RAB Assignment Response is sent to the S-GW in a Create Bearer Response.

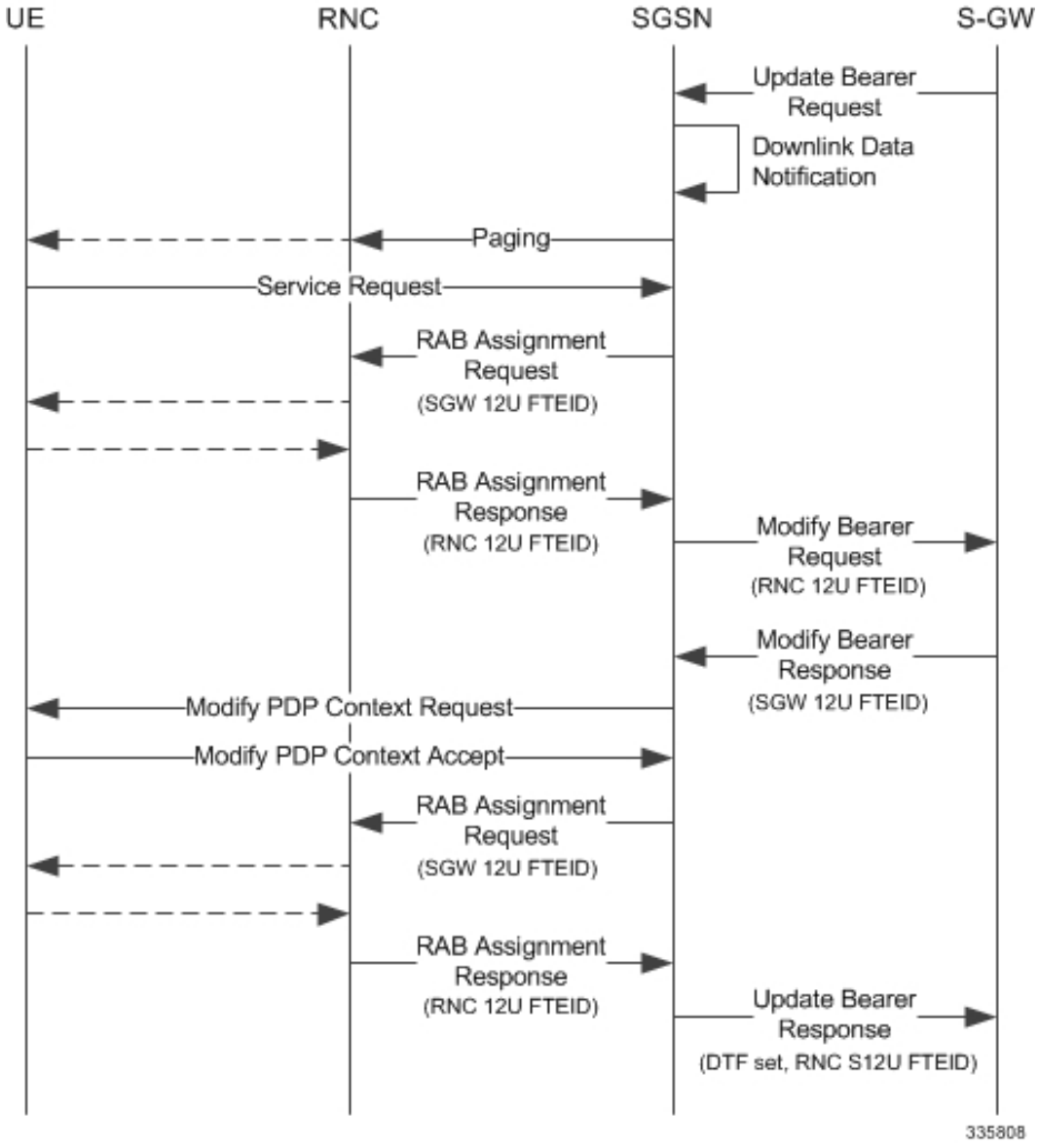
Figure 35: Network Initiated Secondary PDP Context Activation 5



PGW Init Modification when UE is Idle

If UE is in IDLE state and PGW Init Modification is received, the SGSN sends the first MBR. Upon getting PGW Init Modification in Idle State, the SGSN queues the PGW Init Modification and feeds a Downlink Data Notification internally. This sets up all RABs (using old QoS) and sends a Modify Bearer Request. When the Downlink Data Procedure is completed, the queued PGW Init Modification is processed.

Figure 36: PGW Init Modification when UE in Idle State



Limitations

During an intra RAU, intra SRNS or Service Request triggered by RAB establishment, if a few RABs fail the Modify Bearer Request the SGSN will mark those RABs as bearers to be removed. Under current specifications, it is not possible to send a Modify Bearer Request with a few bearers having S12U U-FTEIDs and a few bearers not having U-FTEIDs.

There is an ongoing CR at 3GPP to allow such Modify Bearer Requests and the S-GW should send DDN when it gets downlink data for the bearers that did not have U-FTEIDs. If this CR is approved, the SGSN will support (in a future release) sending a partial set of bearers with S12U FTEID and some bearers without any U-FTEID.

Standards Compliance

The Direct Tunnel complies with the following standards:

- 3GPP TS 23.060 version 10 sec 9.2.2 General Packet Radio Service (GPRS) Service description
- 3GPP TS 29.274 v10.5.0 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

Configuring Support for Direct Tunnel

The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN and S-GW are the only products that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

By default, direct tunnel support is

- *disallowed* on the SGSN/S-GW
- *allowed* on the GGSN/P-GW

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the operator policy named ***default***. If direct tunnel is allowed in the ***default*** operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*. For more information about the purpose and uses of operator policies, refer to the section *Operator Policy*.

Configuring Direct Tunnel on an S4-SGSN

Configuration of a GTP-U direct tunnel (DT) requires enabling DT both in a call control profile and for the RNC.



Important Direct tunneling must be enabled at both end points to allow direct tunneling for the MS/UE.

Enabling Setup of GTP-U Direct Tunnel

The SGSN determines whether a direct tunnel can be setup and by default the SGSN does not support direct tunnel. The following configuration enables a GTP-U DT in a call control profile:

```
config
  call-control-profile policy_name
    direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
    end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.

- **to-ggsn** and **to-sgw** options are added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel to RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service. Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC. By default, DT functionality is enabled for all RNCs.

The following configuration sequence enables DT to a specific RNC that had been previously disabled for direct tunneling:

```
config
  context ctxt_name
    iups-service service_name
      rnc id rnc_id
        default direct-tunnel
        end
```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference.*

Restricting Direct Tunnels

The following configuration scenario prohibits the S4-SGSN to setup direct tunneling over the S12 interface during Inter SGSN RAUs:

```
config
  call-control-profile profile_name
    rau-inter avoid-s12-direct-tunnel
    end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
   context context_name
      iups-service service_name
         rnc id rnc_id
            direct-tunnel not-permitted-by-rnc
            end
```

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

show call-control-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
.
.
.
Re-Authentication
         : Disabled
Direct Tunnel
             : Not Restricted
GTPU Fast Path
            : Disabled
.
.
```

Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

show iups-service name *<service_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name                                                  : iups1
.
.
.
Available RNC:
    Rnc-Id                                                        : 1
    Direct Tunnel                                              : Not Restricted
```

Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the S4 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the S-GW over the S11 interfaces. The S-GW responds with it's own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Use the following example to configure this feature.

```
configure
   context egress_context_name -noconfirm
      interface s12_interface_name
         ip address s12_ipv4_address_primary
         ip address s12_ipv4_address_secondary
         exit
      exit
   port ethernet slot_number/port_number
      no shutdown
      bind interface s12_interface_name egress_context_name
      exit
   context egress_context_name -noconfirm
      gtpu-service s12_gtpu_egress_service_name
         bind ipv4-address s12_interface_ip_address
         exit
      egtp-service s12_egtp_egress_service_name
         interface-type interface-sgw-egress
         validation-mode default
         associate gtpu-service s12_gtpu_egress_service_name
         gtpc bind address s12_interface_ip_address
         exit
      sgw-service sgw_service_name -noconfirm
         associate egress-proto gtp egress-context egress_context_name
egtp-service s12_egtp_egress_service_name
         end
```

Notes:

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

Monitoring and Troubleshooting Direct Tunnel

show subscribers sgsn-only

The output of this command indicates whether. Direct Tunnel has been established.

```
show subscribers sgsn-only full all
```

```
Username: 123456789012345
 Access Type: sgsn-pdp-type-ipv4        Network Type: IP
 Access Tech: WCDMA UTRAN
  |
  |
```

```
NSAPI: 05                                Context Type: Primary
Context initiated by: MS
Direct Tunnel : Established
```

show gmm-sm statistics sm-only

The output of this command indicates the number of total active PDP contexts with direct tunnels.

show gmm-sm statistics sm-only

```
Activate PDP Contexts:
 Total Actv PDP Ctx:
  3G-Actv Pdp Ctx:             1  2G-Avtv Pdp Ctx:       0
  Gn Interface:                1  Gn Interface:          0
  S4 Interface:                1  S4 Interface:          0
 Total Actv Pdp Ctx:
  with Direct Tunnel:          1
```

Direct Tunnel Bulk Statistics

Currently there are no bulk statistics available to monitor the number of PDP contexts with Direct Tunnel.

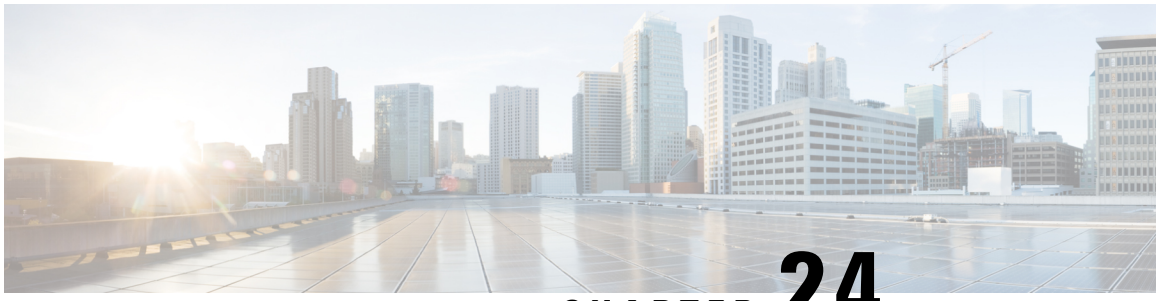
Bulk statistics under the EGTPC schema are applicable for both Direct Tunnel and Idle Mode Signalling Reduction (ISR) [3G and 2G]. The following statistics track the release access bearer request and response messages which are sent by the SGSN to the S-GW upon Iu or RAB release when either a direct tunnel or ISR is active:

- tun-sent-relaccbearreq
- tun-sent-retransrelaccbearreq
- tun-recv-relaccbearresp
- tun-recv-relaccbearrespDiscard
- tun-recv-relaccbearrespaccept
- tun-recv-relaccbearrespdenied

The following bulkstats under EGTPC schema track Downlink Data Notification (DDN) Ack and failure messages between the S-GW and the SGSN when either direct tunnel or ISR is active:

- tun-recv-dlinknotif
- tun-recv-dlinknotifDiscard
- tun-recv-dlinknotifNorsp
- tun-recv-retransdlinknotif
- tun-sent-dlinknotifackaccept
- tun-sent-dlinknotifackdenied
- tun-sent-dlinkdatafail

For complete descriptions of these variables, see the EGTPC Schema Statistics chapter in the *Statistics and Counters Reference*.



CHAPTER 24

Dynamic Guaranteed Bit Rate

This chapter describes the following topics:

- Feature Summary and Revision History, on page 433
- Feature Description, on page 434
- How It Works, on page 434
- Limitations and Restrictions, on page 435
- Configuring Dedicated GBR Bearer, on page 436

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

When a Guaranteed Bit Rate (GBR) dedicated bearer is used, the bandwidth of resources is reserved on the network. If the subscriber data flow is at lower bandwidth than the allocated values, then extra GBR is wasted on the network.

This feature adds flexibility where the Gateway periodically monitors the usage of the GBR on the bearer and depending on the usage. The Gateway steps-up or steps-down the allocated GBR accordingly.

How It Works

This section describes the working of Dynamic GBR functionality.

- Dedicated GBR Bearer is created using local policy configurations on a session setup or on certain call events.
- The SAEGW monitors the GBR after bearer creation for every interval of 30 seconds.
- After every interval, SAEGW verifies the average data-rate with the threshold value configured.
- In case, if the threshold breaches, then the GBR is stepped-up or stepped-down as per the configured value.
- SAEGW allows configuration of an upper and lower threshold of the GBR and also step-up or step-down value corresponding to the upper and lower threshold value.

Upper Threshold Breach

First Threshold Breach:

- Subscriber creates the dedicated bearer with QCI=qci1 with GBR as 1000 kbps with the upper threshold configured as 80%, that is, 800 kbps.
- Every 30 seconds the data-rate is evaluated. If the threshold limit is breached then SAEGW initiates the Update Bearer Request to upgrade the GBR value to step up by the configured percentage value.
- After 30 seconds if data-rate evaluated is more than 800 kbps, then the UBR is initiated to upgrade the GBR. The GBR is upgraded with the aggregate value of the initial configured GBR and the step-up configured percentage. For example, if the step-up increase is configured as 20% (200 kbps), then the Update Bearer Request if triggered with 1200 kbps.

Second Threshold Breach:

- As the GBR is increased to 1200 kbps, new upper threshold being monitored is 80% of 1200, that is, 960 kbps.
- On the next monitoring interval, if data-rate usage crosses 960 kbps, SAEGW again initiates the Update Bearer Request to upgrade the GBR values. These GBR values are upgraded to step-up by configured percentage value (20%). However, this 20% is of the base value, that is 1000, and not 1200 kbps. Hence, the increase is again by 200 kbps and the Update Bearer Request is 1400 kbps as the new GBR.

Important The step increase percentage is of the base(initial) value of the bearer and not the current negotiated value. The maximum value to which GBR can be stepped up is the configured MBR value.

Lower Threshold Breach

First Threshold Breach:

- Subscriber creates the dedicated bearer with QCI=qci1 with GBR as 1000 kbps with lower threshold is configured as 50%.
- Due to upper threshold breach, SAEGW has upgraded the GBR to 1400 kbps.
- When the usage on the bearer reduces below 700 kbps (50% of current GBR), SAEGW initiates the Update Bearer Request to downgrade the GBR. These GBR values are downgraded to step-down by configured value (say 20%), that is 1400 – 200 = 1200 kbps.



Important The step decrease percentage is of the base (initial) value of the bearer and not the current negotiated value. The GBR value will not be stepped down below the initial negotiated value.

Second Threshold Breach:

- As the GBR is decreased to 1200 kbps, the data decreases further to breach the new 50% lower threshold. That is, 50% of 1200 = 600 kbps.
- SAEGW initiates the Update Bearer Request to downgrade the GBR values to step down by configured value (20%). That is, 1200 – 200 = 1000 kbps.

Limitations and Restrictions

This section provides limitations and restrictions of this feature.

- The SAEGW monitors the bearer bandwidth on every 30-seconds interval.
- If GBR usage exceeds a configurable percentage of a configured threshold, SAEGW initiates a bearer modification procedure. SAEGW initiates this procedure with a bearer QoS update using an upper bound configured value. eNB and UER adjust GBR accordingly.
- If GBR usage falls below a configurable percentage of a configured threshold, SAEGW initiates a bearer modification procedure. This bearer modification procedure is initiated with a Bearer QoS update using a lower bound configured value. eNB and UER adjust GBR accordingly.
- In case multiple rules are configured on the same bearer, then QoS is enforced from the current negotiated bearer values. The individual values under charging action corresponding to the ruledef are not honored if this feature is enabled on the bearer.

- For the monitored bearer, if the bit rate is modified or rule is deleted, then the base value of GBR is changed. This change in base value of GBR leads to change in the step-up or step-down values.
- Session recovery and ICSR are supported.
- The step-up and step-down values are calculated as per the base values of the GBR of the bearer and not the current GBR applied on the bearer.

Configuring Dedicated GBR Bearer

This section provides the configuration commands added for this feature.

In addition to this, the following new configurations must be enabled.

1. Lower bound GBR (in %) to determine which GBR value to step-down.
2. Upper bound GBR (in %) to determine which GBR value to step-up.
3. Step-up the threshold (in %).
4. Step-down the threshold (in %). This value must be less than step-up threshold.

trigger

New CLI keywords **bearer-creation** and **monitor-bearer-bandwidth** have been added to this CLI command. The keyword **bearer-creation** triggers for every new bearer created. The keyword **monitor-bearer-bandwidth** triggers whenever the bearer bandwidth is evaluated.

```
configure
    active-charging service <service_name>
       service scheme <service_scheme_name>
          [ no ] trigger {  bearer-creation | flow-create | loc-update |
 monitor-bearer-bandwidth |  sess-setup }
         end
```

Notes:

This CLI is disabled by default.

- **no**: If previously configured, deletes the specified configuration.
- **bearer-creation**: Triggers for every new bearer.
- **flow-create**: Triggers for every new flow.
- **loc-update**: Triggers whenever location changes for the subscriber.
- **sess-setup**: Triggers at the session setup.
- **monitor-bearer-bandwidth**: Triggers whenever bearer bandwidth is evaluated.

committed-data-rate

This CLI command has been added under the ACS Trigger Condition configuration mode to configure the committed data rate of the current negotiated value.

```
configure
    active-charging service <service_name>
       trigger-condition <trigger_condn_name>
          [ no ] committed-data-rate { lower_threshold <value_in_percentage>
| upper_threshold <value_in_percentage> }
          end
```

Notes:

- **no**: Disables the committed data rate of the current negotiated value.
- **committed-data-rate**: Specifies the committed data rate of the current negotiated value.
- **lower threshold**: Configures the threshold as a percentage of the current negotiated value.
- **upper threshold**: Configures the threshold as a percentage of the current negotiated value.
- *value_in_percentage*: Specifies the percentage of initial configured committed-data-rate value. This is an integer value of 0 to 100.

step-up

This new CLI command has been added to the ACS Trigger Action Configuration mode to step up the value of committed data rate.

```
configure
    active-charging service <service_name>
       trigger-action <trigger_action_name>
          [ no ] step-up committed-data-rate <negotiated_value>
          end
```

Notes:

- **no**: If previously configured, deletes the specified configuration.
- **step-up** : Steps up the value of committed data rate by the percentage defined in the *negotiated_value*.
- **committed-data-rate**: Defines the committed data rate.

  negotiated_value: Specifies the percentage of initial configured committed-data-rate value. This is an integer value of 0 through 100.

step-down

This new CLI command has been added to the ACS Trigger Action Configuration mode to step down the value of committed data rate.

```
configure
```

```
active-charging service <service_name>
  trigger-action <trigger_action_name>
    [ no ] step-down committed-data-rate <negotiated_value>
    end
```

Notes:

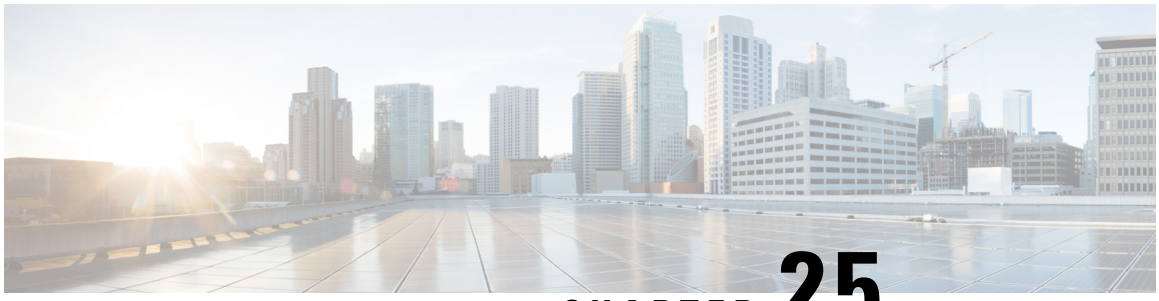
- **no**: If previously configured, deletes the specified configuration.
- **step-down**: Steps down the value of the committed data rate by the percentage defined in the *negotiated_value*.
- **committed-data-rate**: Defines the committed data rate.

  negotiated_value: Specifies the percentage of initial configured committed-data-rate value. This is an integer value of 0 through 100.

Sample Configuration

This section lists the sample configuration of the CLI commands used in this feature.

```
config
  active-charging service ACS
  trigger-action ta1
      step-up  committed-data-rate  20
    exit
  trigger-action ta2
     step-down committed-data-rate  30
    exit
    trigger-condition tc1
      qci = 1
      committed-data-rate upper-threshold 80
    exit
    trigger-condition tc2
      qci = 1
      committed-data-rate lower-threshold 50
    exit
    service-scheme scheme1
      trigger monitor-bandwidth
        priority 1 trigger-condition tc1 trigger-action ta1
        priority 2 trigger-condition tc2 trigger-action ta2
      exit
    subs-class class1
      any-match = TRUE
    exit
    subscriber-base base1
      priority 1 subs-class class1 bind service-scheme scheme1
    exit
exit
```



CHAPTER 25

Dynamic Transport Selection based on Transaction or Origin-Host

- Feature Summary and Revision History, on page 439
- Feature Description, on page 440
- Characteristics of Low and High Priority Channels for Diameter-based Interfaces , on page 441
- Characteristics of Low Priority and High Priority Channels for S11, S5, or S8 interfaces , on page 442
- How it Works, on page 442
- Configuring Dynamic Transport Selection based on Transaction or Origin-Host, on page 446
- Monitoring and Troubleshooting, on page 448

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled-Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	Not applicable

Revision History

Revision Details	Release
First introduced **Important** This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.22

Feature Description

Reliable and secure telecommunications systems are necessary for effectively managing national security incidents and emergencies. The National Security and Emergency Preparedness (NS/EP) is a set of voice, video, and data services that belong to services available from public packet-switched Service Providers and that provide priority services in support of NS/EP communications. The NS/EP communication systems include landline, wireless, broadcast, and cable television, radio, public safety systems, satellite communications, and the Internet.

Wireless Priority Services (WPS) is one of the NS/EP communications programs that provide personnel priority access and prioritized processing in all nationwide and several regional cellular networks, increasing the probability of call completion.

WPS users, also known as first responders, are responsible for the command and control functions that are critical to the management of response to national security and emergencies. When your network carries the traffic for WPS users' all the network elements individually and collectively must adhere to the following conditions:

- **Prioritization of Control Plane Traffic**:WPS user’s control plane traffic is prioritized over other subscribers between different Network Functions in the LTE Core.
- P1, P2, and P3 are the three priority levels available for WPS users:
  - P1 and P2 users are identified in HSS/PCRF and GW uses their priority (ARP) during default and dedicated bearer creation, modification, update, or deletion.
  - P1 and P2 WPS users are always treated as High Priority.
  - DSCP markings for prioritized user’s control plane IP packets is marked with DSCP=47 while all other users control packets IP packets is marked with DSCP=32
- **Diameter Interfaces**:
  - P-GW, Policy Change Rule Function (PCRF) and Diameter Routing Agent (DRA) uses the configuration of Diameter interfaces such as Gx and Rx interfaces to support policy and charging control for subscribers.
  - P-GW and SGW uses non-diameter interfaces such as S5, S8, S11, or S1U with its peer respectively.

Characteristics of Low and High Priority Channels for Diameter-based Interfaces

Low Priority channels indicate normal priority users and High Priority channels indicate WPS users during Differentiated Services Code Point (DSCP) markings. The peer connections towards DRA for PGW (Gx) is shown in the figure.

Figure 37: High-Level Overview of Low and High Priority Channels over Gx Interface

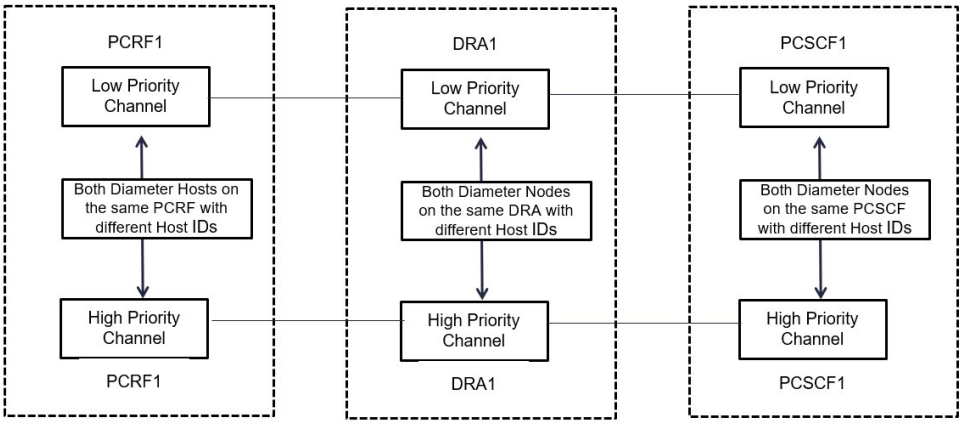


Table 45: Low and High Priority Channels on Gx Interface

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	Gx	Equal to 32	32 **Note** This channel is for non-WPS diameter messages but may carry WPS diameter messages in error scenarios, for example when all the Red Peers are down.	Not Modified Examples: 0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1
High Priority	Gx	Equal to 47	47	Specific to High Priority Examples: 0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

Characteristics of Low Priority and High Priority Channels for S11, S5, or S8 interfaces

The S5 and S11 interfaces are GTPv2 based (which uses UDP as the transport protocol), Low and High Priority channels have the following characteristics.

Table 46: Low and High Priority Channels on Other Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	S11 or S5 or S8	32	—	—
High Priority	S11 or S5 or S8	47	—	—

How it Works

The following is a high-level overview of how this feature works. The PGW selects either High Priority or Low Priority channels based on the **wps profile**. If APN name, QCI, and ARP are matched as shown in the table, session is detected as WPS session at IMSA.

Table 47: WPS Message Prioritization based on APN, QCI, and ARP Priority Level

APN Name	QCI	ARP	DSCP
IMS	66,69	*	47
IMS	*	1,2	47
IMS	8	3	47
IMS	9	5	47
IMS	2	4	47

The following table explains the process of dynamic transport selection based on transaction or Origin Host:

Table 48: Procedure

Process	Description
Identifying WPS and Non-WPS users	• Use the CLI command **priority-select** at diameter end point to enable or disable WPS users. This CLI command is at policy-control configuration in IMS-authorization service. • PGW receives Create session request with every eMPS session is tagged with the Allocation and Retention Priority (ARP) value. • PGW verifies whether that ARP value is matching the WPS. • Session Manager checks whether the received ARP value matches the eMPS session or not. • If the above criteria of matching eMPS session and enabling of priority select is met, then, the user is called as WPS user. Else, the user is called as Normal user.
Prioritizing Session	At Policy Change Rule Function (PCRF), you can define two priority levels such as Low Priority session for non-WPS users and high priority session for WPS users. • **Always-On WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to WPS users are always treated as high priority. • **On-Demand WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to Non-WPS users can be uplifted to higher priority (lower ARP PL value) dynamically. The most common example of this is when a WPS user makes a WPS call (that is initiated by dialing a call starting with *272) to non-WPS user. These types of sessions are called On-Demand eMPS sessions. • Control plane Gx messages that belong to high priority sessions uses High Priority channels. • Control plane Gx messages that belong to nonhigh priority sessions uses high priority channels.

Process	Description
Differentiating paths between normal users and WPS users	On Gx interface, different connections are made to form the second path at the CLI level: • P-GW creates two sets of DRA peer connections. One set for higher priority and other for normal priority messages. • P-GW sends CCR-Initial and CCR-Update Gx messages on specific pair of connections based on type of session (WPS session or Non-WPS session). • After the peer is configured with **priority-select** flag, all CCR messages for WPS session are initiated over High Priority peer. If P-GW identifies the users as a WPS user, it binds to the high priority peer with DSCP marking as 47. However, non-WPS subscriber's Diameter message is initiated over Low Priority peer and the DSCP is set to 32. **Note** If the dscp configuration for peer is not specified, then global dscp value configured under diameter endpoint is used. If global dscp value under diameter endpoint is not configured, then dscp value "0" is used. The following actions are performed before triggering CCR-I message with respect to WPS users: • Selection of High Priority peer. • If an existing AVP string is configured in peer configuration, Origin Host ID is appended with a string. If string is not configured, default **-wps** string is appended to Origin Host ID. • DRA/PCRF responds with CCA-I over high priority channel upon reception of the CCR-I. The subsequent messages follow the high priority channel.

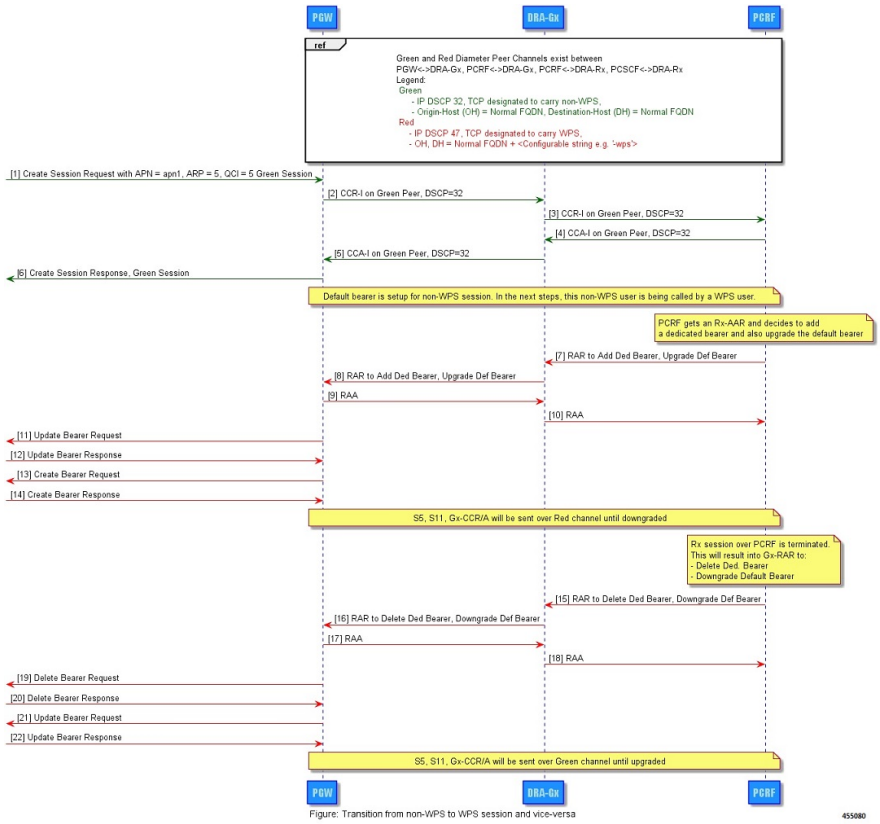
The key call flow for this feature include transitioning from non-WPS to WPS Session and PCRF initiated Bearer Deletion.

If CSR (Creation Session Request) has one bearer and ARP does not match with ARP defined in eMPS profile, the Session is treated as low priority Session. All Gx messages follow low priority channel to PCRF. However, if any dedicated bearer triggered by Mobile has ARP matched with ARP defined in eMPS profile, low priority session is transitioned to WPS session.



Note In this document Low priority channel and Green channel are used interchangeably and the same is true for Red and High priority channel.

Figure 38: Transitioning from Non-WPS to WPS Session and Vice Versa



Note In the StarOS 21.22 release, WPS session is the same as eMPS session and is based on eMPS profile.

Table 49: Procedure

Step	Description
1 through 6	Low Priority channels are used for a non-WPS session.
7 through 14	P-GW receives RAR with an ARP defined in eMPS profile, the following operations are performed. • Internally, the session is updated to an eMPS session. • P-GW identifies high priority peer and appends the string "-wps" (or configured origin-host-suffix string) to Origin Host AVP in the outgoing messages. The subsequent outgoing messages on Gx, S5 and S11 will follow the high priority channel until the session is downgraded again.
15 through 22	P-GW receives RAR with ARP not defined in eMPS profile, the session is downgraded from eMPS (WPS) session to non-WPS.

Step	Description
Note When the session is in eMPS state and if there is no High priority Gx peer available, a Low Priority Peer shall be used for Gx traffic. If there is no peer is available, then the call gets dropped	

Configuring Dynamic Transport Selection based on Transaction or Origin-Host

This section describes how to configure the Dynamic Transport Selection based on Transaction or Origin-Host.

1. Configuring eMPS Profile
2. Associating an eMPS profile with P-GW Service
3. Enabling Gx Prioritization for eMPS Sessions
4. Enabling WPS feature and priority services for APN services

Configuring eMPS Profile

This section describes how to configure eMPS profile. Use the following commands to configure eMPS profile, which is used to identify/mark a bearer/session as an eMPS bearer/session

```
configure
   [ no ] emps-profile emps_profile_name -noconfirm
      [ no ] earp { [string value] }
      [ no ] dscp-marking { dscp-value }
      end
```

Notes:

- **emps-profile emps_profile_name**: Configures eMPS profile for defining attributes of an eMPS session. The *emps_profile_name* is a string of size from 1 to 63.
- **-noconfirm**: Creates a new eMPS profile without prompting for confirmation.
- **earp**: Configures a maximum of 8 eARP priority level (PL) values so that sessions with configured eARP priority values can be marked as eMPS sessions. Maximum of 8 eARP values can be configured under an eMPS profile.
- **dscp-marking**: Specifies the DSCP value to be applied to eMPS sessions. The dscp_value is a hexadecimal number between 0x0 and 0x3F.



Note For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPS bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide or the SAEGW Administration Guide*.

Associating an eMPS-Profile with P-GW and S-GW Service

This section describes how to associate an eMPS profile with P-GW and S-GW services.

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

```
configure
  context context_name
    Sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no**: Disables a emps-profile association with P-GW or S-GW service.
- **associate emps-profile***emps_profile_name*: Associates an eMPS profile with either P-GW or S-GW service.

Enabling Gx Prioritization for eMPS Sessions and Wireless Priority Services

This section describes how to enable Gx prioritization levels for eMPS sessions

```
configure
  context context_name
    [ no ]ims-auth-service service_name
      [ no ] policy control
         [ no ] diameter origin endpoint endpoint_name priority-select
         [ no ] diameter session-prioritization
      end
```

Notes:

- **priority-select**: Enables Wireless Priority Services (WPS) for the selected IMS authorization service.

Note The **priority-select** keyword is mandatory for WPS feature.

- **[no] diameter session-prioritization**: Enables or disables Gx signalling prioritization for eMPS sessions:
  - By default, the **diameter session-prioritization** CLI command is disabled and Gx messages does not get prioritized based on WPS value.
  - If previously configured, use the **no diameter session-prioritization** CLI command to set the default behavior
  - The **diameter session-prioritization** CLI takes effect when Gx, along with eMPS profile, is enabled in the configuration.

- The **diameter session-prioritization**configuration attaches DRMP-0 AVP to Diameter Messages going over the High Priority channel. DRA/PCRF takes appropriate actions based on DRMP-0, incase fallback from High Priority to Low Priority channel takes place on P-GW to DRA or DRA to PCRF Gx links.



Note Diameter session-prioritization is an existing CLI and it is not mandatory for configuring WPS feature.

Differentiating Low Priority and High Priority Peers

This section describes how to differentiate between low and priority peers. Priority Endpoint configuration under policy-control ensures WPS feature is only applicable to IMS-auth-service under policy control area. It is applicable for Gx interface.

```
configure
  context context_name
     [ no] diameter endpoint pgw-gx
      peer PGW-Gx-green-1  realm_address ipv4 address | ipv6 address portport_number

       peer PGW-Gx-wps-1  realm_address ipv4 address | ipv6 address port port_number
priority-select origin-host-suffix value dscp value
     end
```

NOTES:

- **priority-select**: Defines peer as high priority wps peer. It is optional to configure to both parameters. Following conditions apply during peer configuration:
  - If **priority-select** is not configured, peer is not treated as high priority **wps** peer.
  - **origin-host-suffix**: If **priority-select** is set for a peer, it is treated as **wps** peer. If **Origin-host-suffix** is configured for **wps** peer, configured string is appended to Origin Host ID otherwise, default **-wps** string is appended to Origin Host ID (for example, pgw-gx-wps).
  - **dscp**: If DSCP is not configured for high priority peer, endpoint level DSCP is filled in IP packets towards DRA/PCRF. Otherwise, configured DSCP is filled in IP packet.

Monitoring and Troubleshooting

This section describes troubleshooting information, show commands and Outputs, IMSA level statistics, diameter statistics, and Bulk statistics.

Show Commands and Outputs

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics.

show ims-authorization policy-control statistics

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics

Field	Description
DPCA WPS Session Stats	
Total Current Sessions	The total number of DPCA WPS session currently running on this system
Switched from Priority Chnl	Indicates the total subscribers moved from Wireless Priority to Normal
Switched to Priority Chnl	Indicates the total subscribers moved from Normal to Wireless Priority
DPCA WPS Message Stats	
Priority Channel Indicates message statistics for WPS session, which is sent or received on high priority channel.	
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
Total CCA	Total Credit Control Answer (CCA) messages sent in response to CCRs.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.

Field	Description
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message.
CCA-Update Dropped	Total number of CCA-U messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end sessions.
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end sessions but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages, which are dropped due to S-GW restoration, DPCA is off ,or not present, or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization..
RAA	Total number of Re-Auth-Requests(RARs) answered with Re-Auth-Answer (RAA) message.
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.
Non-Priority Channel	**Indicates message statistics for WPS session, which is supposed to be sent/received on Priority channel but sent/received on Non-priority channel**
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.

Field	Description
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages which are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message
CCA-Update Dropped	Total number of CCA-U messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end session/s..
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end session/s but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization.
RAA	Total number of Re-Auth-Requests (RARs) answered with Re-Auth-Answer (RAA) message.

Field	Description
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.

show diameter peers full all

Use this CLI command to view peer details.

Field	Description
Priority Channel	Indicates peer is high priority or not. The options are: • **Yes**: Indicates peer is WPS. • **No**: Indicates Peer is Non-WPS.
DSCP Configured	Indicates the dscp value to be used in Gx IP Packet. • If configured, displays peer specific DSCP. • If not configured, then it will display the dscp configured in endpoint.

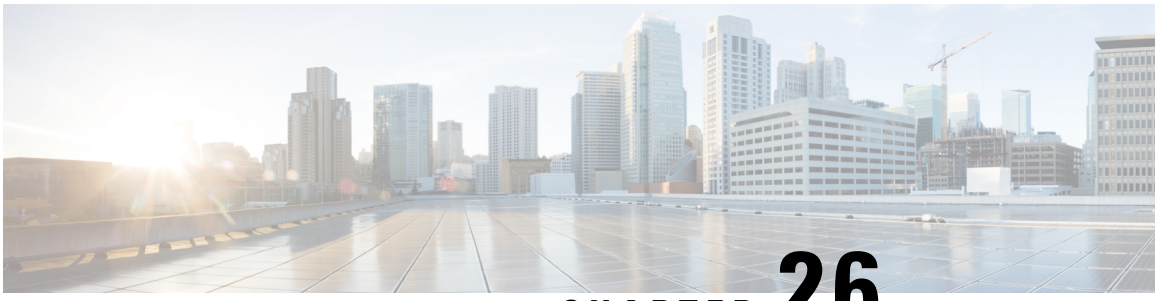
Bulk Statistics

This section provides information on the bulk statistics for the Dynamic Transport Selection based on Transaction or Origin-Host feature on P-GW

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users.

Counters	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca - imsa - total - sessions-switched -from - priority - channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca - imsa- total- sessions-switched - to- priority- channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.



CHAPTER 26

ePDG Selection Using PCO

- Feature Description, on page 453
- How it Works, on page 453
- Limitations, on page 454
- Configuring ePDG Selection Using PCO, on page 454
- Monitoring and Troubleshooting ePDG Selection Using PCO Feature, on page 454

Feature Description

The purpose of this feature is to enable the PGW to send the ePDG IP addresses in an operator PCO so that when connected to a WIFI network the UE will attach to the closest geographic ePDG. This will aid in setting up the IPSEC tunnel to the closest ePDG and therefore reducing latency for VoWIFI and other features.

A new CLI has been introduced to customize PCO options in the network.

Important This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Important ePDG PCO is supported only for the CS request which are received on the S5-S8 interface. This feature is not applicable for the GGSN calls.

How it Works

- One ePDG FQDN can be configured on an APN.
- Operator specific PCO is supported in CSReq/Res on S5/S8 interface and in PBU/PBA on PMIP S2a interface.
- P-GW uses DNS server for FQDN resolution.
- Maximum of 2 IPv4 and 2 IPv6 ePDG addresses can be sent in PCO.

Limitations

This feature is not applicable for the GGSN calls.

Configuring ePDG Selection Using PCO

Configuring epdg fqdn

Use the following example to customize PCO (Protocol Configuration Options) options in the network.

```
configure
     apn apn_name
        pco-options epdg fqdn domain_name
        no pco-options
        end
```

Notes:

- **no:** Does not send customized PCO options to any of the UEs.
- **pco-options:** Controls the sending of customized PCO (Protocol Configuration Options) options in the network.
- **epdg:** Enables operator specific epdg selection in the PCO. By default it is disabled.
- **fqdn:** Specifies fully qualified domain name. Based on this, IP addresses would be queried from the DNS.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show configuration verbose**

Please see the *Monitoring and Troubleshooting* section for the command output.

Monitoring and Troubleshooting ePDG Selection Using PCO Feature

The following section describes commands available to monitor the ePDG Selection Using PCO Feature.

Show Commands for ePDG Selection Using PCO Feature

show apn *apn_name*

This command displays the following output:

```
show apn name intershat
PCO Options:
    custom1      Mode: enabled
    Link MTU:    1500
    ePDG Selection FQDN: <epdg.com> / N.A.

APN QCI Stats: Disabled
Bearer duration stats config: Disabled
Event Reporting: Disabled

HSGW Static PGW-FQDN:
    Primary  FQDN: N/A   Secondary  FQDN: N/A
```

show config

This command has been modified to display the following output when ePDG has been configured:

```
   pco-options epdg fqdn epdg.com
```

show configuration verbose

This command displays the following output when **epdg fqdn** is configured:

```
 no pco-options epdg
```

show pgw-service statistics name

This command displays the following output:

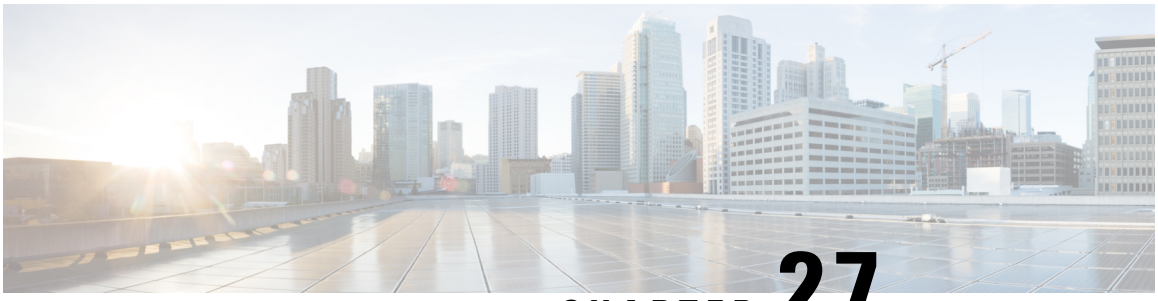
```
ePDG selection PCO statistics:

IPv6 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1

IPv4 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1
```

show saegw-service statistics name function pgw

This command displays the following output:

```
ePDG selection PCO statistics:

IPv6 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1

IPv4 PCO:
Request received: 20
Response sent: 18
```

```
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1
```



CHAPTER 27

Embed IMSI into Session Id

- Feature Summary and Revision History, on page 457
- Feature Description, on page 458
- How It Works, on page 458
- Limitations, on page 458
- Configuring Diameter Accounting Interim Interval, on page 459
- Monitoring and Troubleshooting, on page 460

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW • S-GW
Applicable Platform(s)	• ASR 5500 • VPC - Di • VPC - Si
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

For troubleshooting and investigating network issues related to the Diameter interface, it is important to filter the subscriber or UE specific Diameter traffic. Any traffic associated with a particular IMSI can be easily filtered, even without knowing the Diameter session ID, if the IMSI information is embedded into the Diameter Session ID AVP. This feature allows the operator to filter the subscriber or UE specific Diameter traffic.

This feature introduces a new CLI command **session-id include imsi** under the **diameter endpoint configuration** mode to embed IMSI into Diameter session ID AVP over the Gx, Gy, and Gz (Rf) interface.



Important This feature is license controlled. Contact your Cisco account representative for information on how to obtain a license.

How It Works

A new CLI command **session-id include imsi** has been added under the **diameter endpoint configuration** mode to enable/disable inclusion of IMSI in Session-Id AVP for all Diameter sessions associated with that Diameter endpoint. Operators can enable only the required Diameter endpoints and control the inclusion of IMSI in the Session-ID AVP. IMSI information is included in the Diameter Session-ID AVP over the Gx, Gy, and Gz (Rf) interface, if the **session-id include imsi** is enabled on respective Diameter endpoints.

For emergency call with "only IMEI", IMSI information is not available for that emergency PDN. Hence, this IMSI information is not included in Diameter Session-ID at Gx, Gy, and Gz interface, when **session-id include imsi** is enabled. Configuring **session-id include imsi** impacts only new PDN connection and does not have any impact on existing PDN connection behavior (Gx, Gy, and Gz (Rf)) interface. For example, if the CLI command to include IMSI is enabled for the Gy Diameter endpoint after PDN creation. If a new dedicated bearer is created after this configuration change, then in this case Gy session established for a new dedicated bearer is not included IMSI in Gy Diameter session ID.

There is no impact of session manager recovery/ICSR on the session-ID AVP. Session-ID associated with Gx, Gy, and Gz (Rf) session is recovered transparently (which is irrespective of latest endpoint configuration). New sessions come up with session IDs as per the configuration on the newly active chassis.

Limitations

Following are the known limitations of this feature:

- Assuming IMSI information as sensitive information, operator must consider security aspects before enabling this CLI option.

- For an emergency call with "Only IMEI", IMSI information is not available for the emergency PDN, hence it is not included in the diameter Session-ID at Gx, Gy, and Gz (Rf) interface.
- During ICSR upgrade scenario, it is assumed that the new CLI option must be enabled only when the upgraded chassis is in stable state and there exists no chances of ICSR downgrade.
- If new CLI is enabled in the newer version of chassis, ICSR Downgrade is not recommended.
- As new CLI option is not available in old software versions, hence ICSR downgrade is not recommended. Performing ICSR downgrade should have the following impact on the diameter sessions, which have IMSI, included as part of Session-ID.
  - Gx and Gy: Existing diameter session (Gx, Gy) should be downgraded with old format of Session-Id. In that case, both P-GW and PCRF are out of sync leading to hanging session at P-GW or/and PCRF. Any communication from PCRF (RAR)/P-GW (CCR-U) can lead to stale session deletion.
  - Gz (Rf): However, Rf sessions should be recovered properly and any Rf signaling is sent out to Rf servers properly but responses cannot be processed as diamproxy cannot parse the new format session id which again puts Rf sessions into stale state until purged.

Configuring Diameter Accounting Interim Interval

The following CLI command has been added under the **diameter endpoint** configuration mode to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf). Configuration changes will be applicable only to new Sessions at Gx, Gy and Rf. Configuration changes will not have any impact on existing sessions behavior at Gx, Gy, and Rf. For Gy, multiple Diameter sessions can be initiated per subscriber and the session ID format setting will bind to the subscriber. The setting will be taken to effect when the first Diameter session is established and following Gy sub sessions will keep using the session ID format used in first session.

```
configure
    context context_name
       diameter endpoint endpoint_name
           [no] session-id include imsi
           end
```

Notes:

- **session-id:** Describes Diameter Session-ID format
- **include:** Includes configured information in Diameter Session-ID
- **imsi:** Includes International Mobile Subscriber Identification (IMSI) in Diameter Session-ID
- **no:** Disables this feature, that is, IMSI is not included in the Diameter Session-ID, which is the default behavior.
- By default, CLI is disabled, hence IMSI will not be populated in Diameter Session-ID.

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 configuration

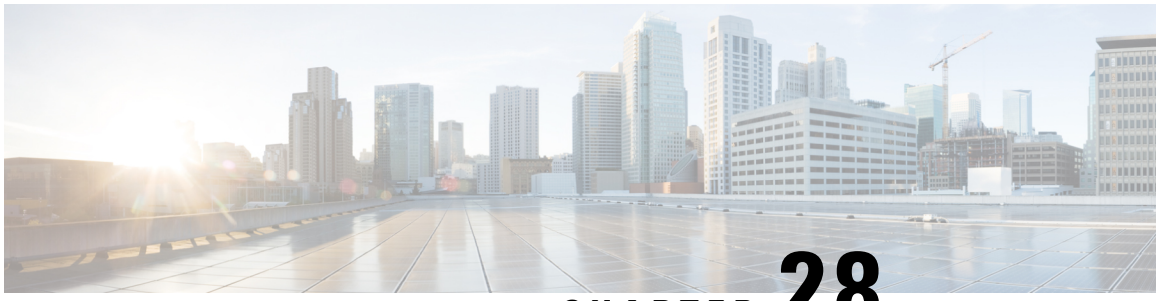
The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi

show configuration [verbose]

The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi



CHAPTER 28

Enabling S6b for IMS APN

This chapter describes the following topics:

- Feature Summary and Revision History, on page 461
- Feature Changes, on page 462
- Configuring Commands for Enabling S6b for IMS APN, on page 462
- Enabling S6b Authentication for Trusted Wi-Fi, on page 463
- Show Commands and Outputs, on page 464

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
In this release, S2a authorization is enabled to separate the authentication request for LTE and Wi-Fi interfaces using authorize-with-hss eGTP configuration. It enables s6b authentication in both APN and P-GW service for S2a interface only.	21.21
With this feature, S6b authorization is enabled for 3G access at the APN level to allows P-GW to update the new P-GW ID to HSS.	21.6
First introduced.	Pre 21.2

Feature Changes

Currently, P-GW supports enabling S6b authentication for 3G access on GGSN service level configuration.

For LTE or Wi-Fi access, S6b authentication is supported on both P-GW service level and APN level configuration. If the S6b authentication is enabled for particular APN, when the subscriber joined on LTE transfers to Wi-Fi then 3G, UE does re-registration of the IMS session on 3G. Different P-GW is selected. However, SGSN does not update the new P-GW. HSS has the history of the old P-GW. When the subscriber transfers back to LTE and then to Wi-Fi, it hands over to the old P-GW. However, the old P-GW does not have the new IMS session and this result in the handover failure. With this feature, S6b authorization is enabled for 3G access at the APN level to let P-GW update the new P-GW ID to HSS. This addresses the inconsistency. Following two **authorize-with-hss** CLI keywords are added at the APN level to enable S6b authentication for 3G access and GnGp handover.

- **gn-gp-enabled**: Enables the S6b authentication for 3G access during the call connect and gn-gp handover.
- **gn-gp-disabled**: Terminates S6b connection when the subscriber moves to 3G access. This is used to override the legacy handover behavior where the session was continued irrespective of the configuration.

Note These new keywords are not configured by default when **authorize-with-hss** or **authorize-with-hss egtp** are configured. You have to explicitly enable this customized behavior by configuring the CLI commands introduced for this feature.

Enhancement to S6b Authentication: In StarOS 21.21 and later releases, S2a authorization is enabled to separate the authentication request for LTE and Wi-Fi interfaces using **authorize-with-hss egtp** configuration. It enables s6b authentication in both APN and P-GW service for S2a interface only.

Configuring Commands for Enabling S6b for IMS APN

S6b authentication can be enables at the APN level, two new keywords have been added to the **authorize-with-hss** CLI command.

To enable or disable S6b, execute the following command:

```
configure
```

```
  context context_name
    apn apn_name
      authorize-with-hss [ egtp [ gn-gp-enabled ] [ s2b [ gn-gp-enabled
[ report-ipv6-addr ] ] ] [ s5-s8 [ gn-gp-disabled | gn-gp-enabled ] ] [
report-ipv6-addr ] | lma [ s6b-aaa-group aaa-group-name | report-ipv6-addr
] | report-ipv6-addr ]
       [ default | no ] authorize-with-hss
       exit
```

NOTES:

- **gn-gp-disabled:** Disables S6b authorization for 3G initial attach and GNGP handover.
- **gn-gp-enabled:** Enables S6b authorization for 3G initial attach and GNGP handover.
- **s2b:** Enable S6b authorization for egtp-S2b.
- **s5-s8:** Enable S6b authorization for egtp-S5S8.
- **report-ipv6-addr:** Enables IPv6 reporting through AAR toward the S6b interface.

Enabling S6b Authentication for Trusted Wi-Fi

Enabling S6b Authentication for Trusted Wi-Fi

S6b authentication is enabled for all LTE and Wi-Fi interface using HSS authentication process. To separate this authentication request for LTE and Wi-Fi interfaces a new configuration is introduced. The parameter S2a is added to represent the trusted Wi-Fi interface in the configuration part of **authorize-with-hss egtp** and this enables the S6b authentication for S2A interface only and this is done in both APN and P-GW service configuration.

Use the following S2a configuration command to indicate Trusted Wi-FI at authorize-with-hss egtp:

```
configure
  context context_name
    apn apn_name| pgw-service service_name
      authorize-with-hss [ egtp [s2a [gn-gp-enabled [report-ipv6-addr]
] ] ]
       [ default | no ] authorize-with-hss
       exit
```



Note Enabling the S6b authentication is allowed with a combination of S2a and S2b, or S2a and S5-S8, or S2b and S5-S8.

Below are the examples to enable the s6b authentication for S2a interface alone in APN and P-GW Service.

Example for APN Service

```
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
```

```
    authorize-with-hss egtp s2a
    ims-auth-service ims-ggsn-auth
    ip access-group acl4-1 in
    ip access-group acl4-1 out
    ip context-name egress
    ipv6 access-group acl6-1 in
    ipv6 access-group acl6-1 out
    active-charging rulebase prepaid
  exit
```

Example for P-GW Service

```
pgw-service pgw_service
    authorize-with-hss egtp s2a
    associate ggsn-service ggsn-service
    associate egtp-service egtp_service
    associate peer-map map_pgw
    egtp create-session-rsp apn-ambr-always-include
  exit
```

Show Commands and Outputs

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

show apn name

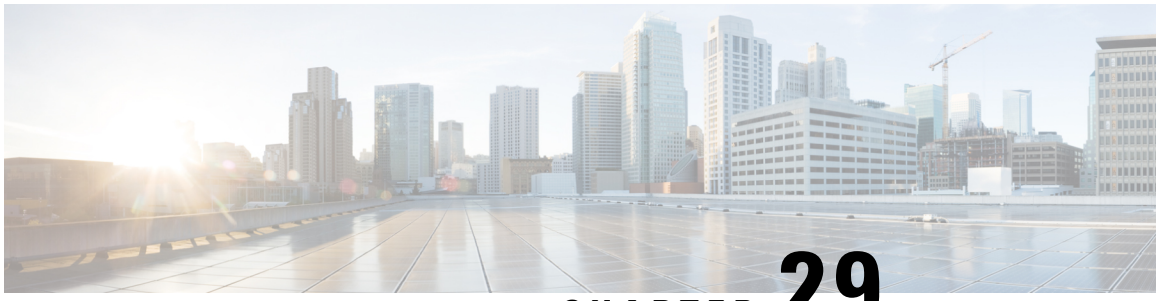
This CLI command is modified to include the gn-gp enabled or disabled status:

- Authorization with S6b : HSS-EGTP-S5S8 GN-GP-Disabled
- Authorization with S6b : HSS-EGTP-S5S8 GN-GP-Enabled

show config apn intershat

The following new fields are added to the show command to indicate the gn-gp enabled or disabled status:

- authorize-with-hss egtp s5-s8 gn-gp-enabled
- authorize-with-hss egtp s5-s8 gn-gp-disabled



CHAPTER 29

Emergency Call Support on the ePDG and P-GW

This feature provides emergency call support on the ePDG and P-GW.

- Feature Summary and Revision History, on page 465
- Feature Description, on page 466
- How it Works, on page 467
- Configuring AAA Failure Handling for S2b Emergency Calls, on page 473
- Configuring APN and S6b Authorization, on page 474
- Monitoring and Troubleshooting, on page 475

Feature Summary and Revision History

Applicable Product(s) or Functional Area	P-GW SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always On
Related Changes in This Release	Not applicable
Related Documentation	• *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
This release supports new emergency calls from S2b Interface. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20
First introduced	21.1

Feature Description

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction.

Supported Functionality

3GPP Release 13 Emergency Call Support on the ePDG and P-GW includes the following functionality:

- Emergency call establishment over untrusted Wi-Fi for the P-GW. The P-GW includes the new **Emergency-Indication** AVP over the AAA S6b interface only during Emergency PDN connection establishment.
- Lawful Intercept is supported for Emergency PDNs over the S2b interface.
- Various Create Session Request message IEs have been modified to support all four different behaviors of emergency bearer establishment.
- Intra- and Inter-chassis recovery are supported for emergency call over the S2b interface.
- Network initiated dedicated bearer creation is supported for emergency calls over the S2b interface.
- The maximum APN restriction is ignored for emergency APN.
- Multiple PDNs are supported for emergency calls over the S2b interface.
- Context replacement for emergency calls over the S2b interface without IMSI with same IMEI is supported.
- P-GW emergency related statistics and bulkstats are available.
- Graceful shutdown of S2b emergency calls is supported.

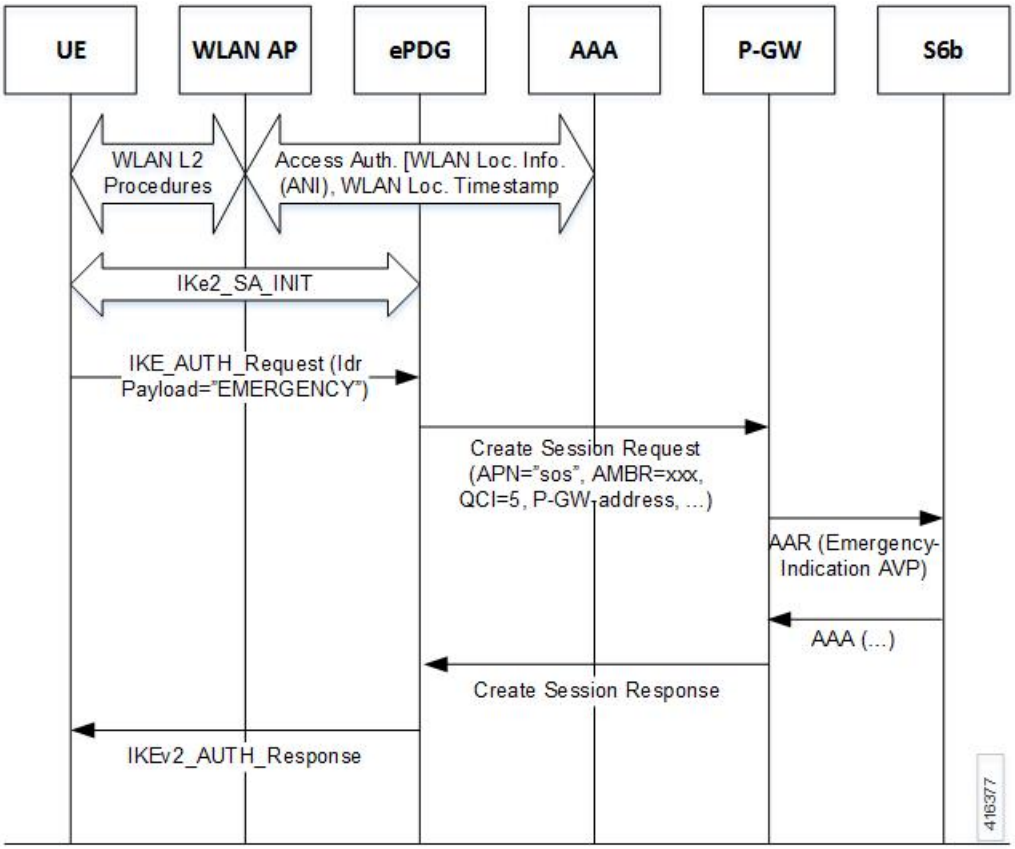
Previous Behavior: Emergency calls were not supported for the S2b interface. Also, handoff between the s2b interface and LTE was not supported for emergency calls.

New Behavior: Emergency calls are now supported on the S2b interface and handover is also supported for emergency calls from the S2b interface to LTE and vice-versa for "authenticated imsi" only.

How it Works

The ePDG sends a Create Session Request (CSReq) message to the P-GW. The P-GW deduces the emergency related policies to apply from the Access Point Name (APN) received in the CSReq message. For emergency attached User Equipment (UE), if the International Mobile Station Identifier (IMSI) cannot be authenticated or the UE has not provided it, then the International Mobile Equipment Identifier (IMEI) is used as UE identifier.

Figure 39: Call Flow: 3GPP R13 Emergency Call Support on the ePDG and P-GW



The P-GW sends the **Emergency-Indication** AVP over the s6b interface so that the 3GPP AAA server only applies specific policies for emergency services. For an unauthenticated UE, the 3GPP AAA server does not update the Home Subscriber Server (HSS) with the identity of the P-GW. For an authenticated UE, this indication is sent together with the "PDN GW currently in use for emergency services" message, which comprises the PDN GW address and the indication that the PDN connection is for emergency services to the HSS, which stores it as part of the UE context for emergency services.

Support is available for all four different behaviors of emergency bearer establishment:

- Valid UEs only.
- Only UEs that are authenticated are allowed.
- IMSI required, authentication optional.
- All UEs are allowed.

This section describes the new Attribute Value Pair (AVP) and modified Information Elements that support the feature.

Emergency-Indication AVP

A new **Emergency-Indication** AVP is defined in the Authentication and Authorization Request to signal a request to establish a PDN connection for emergency services.

Information Elements

This section describes other important elements in a Create Session Request that have been modified to work properly with the feature.

Table 50: Information Elements in a Create Session Request

Information Elements	P	Condition/Comment	IE Type	Ins.
IMSI	C	The IMSI is included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, except for the case: If the UE is emergency attached and the UE is UICCless. The IMSI shall be included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, but not used as an identifier. - If UE is emergency attached but IMSI is not authenticated. The IMSI is included in the message on the S2a/S2b interface.	IMSI	0

Information Elements	P	Condition/Comment	IE Type	Ins.
MSISDN	C	For an E-UTRAN Initial Attach and a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN the IE is included when used on the S11 interface, if provided in the subscription data from the HSS. For a PDP Context Activation procedure and a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN the IE is included when used on the S4 interface, if provided in the subscription data from the HSS. The IE is included for the case of a UE Requested PDN Connectivity, if the MME has it stored for that UE. It is included when used on the S5/S8 interfaces if provided by the MME/SGSN. The ePDG includes this IE on the S2b interface during an Attach with GTP on S2b , UE initiated Connectivity to Additional PDN with GTP on S2b and a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, Initial Attach for emergency session (GTP on S2b), if provided by the HSS/AAA. The TWAN includes this IE on the S2a interface during an Initial Attach in WLAN on GTP S2a, UE initiated Connectivity to Additional PDN with GTP on S2a and a Handover to TWAN with GTP on S2a, if provided by the HSS/AAA.	MSISDN	0
ME Identity (MEI)	C	The MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface: - If the UE is emergency attached and the UE is UICCless. - If the UE is emergency attached and the IMSI is not authenticated. For all other cases the MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface if it is available.	MEI	0
	CO	The TWAN/ePDG shall include the ME Identity (MEI) IE on the S2a/S2b interface, if it is available.		
Serving Network	C	This IE is included on the S4/S11, S5/S8 and S2b interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN, a UE requested PDN connectivity, an Attach with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b and an Initial Attach for emergency session (GTP on S2b).	Serving Network	0

Information Elements	P	Condition/Comment	IE Type	Ins.
Indication Flags	C	This IE shall be included if any one of the applicable flags is set to 1. Applicable flags are: - Unauthenticated IMSI: This flag is set to 1 on the S4/S11 and S5/S8 interfaces if the IMSI present in the message is not authenticated and is for an emergency attached UE.	Indication	0
Selection Mode	C	This IE is included on the S4/S11 and S5/S8 interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN and a UE requested PDN connectivity This IE is included on the S2b interface for an Initial Attach with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b and an Initial Attach for emergency session (GTP on S2b) The IE indicates whether a subscribed APN or a non-subscribed APN chosen by the UE/MME/SGSN/ePDG/TWAN was selected. This IE is included on the S2a interface for an Initial Attach in WLAN on GTP S2a, a Handover to TWAN with GTP on S2a and a UE initiated Connectivity to Additional PDN with GTP on S2a. The value is set to "MS or network provided APN, subscription verified".	Selection Mode	0
	CO	When available, this IE is sent by the MME/SGSN on the S11/S4 interface during TAU/RAU/HO with S-GW relocation.		
UE Local IP Address	CO	The ePDG includes this IE on the S2b interface during an Initial Attach for emergency session (GTP on S2b). Otherwise the ePDG shall include this IE on the S2b interface based on local policy.	IP Address	0
UE PDP Port	CO	The ePDG includes this IE on the S2b interface if NAT is detected and the UE Local IP Address is present.	Port Number	0
WLAN Location Information	CO	This IE is included on the S2b interface if the WLAN Location Information is available.	TWAN Identifier	1
WLAN Location Timestamp	CO	This IE is included on the S2b interface, if the WLAN Location Timestamp is available.	TWAN Identifier Timestamp	0

Emergency Handover Support

When a subscriber makes an emergency call over WLAN, user equipment (UE) adds *sos* to the *NAI* to indicate that this is an emergency attach to ePDG. ePDG informs P-GW about this emergency attach in create session request. When the caller moves away from WLAN into LTE coverage or vice versa, the call gets handed over without being dropped.

P-GW supports following emergency call handovers:

- **Handover of Emergency Calls from LTE to Wi-Fi(S2b)** : Handovers of emergency calls from LTE to Wi-Fi (S2b) for authenticated UE is supported. While the UE moves from LTE to untrusted Wi-Fi, LTE triggers an Authentication Authorization Request (AAR) to the S6b server with the AVP *Emergency-Indication* sent in that Authentication and Authorization Request (AAR). Also, an STR is sent when a Wi-Fi (S2b) call is cleared.:

  1. The ePDG sends Create Session Request to the P-GW.
  2. If the UE requested P-CSCF in the IKE Config request, P-CSCF is requested.
  3. Downlink packets are sent on LTE access. The ePDG includes the IP address that is received within the IKE message from the UE in the PAA (PDN Address Allocation) in the GTPv2 Create Session Request.
  4. The P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
  5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
  6. 3GPP AAA sends AAA to the P-GW.
  7. The Policy and Charging Rules Function (PCRF) acknowledges IP-CAN Session Modification with a Credit Control Answer (CCA).
  8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
  9. ePDG sends Create Bearer Response message.
  10. P-GW sends the Delete Bearer Request message.
  11. The S-GW sends Delete Bearer Response message to the P-GW.

- **Handover of Emergency Calls from Wi-Fi(S2b) to LTE** : Handover of Emergency Calls from Wi-Fi (s2b) to LTE for authenticated UE is supported. Since an emergency call in LTE does not have S6b interface authorization enabled, handover of emergency calls from untrusted Wi-Fi to LTE triggers a Session Termination Request (STR) to the S6b server:

  1. The MME selects the P-GW from the MME Emergency Configuration Data and sends a Create Session Request.
  2. The S-GW sends a Create Session Request.
  3. P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR), if Gx authentication is enabled or P-GW applies the local policy and does not query PCRF if local policy is configured. P-GW sends Session Termination Request to S6b server and P-GW provides IPv6 Prefix and/or IPv4 address in PAA.

Note If the MME indicates Piggyback support, then, the P-GW piggybacks the Create Bearer Request message to the Create Session Response message.

4. The MME sends a Modify Bearer Request message to the S-GW.
5. The S-GW processes each message independently. The S-GW forwards the Create Bearer Response to the P-GW(without piggybacking).

- **Emergency PDN Handover with HO=0**: Handovers from LTE to Wi-Fi is supported:

1. The ePDG sends Create Session Request to the P-GW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.

Note Downlink packets are dropped at the P-GW while the session is being handed over to WLAN.

2. P-GW checks for an LTE session.
3. If there is an LTE session, the P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
4. 3GPP AAA sends AAA to the P-GW.
5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
6. The PCRF acknowledges of IP-CAN Session Modification with a Credit Control Answer (CCA) message. This message includes the Policy and Charging rules. The P-GW enforces and triggers for events that must be reported by the P-GW.
7. If Online flag is enabled and if P-GW does not have quota for the WLAN rating group, or if Online Charging Server (OCS) has not sent a 4011 for the WLAN rating group previously, then the P-GW sends a CCR-u to the OCS reporting the usage.
8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
9. After the P-GW sends the Create Session Response, the P-GW sends an interim Accounting Request (ACR) to the OFCS.
10. The OFCS responds with an ACA to the P-GW.
11. P-GW sends the Delete Bearer Request to the S-GW.
12. The S-GW sends Delete Bearer Response to the P-GW.

Configuring AAA Failure Handling for S2b Emergency Calls

Emergency calls over the S2b interface should not be rejected due to a failure from the S6b server. To ensure this, failure handling must be configured in the APN which is used for emergency calls .

Handling is configured in the **aaa group** so that emergency calls continue regardless of failures as indicated by the result code.

To configure AAA failure handling for S2b emergency calls:

```
configure
  context ingress_context_name
    aaa group default
      diameter authentication failure-handling authorization-request
result-code 3000 to 5999 action continue
       diameter authentication failure-handling authorization-request
request-timeout action continue
          end
```

Note the following assumptions:

- If an IP-CAN Session Modification Request triggered by the PCRF removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signaling, then the PCEF starts a configurable emergency inactivity timer. When the configured period of time expires, the P-GW initiates an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session
- If the Gx/S6b interface returns a Virtual APN, which is not configured as an emergency APN, then the call is rejected with the cause code "APN_DENIED_NO_SUBSCRIPTION

To configure failure handling template for Gx failure (PCRF down):

```
configure
  failure-handling-template gx_template
   msg-type any failure-type diabase-error action continue local-fallback

       end
```

Following example shows failure handling template configuration for Gx failure (PCRF return ErrorCode):

```
configure
  failure-handling-template gx_template
     msg-type credit-control-initial failure-type diameter result-code
3000 to 5999 action continue local-fallback
       msg-type credit-control-update failure-type diameter result-code
 3000 to 5999 action continue local-fallback
           end
```

Following example shows failure handling template configuration for Gx delayed response:

```
configure
  failure-handling-template gx_template
    msg-type credit-control-initial failure-type resp-timeout action
continue
       msg-type credit-control-update failure-type resp-timeout action
```

```
continue
          end
```

To configure local policy for Gx failure (PCRF down or PCRF return ErrorCode):

```
configure
        local-policy-service service_name
          ruledef  ruledef_name
             condition priority  priority  { variable { eq | ge | gt | le |
 lt | match | ne | nomatch } regex | string_value | int_value | set }
            end
```

```
configure
  local-policy-service service_name
    actiondef   actiondef_name
      action priority  priorityaction_name arguments
        end
```

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

```
configure
  contextcontect_name
    ims-auth-service   service_name
      [ no ] policy-control
        associate failure-handling-template gx_template
          associate local-policy-service  service_name
            end
```

Configuring APN and S6b Authorization

Configuring APN to attach emergency PDN on LTE

For emergency PDN handover with S6b Gx, configure APN mode to attach emergency PDN on LTE.

```
configure
  context context_name
    apn apn_name
      emergency-apn
      end
```

Enabling S6b Authorization

Following is the sample configuration to enable S6b authorization:

```
configure
```

```
context context_name
  pgw-service service_name
    apn apn_name
      authorize-with-hss [ egtp[gn-gp-enabled] [ s2b [gn-gp-enabled]
 [ s5-s8 [gn-gp-enabled | gn-gp-enabled]] [ report-ipv6-addr ]| lma [
s6b-aaa-group aaa-group-name | report-ipv6-addr ] | report-ipv6-addr ]
[ default | no ] authorize-with-hss
       end
```

Enabling S2b Interface eGTP Service

Use the following configuration to enable S2b Interface eGTP service:

```
configure
  context context_name
    egtp-service service_name
      interface-type { interface-cgw-egress | interface-epdg-egress |
interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn |
 interface-sgw-egress | interface-sgw-ingress }
      end
```

Following the example configuration to enable S2b Interface eGTP service:

```
configure
       context EPC2
         egtp-service PGW21EGTP
          interface-type | interface-pgw-ingress [ s2b ] [ s2a ]
                          end
```

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature

Show Commands and Output

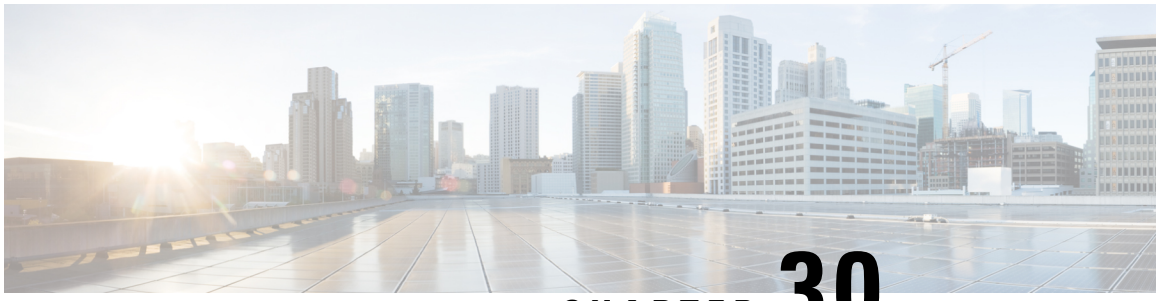
This section provides information regarding show commands and their outputs in support of the feature.

show apn

```
pdp type:  ipv4 and ipv6
apn type:  emergency
ehrpd access: N/A
absolute timeout :  0           idle timeout :  0
emergency inactivity timeout :  1000
idle-timeout-activity ignore-downlink:   Disabled
…..
```

show pgw- service-statistics-all

```
pgw# show pgw-service statistics all
PGW Node Level Statistics:
VPN Name: local
Total bearers active:
  Default bearers:    5                                  Dedicated bearers:  5
    Normal bearers:   2                                  UE-initiated:  0
    Emergency bearers (Auth-IMSI): 1                     Network-initiated: 5
    Emergency bearers (Unauth-IMSI):1                    Normal bearers:   2
    Emergency bearers (Only IMEI): 1                     Emergency bearers (Auth-IMSI):  1
    Emergency bearers (Unauth-IMSI):1

    Emergency bearers (Only IMEI): 1
```



CHAPTER 30

Expanded Prioritization for VoLTE/Emergency Calls

This chapter describes the StarOS support for the Expanded Prioritization for VoLTE/Emergency Calls feature on the P-GW, SAE-GW, and S-GW.

- Feature Description, on page 477
- How It Works, on page 479
- Configuring Expanded Prioritization for VoLTE/Emergency Calls, on page 480
- Monitoring and Troubleshooting the Expanded Prioritization for VoLTE/Emergency Calls, on page 482

Feature Description

The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

The DSCP marking of control message from P-GW and S-GW was based on associated egtpc-service configuration.

For control message belonging to eMPS session or containing Allocation and Retention Priority (ARP) associated with eMPS profile, the DSCP marking is based on eMPS profile configured DSCP value.

As part of this enhancement, support is also added for marking of certain GTP-C message at the P-GW and S-GW for priority treatment as defined in the Government Industry Requirements (GIR) NS/EP NGN.

Relationships to Other Features

Bulkstats for GTP-C Messages by ARP Value: The S-GW/P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW/P-GW level.

To prevent throttling of GTP-C messages corresponding to eMPS PDNs or messages containing ARP from set of configured ARP(PL) reserved for NS/EP NGN priority service, following configuration are to be considered:

1. **Load Overload control**

   In overload control profile, the set of ARPs reserved for NS/EP NGN-PS use for eMPS services should also be defined under **throttling-behavior exclude** and **self-protection-behavior exclude** CLI commands. This will ensure that incoming GTP-C messages for eMPS PDN or containing ARP from set of reserved ARP for eMPS use are not throttled. Example of configuring Load Overload configuration:

   ```
   configure
     gtpc-overload-control-profile profile_name
       throttling-behavior { earp { 1...15 } * } { exclude }
       self-protection-behavior { earp { 1...15 } * }  { exclude }
       end
   ```

2. **For Prioritized handling of calls under Congestion condition**

   ARP reserved under NS/EP NGN-PS for eMPS services is recommended to be configured under following congestion control CLI command. This will ensure that new call requests are not throttled during congestion condition defined by the **congestion-control** CLI command at context level:

   ```
   configure
     context context_name
       egtp-service service_name
         gtpc allow-on-congestion arp arp_value
         end
   ```

3. **GTP-C RLF Throttling**

   - If GTP-C RLF Throttling feature is enabled, then **gtpc overload-protection egress throttling-override-policy** CLI command should be configured with ARP(PL), reserved for NS/EP NGN-PS use, for eMPS services to bypass RLF throttling.
   - If GTP-C RLF Throttling for incoming messages is configured using **gtpc overload-protection ingress msg-rate** *message_rate* CLI command, then eMPS related messages can get throttled. Currently, there is no bypass policy for incoming RLF throttling.



Important Any existing features which works on ARP (PL) configurations will continue to work as before irrespective of whether ARP values configured are same as reserved under NS/EP NGN-PS for eMPS services. If existing features need to work with eMPS requirements, then same ARP (PL) values should be configured as reserved NS/EP NGN-PS for eMPS services.

Licensing

The DSCP marking capability requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

GIR Document References

The following table describes the requirements of this feature as per the GIR document.

Requirement No.	Description
R-127	[202] The S-GW shall transmit with priority a GTP-C “Downlink Data Notification” message or a GTP-C “Create Bearer Request” message or a GTP-C “Update Bearer Request” message, any of which contains an ARP chosen from the set allocated by the Service Provider for use by NS/EP NGN-PS.
R-130	[204] The S-GW shall mark for priority treatment the S11 “Create Session Response” message from the S-GW to the MME which contains request to establish a bearer or bearers with an ARP corresponding to an NS/EP NGN-PS call/session.
R-132	[205] The S-GW shall mark for priority treatment the S11 “Create Bearer Request” and S11 “Update Bearer Request” messages from the SGW to the MME which contains an indication that a UE currently has an established/updated bearer or bearers for NS/EP NGN-PS service.
R-134	[206] In the case where the S5/S8 Interface is GTP-based, the S-GW shall mark for priority treatment the S5/S8 “Create Session Request” message from the S-GW to the PDN-GW which contains an indication that a UE will establish a bearer or bearers for NS/EP NGN-PS.
R-137	[207] In the case where the S5/S8 Interface is GTP-based, the S-GW shall mark for priority treatment the S5/S8 “Create Bearer Response” and “Update Bearer Response” messages from the S-GW to the PDN-GW which contain an indication that a UE currently has established / updated a bearer or bearers for NS/EP NGN-PS.
R-143	[213] In the case where the S5/S8 Interface is GTP-based, the PDN-GW shall mark for priority treatment the S5/S8 “Create Session Response” message from the PDN-GW to the S-GW which contains a request to establish a bearer or bearers with an ARP corresponding to an NS/EP NGN-PS call/session.
R-146	[216] In the case where the S5/S8 Interface is GTP- based, the PDN-GW shall mark for priority treatment the S5/S8 “Create Bearer Request” and “Update Bearer Request” messages from the PDN-GW to the S-GW which contain an indication that a UE currently has an established/updated bearer or bearers for NS/EP NGN-PS.

Configuring Expanded Prioritization for VoLTE/Emergency Calls

The following section provides the configuration commands to enable the feature.

Configuring eMPS Profile and its Associated Attributes

At Configuration Mode level, CLI command option is introduced to define an eMPS profile and its associated attributes like:

- **eARP configuration**: This configuration is used for marking a bearer/PDN as an eMPS.
- **DSCP configuration**: This configuration is used at S-GW/P-GW to mark various outgoing GTP-C messages associated with an eMPS PDN with configured DSCP marking.

```
configure
   [ no ] emps-profile emps_profile_name -noconfirm
   [ no ] earp { [ 1...15 ] { [ 1...15 ] { [ 1...15 ] } } }
   [ no ] dscp-marking dscp_value
   end
```

Notes:

- **emps-profile** *emps_profile_name*: Configures eMPS profile for defining attributes of an eMPS session. The *emps_profile_name* is a string of size from 1 to 63.
- **earp**: Configures a maximum of 3 eARP priority level (PL) values so that sessions with configured eARP priority values can be marked as eMPS sessions.
- **-noconfirm**: Creates a new eMPS profile without prompting for confirmation.
- **dscp-marking** *dscp_value*: Specifies the DSCP value to be applied to eMPS sessions. The *dscp_value* is a hexadecimal number between 0x0 and 0x3F.
- Maximum of 3 eARP values can be configured under an eMPS profile. The above CLI syntax provides flexibility to configure one or more (max 3) eARP values in a single command. For example:

  earp 1 2 3

  -Or-

  earp 4
- The latest set of eARP values configured will overwrite the previous configuration. For example: Invoking below two commands in sequence will configure only eARP value 4.

  earp 1 2 3

  earp 4
- eMPS profile name should be unique and is treated case insensitive across context.
- The **no earp** command can be used to disable all configured eARP values. However, this will not delete the corresponding eMPS profile. The **no emps-profile** *emps_profile_name* CLI command will delete the profile.

- Warning message: When **no** of a non-existent eMPS profile is executed, a warning message is displayed. For example:

```
no emps-profile xyz
eMPS Profile : xyz does not exist
```

  There will be no warning message if **no** of an un-configured eARP is executed.

- There will be a warning and confirmation message when existing profile is deleted:

```
This operation will result in deletion of this eMPS Profile.
Are you sure? [Yes|No]:
```

- Maximum of 64 different eMPS profiles can be configured.

Associating an eMPS Profile with P-GW Service

The commands illustrated below associates an eMPS profile to P-GW service.

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no associate emps-profile**: Disables the feature.
- **emps-profile** *emps_profile_name*: Associates an eMPS profile with the P-GW service. The *emps_profile_name* is a string of size 1 to 63.
- The eMPS profile name in input is treated as case insensitive.
- By default, no eMPS profile is associated with pgw-service.
- For SAE-GW associated P-GW service, the eMPS profiles should be same as configured in associated S-GW service. In case of any discrepancy, it will be reported in the **show configuration error** CLI command output.

Associating an eMPS Profile with S-GW Service

The commands illustrated below associates an eMPS profile to S-GW service.

```
configure
  context context_name
    sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no associate emps-profile**: Disables the feature.
- **emps-profile** *emps_profile_name*: Associates an eMPS profile with the S-GW service. The *emps_profile_name* is a string of size 1 to 63.

- The eMPS profile name in input is treated as case insensitive.
- By default, no eMPS profile is associated with sgw-service.
- For SAE-GW associated S-GW service, the eMPS profiles should be same as configured in associated P-GW service. In case of any discrepancy, it will be reported in the **show configuration error** CLI command output.

Monitoring and Troubleshooting the Expanded Prioritization for VoLTE/Emergency Calls

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

Show Command(s) and/or Outputs

show emps-profile { all | name <emps_profile_name> }

The above CLI command is introduced to see a particular or all eMPS profile(s) configured with its associated attributes. Also, the output of an existing **show config [verbose]** CLI command is modified to reflect an eMPS configuration:

- **earp configured**: <earp_value>
- **dscp-marking configured**: <dscp-value>

These CLI commands can be used to verify if the configuration is appropriate.

show pgw-service { name <name> | all }

The output of this command is modified to reflect the eMPS profile associated with the P-GW service:

- **eMPS Profile Name** : <emps_profile_name>



Important Maximum of one eMPS profile can be associated with P-GW service at a time; the latest configuration will overwrite the previously associated configuration.

show sgw-service { name <name> | all }

The output of this command is modified to reflect the eMPS profile associated with the S-GW service:

- **eMPS Profile Name** : <emps_profile_name>



Important Maximum of one eMPS profile can be associated with S-GW service at a time; the latest configuration will overwrite the previously associated configuration.

show subscribers pgw-only full all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Username: 0123456789@username
 Subscriber Type   : Visitor
 Status            : Online/Active
 State             : Connected
 Connect Time      : Wed Sep  7 07:02:49 2016
 Auto Delete       : No
 Idle time         : 00h00m08s
 MS TimeZone       : n/a                    Daylight Saving Time: n/a
 Access Type: gtp-pdn-type-ipv4             Network Type: IP
 Access Tech: eUTRAN                        pgw-service-name: pgw_service
 Callid: 00004e21                           IMSI: 123456789012341
 MSISDN: 0123456789
 Interface Type: S5S8GTP                    Low Access Priority: N/A
 TWAN Mode: N/A
 eMPS Bearer: Yes
 Emergency Bearer Type: N/A
 IMS-media Bearer: No
```

show subscribers saegw-only full all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Username: 0123456789@username
 SAEGW Call mode   : Co-located
 Subscriber Type   : Home
 .
 .
 .
 MSISDN: 0123456789
 TWAN Mode: N/A
 eMPS Bearer: Yes
 MS TimeZone       :                     Daylight Saving Time: n/a
 MEI               : 1122334455667788    Accounting mode      : GTPP
```

show pgw-service statistics

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:               0    Setup:            0
   Authentic IMSI:      0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                  1       Cumulative Activated:   1
  Cumulative De-activated:         1
IPv4v6 PDN-Type Received with DAF False :         0
```

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.

- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show saegw-service statistics all function pgw

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:              0    Setup:            0
   Authentic IMSI:     0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         1
IPv4v6 PDN-Type Received with DAF False :         0
```

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.
- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show saegw-service statistics

The output of this command is modified to display the eMPS statistics for PGW-Anchored/SGW-Anchored PDNs associated with the saegw-service. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:              0    Setup:            0
  Released:      0
 .
 .
 .
eMPS PDNs:
 Colocated PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
 PGW-Anchor PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
 SGW-Anchor PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
```

The above statistics information are further classified based on SAE-GW call types:

- **Colocated eMPS PDNs**: It reflects the eMPS PDN statistics information for collapsed PDNs.
- **PGW-Anchor eMPS PDNs**: It reflects the eMPS PDN statistics information for PGW-Anchor PDNs.

- **SGW-Anchor eMPS PDNs**: It reflects the eMPS PDN statistics information for SGW-Anchor PDNs.

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.
- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show sgw-service statistics all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Subscribers Total:
  Active:               0    Setup:            2
  Released:             1
 .
 .
 .
eMPS PDN Statistics:
  Current Active:                   1       Cumulative Activated:    1
  Cumulative De-activated:          0
```

show saegw-service statistics all function sgw

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
Subscribers Total:
  Active:               0    Setup:            0
  Released:             0
 .
 .
 .
eMPS PDN Statistics:
  Current Active:                   1       Cumulative Activated:    1
  Cumulative De-activated:          0
```

show configuration error

System will show configuration errors for following scenarios:

- When different eMPS profiles are configured under pgw-service and sgw-service associated to same sae-gw service. For example:

```
##############################################################
    Displaying SAEGW-Service system errors
##############################################################
Error   : eMPS profile of SGW <sgw-service> and PGW service <pgw_service>
is not same for SAEGW service <saegw-service> in the context <context_name>.
Total 1 error(s) in this section !
```

- When non-existent emps-profile is associated to pgw-service. For example:

```
##############################################################
    Displaying PGW-Service system errors
##############################################################
```

```
Error   : eMPS Profile <emps_profile_pgw> configured for PGW service <pgw_service>
is not present in the system
Total 1 error(s) in this section !
```

- When non-existent emps-profile is associated to sgw-service. For example:

```
##########################################################
    Displaying SGW-Service system errors
##########################################################
Error   : eMPS Profile <emps_profile_sgw> configured for SGW service <sgw_service>
is not present in the system
Total 1 error(s) in this section !
```

Bulkstats for Expanded Prioritization for VoLTE/Emergency Calls

PGW Schema

The following bulk statistics have been added to the P-GW schema as part of this enhancement:

- sessstat-pdn-emps-current-active – The total number of currently active P-GW eMPS PDNs.
- sessstat-pdn-emps-cumulative-activated – The total number of P-GW PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sessstat-pdn-emps-cumulative-deactivated – The total number of P-GW PDNs that were either released or degrades to a non-eMPS PDN.

SGW Schema

The following bulk statistics have been added to the S-GW schema as part of this enhancement:

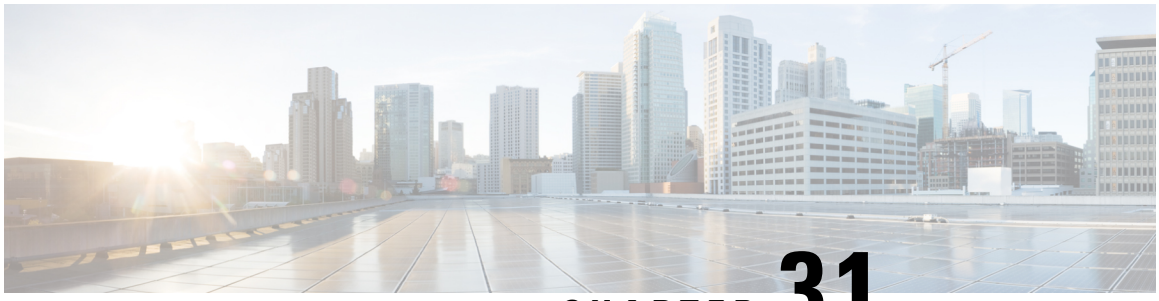
- sessstat-pdn-emps-current-active – The total number of currently active S-GW eMPS PDNs.
- sessstat-pdn-emps-cumulative-activated – The total number of S-GW PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sessstat-pdn-emps-cumulative-deactivated – The total number of S-GW PDNs that were either released or degrades to a non-eMPS PDN.

SAEGW Schema

The following bulk statistics have been added to the SAE-GW schema as part of this enhancement:

- pgw-anchor-pdns-emps-current-active – The total number of currently active P-GW anchored eMPS PDNs.
- pgw-anchor-pdns-emps-cumulative-activated – The total number of P-GW anchored PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- pgw-anchor-pdns-emps-cumulative-deactivated – The total number of P-GW anchored PDNs that were either released or degrades to a non-eMPS PDN.
- saegw-colocated-pdns-emps-current-active – The total number of currently active SAE-GW collapsed eMPS PDNs.
- saegw-colocated-pdns-emps-cumulative-activated – The total number of SAE-GW collapsed PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.

- saegw-colocated-pdns-emps-cumulative-deactivated – The total number of SAE-GW collapsed PDNs that were either released or degrades to a non-eMPS PDN.
- sgw-anchor-pdns-emps-current-active – The total number of currently active S-GW anchored eMPS PDNs.
- sgw-anchor-pdns-emps-cumulative-activated – The total number of S-GW anchored PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sgw-anchor-pdns-emps-cumulative-deactivated – The total number of S-GW anchored PDNs that were either released or degrades to a non-eMPS PDN.



CHAPTER 31

Extended QCI Options

This chapter describes extended QCI functionality.

- Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters, on page 489
- DSCP Marking Based on Both QCI and ARP Values, on page 502
- New Standard QCI Support, on page 505
- Non-standard QCI Support, on page 542

Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Feature Description

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

Important For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

The existing **show apn statistics name** *apn-name* and **show apn statistics** *Exec Mode* CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.

Licensing

Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring ARP Granularity for QCI Level Counters

This section describes how to configure the ARP Granularity for QCI Level Counters feature.

Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring the feature consists of the following tasks:

1. Create a Stats Profile.
2. Enable the Collection of Per QCI Packet Drop Counters.
3. Enable the Collection of QCI/ARP Level Statistics.
4. Associate a Stats Profile with an APN.
5. Verify the Configuration.

Create a Stats Profile

Use the following example to access *Global Configuration Mode* and create a Stats Profile:

```
configure
  stats-profile stats_profile_name
  end
```

Notes:

- *stats_profile_name* must be an alphanumeric string from 1 to 63 characters in length.

Enable the Collection of Packet Drop Statistics

Use the following example to access *Stats Profile Configuration Mode* and create a Stats Profile and enable the collection of packet drop statistics:

```
configure
  stats-profile stats_profile_name
    packet-drop
    end
```

To disable the collection of packet drop statistics

```
configure
  stats-profile stats_profile_name
    no packet-drop
    end
```

Notes:

- *stats_profile_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- **packet-drop**: enables the collection of packet drop statistics for the specified Stats Profile.
- **no packet-drop**: disables the collection of packet drop statistics for the specified Stats Profile.

Enable the Collection of QCI/ARP Level Statistics

Use the following example to access *Stats Profile Configuration Mode* and enable the collection of QCI/ARP level statistics for a Stats Profile:

```
configure
  stats-profile stats_profile_name
    qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
 |12 | 13 | 14 | 15 ] + } }
    end
```

To disable the collection of QCI/ARP statistics:

```
configure
  stats-profile stats_profile_name
  no qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
 |12 | 13 | 14 | 15 ] + } }
  end
```

Notes:

- *stats_proflle_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 64 characters in length.
- **qci**: configures the collection of ARP priority level statistics for the specified QCI(s).
- **non-std**: configures the collection of ARP priority level statistics for non-standard QCIs.
- **non-gbr**: configures the collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.

- **gbr**: configures the collection of ARP priority level statistics for non-standard GBR QCIs.
- **arp**: configures the collection of ARP priority level statistics for the specified ARP values.
- **no**: disables the collection of ARP priority level statistics for the specified **qci** and **arp** settings.

Associate a Stats Profile with an APN

Use the following example to access *APN Configuration Mode* and associate a Stats Profile with an APN:

```
configure
  apn apn_name
    stats-profile stats_profile_name
    end
```

To disassociate a Stats Profile from a specified APN:

```
configure
  apn apn_name
    no stats-profile
    end
```

Notes:

- *stats_profile_name*: must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- A maximum of 64 Stats Profiles can be configured per P-GW/SAEGW/GGSN service.
- **no stats-profile**: disassociates the Stats Profile from the APN.



Important If a Stats Profile is associated with more than 12 APNs, the following memory and performance impact warning is provided:

```
[WARNING] Configuring QCI/ ARP level statistics for more then 12 APNs will have
memory and performance impact. Do you want to continue [Y/N]
```

Verify the Configuration

Use the following procedure to verify the configuration:

First, verify that the Stats Profile is associated with the correct APN. In *Exec Mode*, enter the following command:

```
show apn name apn_name
```

Notes:

- In the command output, look for the **stats profile** field. It should contain the name of the Stats Profile which is associated with this APN.

Next, verify that the Stats Profile configuration settings are correct. In *Exec Mode*, enter the following command:

```
show stats-profile name stats_profile_name
```

Notes:

- Where *stats_profile_name* is the name of the Stats Profile for which you want to view settings.
- The command output includes the following information:
  - Stats Profile name
  - Packet-drop configuration settings for both QCI and ARP
  - QCI ARP combinations for which the StarOS will collect granular ARP statistics

If any of the above settings are incorrect, perform the configuration procedure again to reconfigure the Stats Profile with the proper settings.

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes how to monitor the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Bulk Statistics

This section provides the bulk statistics that have been added to support the ARP Granularity and per QCI Packet Drop Counters feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
```

```
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

Show Commands

This section provides the Exec Mode show commands that are available to support the Per Packet QCI Drop Counters and ARP Granularity for QCI Level Counters feature.

show apn statistics

The **qci** and **arp** keywords have been added to this command. The new keywords enable operators to view output for four basic scenarios that apply to the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Scenario 1

View packet drop counters with granularity at the QCI/ARP level for a single APN. The output of this command is useful for isolating network issues that may be affecting packet drops.

show apn statistics name *apn_name* **qci { all | 1-9 | non-std { gbr | non-gbr } } arp { all | 1-15 }**

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.

- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 2

View packet drop counters with granularity at the QCI/ARP level for all APNs.

```
show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } } arp {
all | 1-15 }
```

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 3

View the new packet drop counters at granularity of QCI level, and pre-existing QCI level counters for the specified APN.

```
show apn statistics name apn_name qci { all | 1-9 | non-std { gbr | non-gbr
 } }
```

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).

- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 4

View the packet drop counters at the granularity of the QCI level, and view pre-existing QCI counters consolidated for all APNs.

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } }

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

The output of the **show apn statistics name** *apn_name* **qci all arp all** command has been enhanced to display the following new statistics:

```
Data Statistics:

    Uplink Bytes:                0   Downlink Bytes:                          0
    Uplink Pkts:                 0   Downlink Pkts:                           0
    Uplink Bytes dropped:        0   Downlink Bytes dropped:                  0
    Uplink Pkts dropped:         0   Downnlink Pkts dropped:                  0

  Uplink Dropped:                          Downlink Dropped:
    MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                  0
    MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                   0
    AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):                 0
    AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                  0
    Miscellaneous(Bytes):                0  Miscellaneous(Bytes):                 0
    Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                  0
    Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):             0
    Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):              0
    SGW Restoration(Bytes):              0  SGW Restoration(Bytes):               0
```

```
    SGW Restoration(Pkts):                  0  SGW Restoration(Pkts):                  0
    SDF Gate(Bytes):                        0  SDF Gate(Bytes):                        0
    SDF Gate(Pkts):                         0  SDF Gate(Pkts):                         0
    ITC Gate(Bytes):                        0  ITC Gate(Bytes):                        0
    ITC Gate(Pkts):                         0  ITC Gate(Pkts):                         0
    Flow Terminated(Bytes):                 0  Flow Terminated(Bytes):                 0
    Flow Terminated(Pkts):                  0  Flow Terminated(Pkts):                  0
    Subsession Terminated(Bytes):           0  Subsession Terminated(Bytes):           0
    Subsession Terminated(Pkts):            0  Subsession Terminated(Pkts):            0
    Call Terminated(Bytes):                 0  Call Terminated(Bytes):                 0
    Call Terminated(Pkts):                  0  Call Terminated(Pkts):                  0
    DCCA Discard(Bytes):                    0  DCCA Discard(Bytes):                    0
    DCCA Discard(Pkts):                     0  DCCA Discard(Pkts):                     0
    No Rule Match(Bytes):                   0  No Rule Match(Bytes):                   0
    No Rule Match(Pkts):                    0  No Rule Match(Pkts):                    0
    ICAP(Bytes):                            0  ICAP(Bytes):                          N/A
    ICAP(Pkts):                             0  ICAP(Pkts):                           N/A
    SFW(Bytes):                             0  SFW(Bytes):                             0
    SFW(Pkts):                              0  SFW(Pkts):                              0
    Hierarchical ENF(Bytes):                0  Hierarchical ENF(Bytes):                0
    Hierarchical ENF(Pkts):                 0  Hierarchical ENF(Pkts):                 0
    Dynamic CA Gate(Bytes):                 0  Dynamic CA Gate(Bytes):    :            0
    Dynamic CA Gate(Pkts):                  0  Dynamic CA Gate(Pkts):                  0
    NAT64 Cancel(Bytes):                    0  NAT64 Cancel(Bytes):                    0
    NAT64 Cancel(Pkts):                     0  NAT64 Cancel(Pkts):                     0
    Bearer Not Found(Bytes):                0  Bearer Not Found(Bytes):                0
    Bearer Not Found(Pkts):                 0  Bearer Not Found(Pkts):                 0


4G Bearers Released By Reasons:
                 QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
```

```
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0


Subscriber QoS Statistics:


4G Bearers Released By Reasons:
                QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0

  QCI 1:
```

```
 ARP 1:
  Bearer Active:                0   Bearer setup:                                2
  Bearer Released:              2   Bearer Rejected:                             0

  Uplink Bytes forwarded:       0   Downlink Bytes forwarded:                    0
  Uplink Pkts forwarded:        0   Downlink Pkts forwarded:                     0
  Uplink Bytes dropped:         0   Downlink Bytes dropped:                      0
  Uplink Pkts dropped:          0   Downlink Pkts dropped:                       0
 Uplink Dropped:                          Downlink Dropped:
  MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                  0
  MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                   0
  AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):                 0
  AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                  0
  Miscellaneous(Bytes):                0  Miscellaneous(Bytes):                 0
  Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                  0
  Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):             0
  Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):              0
  SGW Restoration(Bytes):              0  SGW Restoration(Bytes):               0
  SGW Restoration(Pkts):               0  SGW Restoration(Pkts):                0
  SDF Gate(Bytes):                     0  SDF Gate(Bytes):                      0
  SDF Gate(Pkts):                      0  SDF Gate(Pkts):                       0
  ITC Gate(Bytes):                     0  ITC Gate(Bytes):                      0
  ITC Gate(Pkts):                      0  ITC Gate(Pkts):                       0
  Flow Terminated(Bytes):              0  Flow Terminated(Bytes):               0
  Flow Terminated(Pkts):               0  Flow Terminated(Pkts):                0
  Subsession Terminated(Bytes):        0  Subsession Terminated(Bytes):         0
  Subsession Terminated(Pkts):         0  Subsession Terminated(Pkts):          0
  Call Terminated(Bytes):              0  Call Terminated(Bytes):               0
  Call Terminated(Pkts):               0  Call Terminated(Pkts):                0
  DCCA Discard(Bytes):                 0  DCCA Discard(Bytes):                  0
  DCCA Discard(Pkts):                  0  DCCA Discard(Pkts):                   0
  No Rule Match(Bytes):                0  No Rule Match(Bytes):                0
  No Rule Match(Pkts):                 0  No Rule Match(Pkts):                 0
  ICAP(Bytes):                         0  ICAP(Bytes):                        N/A
  ICAP(Pkts):                          0  ICAP(Pkts):                         N/A
  SFW(Bytes):                          0  SFW(Bytes):                           0
  SFW(Pkts):                           0  SFW(Pkts):                            0
  Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):              0
  Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):               0
  Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :          0
  Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):                0
  NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                  0
  NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                   0
  Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):              0
  Bearer Not Found(Pkts):              0  Bearer Not Found(Pkts):               0
QCI 1:
 ARP 2:
  Bearer Active:                0   Bearer setup:                                2
  Bearer Released:              2   Bearer Rejected:                             0

  Uplink Bytes forwarded:       0   Downlink Bytes forwarded:                    0
  Uplink Pkts forwarded:        0   Downlink Pkts forwarded:                     0
  Uplink Bytes dropped:         0   Downlink Bytes dropped:                      0
  Uplink Pkts dropped:          0   Downlink Pkts dropped:                       0
 Uplink Dropped:                          Downlink Dropped:
  MBR Exceeded(Bytes):          0  MBR Exceeded(Bytes):                  0
  MBR Exceeded(Pkts):           0  MBR Exceeded(Pkts):                   0
  AMBR Exceeded(Bytes):         0  AMBR Exceeded(Bytes):                 0
  AMBR Exceeded(Pkts):          0  AMBR Exceeded(Pkts):                  0
  Miscellaneous(Bytes):         0  Miscellaneous(Bytes):                 0
  Miscellaneous(Pkts):          0  Miscellaneous(Pkts):                  0
  Overcharge Prtctn(Bytes)      0  Overcharge Prtctn(Bytes):             0
  Overcharge Prtctn(Pkts):      0  Overcharge Prtctn(Pkts):              0
  SGW Restoration(Bytes):       0  SGW Restoration(Bytes):               0
```

```
    SGW Restoration(Pkts):          0  SGW Restoration(Pkts):                0
    SDF Gate(Bytes):                0  SDF Gate(Bytes):                      0
    SDF Gate(Pkts):                 0  SDF Gate(Pkts):                       0
    ITC Gate(Bytes):                0  ITC Gate(Bytes):                      0
    ITC Gate(Pkts):                 0  ITC Gate(Pkts):                       0
    Flow Terminated(Bytes):         0  Flow Terminated(Bytes):               0
    Flow Terminated(Pkts):          0  Flow Terminated(Pkts):                0
    Subsession Terminated(Bytes):   0  Subsession Terminated(Bytes):          0
    Subsession Terminated(Pkts):    0  Subsession Terminated(Pkts):           0
    Call Terminated(Bytes):         0  Call Terminated(Bytes):               0
    Call Terminated(Pkts):          0  Call Terminated(Pkts):                0
    DCCA Discard(Bytes):            0  DCCA Discard(Bytes):                  0
    DCCA Discard(Pkts):             0  DCCA Discard(Pkts):                   0
    No Rule Match(Bytes):           0  No Rule Match(Bytes):                 0
    No Rule Match(Pkts):            0  No Rule Match(Pkts):                  0
    ICAP(Bytes):                    0  ICAP(Bytes):                        N/A
    ICAP(Pkts):                     0  ICAP(Pkts):                         N/A
    SFW(Bytes):                     0  SFW(Bytes):                           0
    SFW(Pkts):                      0  SFW(Pkts):                            0
    Hierarchical ENF(Bytes):        0  Hierarchical ENF(Bytes):              0
    Hierarchical ENF(Pkts):         0  Hierarchical ENF(Pkts):               0
    Dynamic CA Gate(Bytes):         0  Dynamic CA Gate(Bytes):    :          0
    Dynamic CA Gate(Pkts):          0  Dynamic CA Gate(Pkts):                0
    NAT64 Cancel(Bytes):            0  NAT64 Cancel(Bytes):                  0
    NAT64 Cancel(Pkts):             0  NAT64 Cancel(Pkts):                   0
    Bearer Not Found(Bytes):        0  Bearer Not Found(Bytes):              0
    Bearer Not Found(Pkts):         0  Bearer Not Found(Pkts):               0
```

The output of the **show apn statistics name** *apn_name* **qci all** command has been enhanced to display the following new statistics:

```
Data Statistics:

    Uplink Bytes:                   0   Downlink Bytes:                       0
    Uplink Pkts:                    0   Downlink Pkts:                        0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:               0
    Uplink Pkts dropped:            0   Downnlink Pkts dropped:               0

  Uplink Dropped:                         Downlink Dropped:
    MBR Exceeded(Bytes):              0   MBR Exceeded(Bytes):                0
    MBR Exceeded(Pkts):               0   MBR Exceeded(Pkts):                 0
    AMBR Exceeded(Bytes):             0   AMBR Exceeded(Bytes):               0
    AMBR Exceeded(Pkts):              0   AMBR Exceeded(Pkts):                0
    Miscellaneous(Bytes):             0   Miscellaneous(Bytes):               0
    Miscellaneous(Pkts):              0   Miscellaneous(Pkts):                0
    Overcharge Prtctn(Bytes)          0   Overcharge Prtctn(Bytes):           0
    Overcharge Prtctn(Pkts):          0   Overcharge Prtctn(Pkts):            0
    SGW Restoration(Bytes):           0   SGW Restoration(Bytes):             0
    SGW Restoration(Pkts):            0   SGW Restoration(Pkts):              0
    SDF Gate(Bytes):                  0   SDF Gate(Bytes):                    0
    SDF Gate(Pkts):                   0   SDF Gate(Pkts):                     0
    ITC Gate(Bytes):                  0   ITC Gate(Bytes):                    0
    ITC Gate(Pkts):                   0   ITC Gate(Pkts):                     0
    Flow Terminated(Bytes):           0   Flow Terminated(Bytes):             0
    Flow Terminated(Pkts):            0   Flow Terminated(Pkts):              0
    Subsession Terminated(Bytes):     0   Subsession Terminated(Bytes):       0
    Subsession Terminated(Pkts):      0   Subsession Terminated(Pkts):        0
    Call Terminated(Bytes):           0   Call Terminated(Bytes):             0
    Call Terminated(Pkts):            0   Call Terminated(Pkts):              0
    DCCA Discard(Bytes):              0   DCCA Discard(Bytes):                0
    DCCA Discard(Pkts):               0   DCCA Discard(Pkts):                 0
    No Rule Match(Bytes):             0   No Rule Match(Bytes):               0
    No Rule Match(Pkts):              0   No Rule Match(Pkts):                0
    ICAP(Bytes):                      0   ICAP(Bytes):                      N/A
    ICAP(Pkts):                       0   ICAP(Pkts):                       N/A
```

```
    SFW(Bytes):                          0  SFW(Bytes):                          0
    SFW(Pkts):                           0  SFW(Pkts):                           0
    Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):             0
    Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):              0
    Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :          0
    Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):              0
    NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                 0
    NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                  0
    Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):             0
    Bearer Not Found(Pkts):              0  Bearer Not Found(Pkts):              0

4G Bearers Released By Reasons:

                      QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8    QCI9
   Admin disconnect:     0     0     0     0     0     0     0     0       0


Subscriber QoS Statistics:

  QCI 1:
    Bearer Active:                   0   Bearer setup:                          0
    Bearer Released:                 0   Bearer Rejected:                       0

    Uplink Bytes forwarded:          0   Downlink Bytes forwarded:              0
    Uplink Pkts forwarded:           0   Downlink Pkts forwarded:               0
    Uplink Bytes dropped:            0   Downlink Bytes dropped:                0
    Uplink Pkts dropped:             0   Downlink Pkts dropped:                 0
  Uplink Dropped:                          Downlink Dropped:
    MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                0
    MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                 0
    AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):               0
    AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                0
    Miscellaneous(Bytes):                0  Miscellaneous(Bytes):               0
    Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                0
    Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):           0
    Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):            0
    SGW Restoration(Bytes):              0  SGW Restoration(Bytes):             0
    SGW Restoration(Pkts):               0  SGW Restoration(Pkts):              0
    SDF Gate(Bytes):                     0  SDF Gate(Bytes):                    0
    SDF Gate(Pkts):                      0  SDF Gate(Pkts):                     0
    ITC Gate(Bytes):                     0  ITC Gate(Bytes):                    0
    ITC Gate(Pkts):                      0  ITC Gate(Pkts):                     0
    Flow Terminated(Bytes):              0  Flow Terminated(Bytes):             0
    Flow Terminated(Pkts):               0  Flow Terminated(Pkts):              0
    Subsession Terminated(Bytes):        0  Subsession Terminated(Bytes):       0
    Subsession Terminated(Pkts):         0  Subsession Terminated(Pkts):        0
    Call Terminated(Bytes):              0  Call Terminated(Bytes):             0
    Call Terminated(Pkts):               0  Call Terminated(Pkts):              0
    DCCA Discard(Bytes):                 0  DCCA Discard(Bytes):                0
    DCCA Discard(Pkts):                  0  DCCA Discard(Pkts):                 0
    No Rule Match(Bytes):                0  No Rule Match(Bytes):               0
    No Rule Match(Pkts):                 0  No Rule Match(Pkts):                0
    ICAP(Bytes):                         0  ICAP(Bytes):                      N/A
    ICAP(Pkts):                          0  ICAP(Pkts):                       N/A
    SFW(Bytes):                          0  SFW(Bytes):                         0
    SFW(Pkts):                           0  SFW(Pkts):                          0
    Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):            0
    Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):             0
    Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :        0
    Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):              0
    NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                0
    NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                 0
    Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):            0
```

```
    Bearer Not Found(Pkts):                0  Bearer Not Found(Pkts):                0

.
.
.
QCI 9:
    Bearer Active:                  0   Bearer setup:                           0
    Bearer Released:                0   Bearer Rejected:                        0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:               0
    Uplink Pkts forwarded:          0   Downlink Pkts forwarded:                0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                 0
    Uplink Pkts dropped:            0   Downlink Pkts dropped:
```

show configuration

The output of this command has been enhanced to show the Stats Profile configuration settings.

- stats-profile <*stats_profile_name*>
- qci <*qci number*> arp <*arp number*>
- packet-drop (*if packet-drop is enabled*)

show stats-profile name

This new command in *Exec Mode* shows the configuration settings for the specified Stats Profile.

- Stats Profile Name: <*stats_profile_name*>
- qci <*qci number*> arp <*arp_number(s)*>
- packet-drop <*if packet drop is enabled*>

DSCP Marking Based on Both QCI and ARP Values

Feature Description

P-GW allows users to perform DSCP marking based on QoS Class Identifier (QCI) values. This functionality has been expanded to include the Priority Level (PL) values 1-15 of Allocation and Retention Priority (ARP), which allows users to assign different DSCP values for bearers with the same QCI but different ARP priority values. For example, the ability to assign DSCP values based on QCI+ARP could be used to meet compliance on priority and emergency calling via VoLTE.

Applies to the P-GW for the following interfaces:

- S5
- S8
- SGi
- S2b

Applies to the S-GW for the following interfaces:

- S1-U
- S5
- S8
- S11
- S4

Relationships to Other Features

ECS populates the DSCP values in inner IP header. These values are fetched from the DSCP table by means of a sessmanager API. Since DSCP values are now available for QCI-ARP combination, the API is replaced by a wrapper API that will accept both QCI and ARP and provide the DSCP values to ECS in a new data structure.

The API will return correct values in the following scenarios:

1. QCI-DSCP table is not configured, or it is not associated for this session.

   API will return an indication to ECS that table was not found.

2. Table is configured, but entry for the given QCI value is not present in the table.

   API will not populate the structure and keep the same unaltered.

3. Entry for given QCI is present, but it is not available for the given QCI-ARP pair.

   The default DSCP values for that particular QCI will be populated in the return structure.

4. Entry for given QCI-ARP combination is present.

   The DSCP values for given QCI-ARP combination will be populated in the return structure.

Once values are received from SM, ECS caches these values and uses the cached values for marking the further packets. Another lookup into the table is done only when there is a mismatch between the currently cached QCI-ARP value and the current packet's QCI-ARP value. Therefore, any change in the QCI-ARP table would be affected for inner DSCP marking on existing flows only in case of QCI or ARP change.

Licensing

DSCP marking capability requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

The expansion of functionality to allow assigning different DSCP values for bearers with the same QCI, but different APR values, works as follows.

- DSCP marking of packets based on QCI+ARP combination allowed
- QCI + ARP configuration will override any DSCP entry for that QCI+ARP combination
- QCI only DSCP entry will override all existing QCI+ARP configuration
- Applying associated DSCP marking for QCI+ARP for Uplink and Downlink functionality is also allowed

Configuring DSCP Marking Based on Both QCI and ARP Values

This section describes how to configure DSCP marking based on both QCI and ARP values.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI and ARP values to enforceable Quality of Service (QoS) parameters:

```
configure
   qci-qos-mapping name
      qci num [ arp-priority-level arp_value ] [ downlink [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ] [ internal-qos priority priority ] [ user-datagram dscp-marking dscp-marking-value  ] ] [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ]  [ internal-qos priority priority ]  [ user-datagram dscp-marking dscp-marking-value  ] ]
      end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values. In addition, QCI values 65, 66, 69, and 70 can be used in StarOS release 21.0 and later.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs are supported and carriers can define QCI 128- 254.

- **arp-priority-level** *arp_value*: Specifies the address retention priority (ARP) priority level.

  arp_value must be an integer from 1 through 15.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Use the following example to disable QCI and ARP values:

```
configure
   qci-qos-mapping name
      no qci num [ arp-priority-level arp_value ]
      end
```

Associating QCI-QoS Mapping Configuration

Use the following example to specify that the P-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
   contextcontext_name
      pgw-service pgw_service_name
         associate qci-qos-mapping name
         end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Use the following example to specify that the S-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
  context context_name
    sgw-service sgw_service_name
      associate qci-qos-mapping name
      end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Configuring CS5 Marking for GTP-C

Use the following example to mark DSCP precedence CS5 on control packets:

```
configure
  context context_name
    ggsn-service ggsn_service_name
      ip qos-dscp gtpc cs5
      end
```

Notes:

- Designates Class Selector 5 DSCP precedence for GTP-C packets.

Verifying the Configuration

Use the following command in Exec mode to display/verify the configuration.

```
show configuration
```

Monitoring DSCP Marking Based on Both QCI and ARP Values

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of DSCP marking based on both QCI and ARP values.

show qci-qos-mapping table all

The output of this command has been enhanced to show the ARP value:

- arp-priority-level

New Standard QCI Support

CDETS: CSCuy20910 - Support of new standard QCIs (65, 66, 69, 70)

Applicable Products: P-GW, SAEGW, S-GW

Feature Description

The P-GW/SAEGW/S-GW support additional new 3GPP-defined standard QCIs. QCIs 65, 66, 69, and 70 are now supported for Mission Critical and Push-to-Talk (MCPTT) applications. These new standard QCIs are supported in addition to the previously supported QCIs of 1 through 9, and operator-defined QCIs 128 through 254.

The StarOS will continue to reject QCIs 10 through 127 sent by the PCRF.

Licensing



Important New Standard QCI Support is a licensed feature. Contact your Cisco account or support representative for licensing details.

How it Works

Although the 3GPP specification mentions that only QCIs 65 and 69 can co-exist, there is no hard restriction on the QCIs in the StarOS implementation of this feature, as that is applicable to the PCRF. The P-GW acts as a pass-through node and allows QCIs 65 and 69 if a different QCI combination is requested from PCRF.

With support for standard QCIs 65, 66, 69, and 70 present, the implementation has also added support across the following StarOS interfaces:

- **Gx**: Gx processes Default Bearer QoS and Rule Validation allowing the new Mission Critical (MC)/Push to Talk (PTT) QCIs. When the MC/PTT bit is not negotiated with the PCRF, the PCEF will reject the creation of a bearer or reject call setup.
- **sessmgr**: The P-GW sessmgr now processes the updating and modification of QoS. The P-GW rejects all UE initiated BRC creation for the new standard QCIs.
- **ECS**: ECS accepts the new standard QCIs when received from the PCRF and will reject them when either the license is not configured or the same is received in 3G. The ECS is able to update a Default bearer with this QoS change or create a Dedicated Bearer for the new standard QCIs.

Handoff Behavior

For Gn/Gp handoffs, local mapping via the CLI is supported so that the P-GW/SAEGW/S-GW is in sync with the MME-to-SGSN context transfer. The following scenarios are supported:

No Local QoS Mapping Present: When no local mapping is present for the new QCIs, a call handoff from 4G to 3G will be rejected.

Local QoS Mapping Present: Three scenarios are supported when local mapping is present:

- **Local Mapping present for MME-SGSN and PCRF Out of Synchronization**: When local mapping is present it is assumed that the QoS mapping in the P-GW is in sync with the mapping from the MME to SGSN. Even if the QoS mapping for one of the transferred PDPs during a Gn/Gp handoff is not in sync with MME-SGSN mapping, the P-GW/SAEGW/S-GW still continues with the handoff with the local mapping present. However, the CDR generated while waiting for the PCRF response during the handoff would be out of sync with the CDR's received after the handoff.

- **Mapping present for MME-SGSN and PCRF in Synchronization**: When local mapping is in sync with the MME-SGSN there is no difference in the CDR generated after the handoff.
- **Partial Mapping Present**: Partial mapping occurs when some MC/PTT QCI(s) have mapping and the remainder of the MC/PTT QCI(s) do not have mapping. In this case the call is dropped.

Expected Call Flow Output

This section provides detailed information on the expected call flow output for various scenarios with the New Standard QCI support feature:

- New Call Procedure
- Handoff Procedures
- UE Initiated Bearer Creation
- Bearer Creation
- Bearer Update

These sections describe new behaviors and provide behavior clarification for this feature. Behavior not described is similar to that for Standard QCIs.

New Call Procedure

This section provides detailed information on the expected call flow output for various new call procedure scenarios with the New Standard QCI Support feature.

Table 51: Expected Call Flow Output: New Call Procedure

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Setup 3G (GGSN)	N/A	N/A	Create PDP Req	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call rejected by application
Setup eHRPD	N/A	N/A	PBU	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call accepted and created with this rule
Setup 4G (RAT: S4-SGSN)	N/A	N/A	Create Session Req	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call accepted and created with this rule

Handoff Procedures

This section provides detailed information on expected call flow output for various handoff procedure scenarios with the New Standard QCI Support feature.

Table 52: Expected Call Flow Output: Handoff Procedures

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Default bearer existing for WiFi	Call existing with MC/PTT-QCI requested to handoff to MC/PTT-QCI	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT-Std QCI received for default bearer	N/A	Handoff accepted and dowlnadd MC/PTT Std QCI applied	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GnGp Handoff (4G (LTE) to 3G (GGSN))	Update PDP request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI where mapping not received for few MC/PTT-QCI bearers	Update PDP Req	Partial mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	Partial mapped Std QCI for MC/PTT-QCIs received. Here mapping is not Received for some PDP bearers .	N/A	Handoff rejected and call drop Initiated
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI where no mapping received for few MC/PTT-QCI bearers	Update PDP Req	No mapping Received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	No mapping received	N/A	Handoff rejected and call drop initiated
	Update PDP request received for primary PDP and pending response (No-Local Mapping Present)	Call existing with Std primary PDP & MC/PTT-QCI requested to Std-QCI	Update PDP Req	N/A	Enabled	N/A	MC/PTT update rules received for Std QCI dedicated bearers	N/A	MC/PTT QCI mapped rule associated dedicated bearer purged and handoff accepted
		Call existing with MC/PTT primary PDP	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response (No-local mapping present)								Handoff rejected and call drop Initiated (dropped before Initiating CCA-U for handoff)
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	PCRF Timeout No Response received	Enabled	N/A	No response from PCRF / CCA-U timeout	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and same as what QCI values comes in UPC during HO)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
			Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and not same as what QCI values comes in UPC during HO).	Call existing with MC/PTT-QCI requested to Std-QCI							
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and same as what QCI values come in UPC during HO)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
		Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and not same as what QCI values come in UPC during HO.)								
	Update PDP Request received for primary PDP and pending response (Local mapping present/not present)	Call existing with MC/PTT-QCI requested to Std-QCI. Also suppress-NRUPC UPC is configured at the GGSN service level.	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and response sent (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers	Update PDP Req	Complete mapping Received from PCRF for MC/PTT- QCI to Std-QCI (as per Local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT-QCI	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and response sent (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers	Update PDP Req	Complete mapping received from PCRF for MC/PTT- QCI to Std-QCI (different from local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT-QCI	N/A	Handoff accepted and Update PDP Response sent for all bearers
eHRPD -> LTE	Create Session Req received with ho_ind = 1	Only one bearer existing with the call	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT-Std QCI received with rules	N/A	Handoff accepted and dedicated bearer are created with the MC/PTT-Std QCI received.
LTE -> eHRPD	Default + dedicated bearer existing for LTE	Call existing with MC/PTT-QCI	PBU	N/A	Enabled	N/A	N/A	N/A	Handoff accepted and PBA is sent and dedicated bearer rules are added under single bearer

UE Initiated Bearer Creation

This section provides detailed information on the expected call flow output for various UE initiated bearer creation scenarios with the New Standard QCI Support feature.

Table 53: Expected Call Flow Output: UE Initiated Bearer Creation

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
LTE UE Initiated Bearer	Default bearer existing for LTE	N/A	Bearer Resource Command	MC/PTT- Std QCI	N/A	N/A	N/A	N/A	BRC rejected by application
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Disabled	N/A	MC/PTT-Std dedicated QCI	N/A	BRC rejected / rule rejected with resource allocation failure
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Enabled	N/A	MC/PTT-Std dedicated QCI	N/A	BRC rejected /CBReq initiated with MC/PTT- Std QCI

Bearer Creation

This section provides detailed information on the expected call flow output for Bearer Creation scenarios with the New Standard QCI Support feature.

Table 54: Expected Call Flow Output: Bearer Creation

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN secondary PDP creation	Primary PDP existing for GGSN	New secondary PDP requested with MC/PTT-Std-QCI	RAR Procedure	N/A	Enabled	N/A	N/A	Rules received with MC/PTT-Std QCI	CCR-I resource allocation failure for secondary PDP sent to PCRF

Bearer Update

This section provides detailed information on the expected call flow output for Bearer Update scenarios with the New Standard QCI Support feature.

Table 55: Expected Call Flow Output: Bearer Update

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN Primary PDP QoS modification	Primary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT-Std QCI modification	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MC/PTT-Std QCI for primary PDP received	CCR-I QoS modification failure for primary PDP QoS modification rejected
GGSN Secondary PDP Qos Modification	Primary PDP & secondary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT-Std QCI modification for secondary PDP	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MC/PTT-Std QCI for secondary PDP with rules received	CCR-I resource allocation failure for secondary PDP QoS modification sent

Configuring New Standard QCIs

Configuring New Standard QCIs consists of the following tasks:

- Configuring QCI-QoS Mapping
- Configuring Local Mapping for Gn/Gp Support
- Configuring Transaction Rate Network Initiated Setup/Teardown Events
- Enable Mission Critical QCIs

Configuring QCI-QoS Mapping

Standard QCI options **65**, **66**, **69**, and **70** have been added to the **qci** command in *QCI-QoS Mapping Configuration Mode*.

To configure QCI-QoS Mapping for new standard QCIs:

```
configure
  qci-qos-mapping qci_qos_map_name
    qci { 1-9 | 65 | 66 | 69 | 70 }
    end
```

To disable new QCI-QoS mapping for new standard QCIs:

```
configure
  qci-qos-mapping qci_qos_map_name
```

```
no qci { 1-9 | 65 | 66 | 69 | 70 }
end
```

Notes:

- **qci** options 65 and 66 are available for guaranteed bit rate (GBR) network initiated QCI values only.

  qci options 69 and 70 are available for non-GBR network initiated QCI values only.

- **no** disables the specified standard **qci** value.

Configuring Local QCI Mapping for Gn/Gp QoS Support

Use the following example to configure local QCI mapping for Gn/Gp support:

```
configure
  qci-qos-mapping mapping_name
    qci  { 1-9 | 65 | 66 | 69 | 70 } pre-rel8-qos-mapping qci_value
    end
```

Notes:

- **qci**: When the MPS license is disabled, this value must be a Standard QoS Class Identifier (QCI) from 1 to 9. When the MPS license is enabled, this value must be a Standard QCI from 1 to 9, or 65, 66, 69, 70.
- **qci** 65 and 66 are Mission Critical/Push to Talk (MC/PTT) GBR values and values 69 and 70 are MC/PTT Non-GBR values.
- **qci** values 65 and 66 can only be mapped to QCI values 1 through 4, and QCI values 69 and 70 can only be mapped to QCI values 5 through 9.

Configuring Transaction Rate Network Initiated Setup/Teardown Events

To configure transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
  transaction-rate nw-initiated-setup-teardown-events qci { 1-9 | 65 |
66 | 69 | 70 | 128-254 }
  end
```

To disable transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
  no transaction-rate nw-initiated-setup-teardown-events qci qci_value
  end
```

Notes:

- **65** and **66** are available options for GBR network-initiated QCI values.
- **69** and **70** are available options for non-GBR network-initiated QCI values.
- **no** disables transaction rate network initiated setup/teardown events for the specified new standard QCI value.

Enable Mission Critical QCIs

The **mission-critical-qcis** keyword in the **diameter encode-supported-features** command is required for support between the PCEF and PCRF for new standard QCI support. Use the following example to enable mission critical QCIs in *Policy Control Configuration Mode*:

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

To disable this feature, enter the following commands:

```
configure
  context context_name
    ims-auth-service ims-ggsn-auth
      policy-control
        no diameter encode-supported-features
        end
```

Notes:



Important The LTE Wireless Priority Feature Set must be enabled to configure the **mission-critical-qcis** option. The LTE Wireless Priority Feature Set is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

Verifying the Configuration

Use the following example to verify the new standard QCI configuration:

```
show qci-qos-mapping table name qci_qos_mapping_table_name
```

Notes:

- The command output provides all qci-qos mapping attributes, including the new standard qci number. If any of the attributes are incorrect, repeat the configuration procedure in this chapter to correct the settings.

Monitoring the Feature

This section describes how to monitor the New Standard QCI Support feature.

Bulk Statistics

This section lists the bulk statistics that have been added to support the New Standard QCIs feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
```

```
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

GTPU Schema

The following bulk statistics have been added to the GTPU Schema to support the New Standard QCIs feature.

```
qci65-uplink-pkts
qci65-uplink-bytes
qci65-dwlink-pkts
qci65-dwlink-byte
qci65-pkts-discard
qci65-bytes-discard
qci66-uplink-pkts
qci66-uplink-bytes
qci66-dwlink-pkts
qci66-dwlink-byte
qci66-pkts-discard
qci66-bytes-discard
qci69-uplink-pkts
qci69-uplink-bytes
qci69-dwlink-pkts
qci69-dwlink-byte
qci69-pkts-discard
qci69-bytes-discard
qci70-uplink-pkts
qci70-uplink-bytes
qci70-dwlink-pkts
qci70-dwlink-byte
qci70-pkts-discard
qci70-bytes-discard
```

P-GW Schema

The following bulk statistics have been added to the P-GW schema to support the New Standard QCIs feature.

```
subqosstat-bearact-qci65
subqosstat-bearact-qci66
subqosstat-bearact-qci69
subqosstat-bearact-qci70
subqosstat-bearsetup-qci65
subqosstat-bearsetup-qci66
subqosstat-bearsetup-qci69
subqosstat-bearsetup-qci70
subqosstat-bearrel-qci65
subqosstat-bearrel-qci66
subqosstat-bearrel-qci69
subqosstat-bearrel-qci70
subdatastat-uppktfwd-qci65
subdatastat-uppktfwd-qci66
subdatastat-uppktfwd-qci69
subdatastat-uppktfwd-qci70
subdatastat-upbytefwd-qci65
subdatastat-upbytefwd-qci66
subdatastat-upbytefwd-qci69
subdatastat-upbytefwd-qci70
subdatastat-downpktfwd-qci65
subdatastat-downpktfwd-qci66
subdatastat-downpktfwd-qci69
subdatastat-downpktfwd-qci70
subdatastat-downbytefwd-qci65
subdatastat-downbytefwd-qci66
```

```
subdatastat-downbytefwd-qci69
subdatastat-downbytefwd-qci70
subdatastat-uppktdrop-qci65
subdatastat-uppktdrop-qci66
subdatastat-uppktdrop-qci69
subdatastat-uppktdrop-qci70
subdatastat-upbytedrop-qci65
subdatastat-upbytedrop-qci66
subdatastat-upbytedrop-qci69
subdatastat-upbytedrop-qci70
subdatastat-downpktdrop-qci65
subdatastat-downpktdrop-qci66
subdatastat-downpktdrop-qci69
subdatastat-downpktdrop-qci70
subdatastat-downbytedrop-qci65
subdatastat-downbytedrop-qci66
subdatastat-downbytedrop-qci69
subdatastat-downbytedrop-qci70
subdatastat-uppktdropmbrexc-qci65
subdatastat-uppktdropmbrexc-qci66
subdatastat-uppktdropmbrexc-qci69
subdatastat-uppktdropmbrexc-qci70
subdatastat-upbytedropmbrexc-qci65
subdatastat-upbytedropmbrexc-qci66
subdatastat-upbytedropmbrexc-qci69
subdatastat-upbytedropmbrexc-qci70
subdatastat-downpktdropmbrexc-qci65
subdatastat-downpktdropmbrexc-qci66
subdatastat-downpktdropmbrexc-qci69
subdatastat-downpktdropmbrexc-qci70
subdatastat-downbytedropmbrexc-qci65
subdatastat-downbytedropmbrexc-qci66
subdatastat-downbytedropmbrexc-qci69
subdatastat-downbytedropmbrexc-qci70
```

SAEGW Schema

The following bulk statistics have been added to the SAEGW Schema to support the New Standard QCIs feature.

```
sgw-totepsbearact-qci65
sgw-totepsbearact-qci66
sgw-totepsbearact-qci69
sgw-totepsbearact-qci70
sgw-totepsbearset-qci65
sgw-totepsbearset-qci66
sgw-totepsbearset-qci69
sgw-totepsbearset-qci70
sgw-totepsbearrel-qci65
sgw-totepsbearrel-qci66
sgw-totepsbearrel-qci69
sgw-totepsbearrel-qci70
sgw-totepsbearmod-qci65
sgw-totepsbearmod-qci66
sgw-totepsbearmod-qci69
sgw-totepsbearmod-qci70
sgw-totepsbearrel-dedrsn-pgw-qci65
sgw-totepsbearrel-dedrsn-pgw-qci66
sgw-totepsbearrel-dedrsn-pgw-qci69
sgw-totepsbearrel-dedrsn-pgw-qci70
sgw-totepsbearrel-dedrsn-s1err-qci65
sgw-totepsbearrel-dedrsn-s1err-qci66
sgw-totepsbearrel-dedrsn-s1err-qci69
sgw-totepsbearrel-dedrsn-s1err-qci70
```

```
sgw-totepsbearrel-dedrsn-s5err-qci65
sgw-totepsbearrel-dedrsn-s5err-qci66
sgw-totepsbearrel-dedrsn-s5err-qci69
sgw-totepsbearrel-dedrsn-s5err-qci70
sgw-totepsbearrel-dedrsn-s4err-qci65
sgw-totepsbearrel-dedrsn-s4err-qci66
sgw-totepsbearrel-dedrsn-s4err-qci69
sgw-totepsbearrel-dedrsn-s4err-qci70
sgw-totepsbearrel-dedrsn-s12err-qci65
sgw-totepsbearrel-dedrsn-s12err-qci66
sgw-totepsbearrel-dedrsn-s12err-qci69
sgw-totepsbearrel-dedrsn-s12err-qci70
sgw-totepsbearrel-dedrsn-local-qci65
sgw-totepsbearrel-dedrsn-local-qci66
sgw-totepsbearrel-dedrsn-local-qci69
sgw-totepsbearrel-dedrsn-local-qci70
sgw-totepsbearrel-dedrsn-pdn-qci65
sgw-totepsbearrel-dedrsn-pdn-qci66
sgw-totepsbearrel-dedrsn-pdn-qci69
sgw-totepsbearrel-dedrsn-pdn-qci70
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-qci70
sgw-totepsbearrel-dedrsn-pathfail-s11-qci65
sgw-totepsbearrel-dedrsn-pathfail-s11-qci66
sgw-totepsbearrel-dedrsn-pathfail-s11-qci69
sgw-totepsbearrel-dedrsn-pathfail-s11-qci70
sgw-totepsbearrel-dedrsn-pathfail-s12-qci65
sgw-totepsbearrel-dedrsn-pathfail-s12-qci66
sgw-totepsbearrel-dedrsn-pathfail-s12-qci69
sgw-totepsbearrel-dedrsn-pathfail-s12-qci70
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci70
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci65
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci66
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci69
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci70
sgw-totepsbearrel-dedrsn-other-qci65
sgw-totepsbearrel-dedrsn-other-qci66
sgw-totepsbearrel-dedrsn-other-qci69
sgw-totepsbearrel-dedrsn-other-qci70
sgw-datastat-ul-qci65totbyte
sgw-datastat-ul-qci65totpkt
sgw-datastat-ul-qci66totbyte
sgw-datastat-ul-qci66totpkt
sgw-datastat-ul-qci69totbyte
sgw-datastat-ul-qci69totpkt
sgw-datastat-ul-qci70totbyte
sgw-datastat-ul-qci70totpkt
sgw-datastat-ul-dropstat-qci65totbyte
sgw-datastat-ul-dropstat-qci65totpkt
sgw-datastat-ul-dropstat-qci66totbyte
sgw-datastat-ul-dropstat-qci66totpkt
```

```
sgw-datastat-ul-dropstat-qci69totbyte
sgw-datastat-ul-dropstat-qci69totpkt
sgw-datastat-ul-dropstat-qci70totbyte
sgw-datastat-ul-dropstat-qci70totpkt
sgw-datastat-dl-qci65totbyte
sgw-datastat-dl-qci65totpkt
sgw-datastat-dl-qci66totbyte
sgw-datastat-dl-qci66totpkt
sgw-datastat-dl-qci69totbyte
sgw-datastat-dl-qci69totpkt
sgw-datastat-dl-qci70totbyte
sgw-datastat-dl-qci70totpkt
sgw-datastat-dl-dropstat-qci65totbyte
sgw-datastat-dl-dropstat-qci65totpkt
sgw-datastat-dl-dropstat-qci66totbyte
sgw-datastat-dl-dropstat-qci66totpkt
sgw-datastat-dl-dropstat-qci69totbyte
sgw-datastat-dl-dropstat-qci69totpkt
sgw-datastat-dl-dropstat-qci70totbyte
sgw-datastat-dl-dropstat-qci70totpkt
sgw-s1u-ul-qci65totbyte
sgw-s1u-ul-qci65totpkt
sgw-s1u-ul-qci66totbyte
sgw-s1u-ul-qci66totpkt
sgw-s1u-ul-qci69totbyte
sgw-s1u-ul-qci69totpkt
sgw-s1u-ul-qci70totbyte
sgw-s1u-ul-qci70totpkt
sgw-s1u-ul-drop-qci65totbyte
sgw-s1u-ul-drop-qci65totpkt
sgw-s1u-ul-drop-qci66totbyte
sgw-s1u-ul-drop-qci66totpkt
sgw-s1u-ul-drop-qci69totbyte
sgw-s1u-ul-drop-qci69totpkt
sgw-s1u-ul-drop-qci70totbyte
sgw-s1u-ul-drop-qci70totpkt
sgw-s1u-dl-qci65totbyte
sgw-s1u-dl-qci65totpkt
sgw-s1u-dl-qci66totbyte
sgw-s1u-dl-qci66totpkt
sgw-s1u-dl-qci69totbyte
sgw-s1u-dl-qci69totpkt
sgw-s1u-dl-qci70totbyte
sgw-s1u-dl-qci70totpkt
sgw-s1u-dl-drop-qci65totbyte
sgw-s1u-dl-drop-qci65totpkt
sgw-s1u-dl-drop-qci66totbyte
sgw-s1u-dl-drop-qci66totpkt
sgw-s1u-dl-drop-qci69totbyte
sgw-s1u-dl-drop-qci69totpkt
sgw-s1u-dl-drop-qci70totbyte
sgw-s1u-dl-drop-qci70totpkt
sgw-s4u-ul-qci65totbyte
sgw-s4u-ul-qci65totpkt
sgw-s4u-ul-qci66totbyte
sgw-s4u-ul-qci66totpkt
sgw-s4u-ul-qci69totbyte
sgw-s4u-ul-qci69totpkt
sgw-s4u-ul-qci70totbyte
sgw-s4u-ul-qci70totpkt
sgw-s4u-ul-drop-qci65totbyte
sgw-s4u-ul-drop-qci65totpkt
sgw-s4u-ul-drop-qci66totbyte
sgw-s4u-ul-drop-qci66totpkt
```

```
sgw-s4u-ul-drop-qci69totbyte
sgw-s4u-ul-drop-qci69totpkt
sgw-s4u-ul-drop-qci70totbyte
sgw-s4u-ul-drop-qci70totpkt
sgw-s4u-dl-qci65totbyte
sgw-s4u-dl-qci65totpkt
sgw-s4u-dl-qci66totbyte
sgw-s4u-dl-qci66totpkt
sgw-s4u-dl-qci69totbyte
sgw-s4u-dl-qci69totpkt
sgw-s4u-dl-qci70totbyte
sgw-s4u-dl-qci70totpkt
sgw-s4u-dl-drop-qci65totbyte
sgw-s4u-dl-drop-qci65totpkt
sgw-s4u-dl-drop-qci66totbyte
sgw-s4u-dl-drop-qci66totpkt
sgw-s4u-dl-drop-qci69totbyte
sgw-s4u-dl-drop-qci69totpkt
sgw-s4u-dl-drop-qci70totbyte
sgw-s4u-dl-drop-qci70totpkt
sgw-s12-ul-qci65totbyte
sgw-s12-ul-qci65totpkt
sgw-s12-ul-qci66totbyte
sgw-s12-ul-qci66totpkt
sgw-s12-ul-qci69totbyte
sgw-s12-ul-qci69totpkt
sgw-s12-ul-qci70totbyte
sgw-s12-ul-qci70totpkt
sgw-s12-ul-drop-qci65totbyte
sgw-s12-ul-drop-qci65totpkt
sgw-s12-ul-drop-qci66totbyte
sgw-s12-ul-drop-qci66totpkt
sgw-s12-ul-drop-qci69totbyte
sgw-s12-ul-drop-qci69totpkt
sgw-s12-ul-drop-qci70totbyte
sgw-s12-ul-drop-qci70totpkt
sgw-s12-dl-qci65totbyte
sgw-s12-dl-qci65totpkt
sgw-s12-dl-qci66totbyte
sgw-s12-dl-qci66totpkt
sgw-s12-dl-qci69totbyte
sgw-s12-dl-qci69totpkt
sgw-s12-dl-qci70totbyte
sgw-s12-dl-qci70totpkt
sgw-s12-dl-drop-qci65totbyte
sgw-s12-dl-drop-qci65totpkt
sgw-s12-dl-drop-qci66totbyte
sgw-s12-dl-drop-qci66totpkt
sgw-s12-dl-drop-qci69totbyte
sgw-s12-dl-drop-qci69totpkt
sgw-s12-dl-drop-qci70totbyte
sgw-s12-dl-drop-qci70totpkt
sgw-s5-ul-qci65totbyte
sgw-s5-ul-qci65totpkt
sgw-s5-ul-qci66totbyte
sgw-s5-ul-qci66totpkt
sgw-s5-ul-qci69totbyte
sgw-s5-ul-qci69totpkt
sgw-s5-ul-qci70totbyte
sgw-s5-ul-qci70totpkt
sgw-s5-ul-drop-qci65totbyte
sgw-s5-ul-drop-qci65totpkt
sgw-s5-ul-drop-qci66totbyte
sgw-s5-ul-drop-qci66totpkt
```

```
sgw-s5-ul-drop-qci69totbyte
sgw-s5-ul-drop-qci69totpkt
sgw-s5-ul-drop-qci70totbyte
sgw-s5-ul-drop-qci70totpkt
sgw-s5-dl-qci65totbyte
sgw-s5-dl-qci65totpkt
sgw-s5-dl-qci66totbyte
sgw-s5-dl-qci66totpkt
sgw-s5-dl-qci69totbyte
sgw-s5-dl-qci69totpkt
sgw-s5-dl-qci70totbyte
sgw-s5-dl-qci70totpkt
sgw-s5-dl-drop-qci65totbyte
sgw-s5-dl-drop-qci65totpkt
sgw-s5-dl-drop-qci66totbyte
sgw-s5-dl-drop-qci66totpkt
sgw-s5-dl-drop-qci69totbyte
sgw-s5-dl-drop-qci69totpkt
sgw-s5-dl-drop-qci70totbyte
sgw-s5-dl-drop-qci70totpkt
sgw-s8-ul-qci65totbyte
sgw-s8-ul-qci65totpkt
sgw-s8-ul-qci66totbyte
sgw-s8-ul-qci66totpkt
sgw-s8-ul-qci69totbyte
sgw-s8-ul-qci69totpkt
sgw-s8-ul-qci70totbyte
sgw-s8-ul-qci70totpkt
sgw-s8-ul-drop-qci65totbyte
sgw-s8-ul-drop-qci65totpkt
sgw-s8-ul-drop-qci66totbyte
sgw-s8-ul-drop-qci66totpkt
sgw-s8-ul-drop-qci69totbyte
sgw-s8-ul-drop-qci69totpkt
sgw-s8-ul-drop-qci70totbyte
sgw-s8-ul-drop-qci70totpkt
sgw-s8-dl-qci65totbyte
sgw-s8-dl-qci65totpkt
sgw-s8-dl-qci66totbyte
sgw-s8-dl-qci66totpkt
sgw-s8-dl-qci69totbyte
sgw-s8-dl-qci69totpkt
sgw-s8-dl-qci70totbyte
sgw-s8-dl-qci70totpkt
sgw-s8-dl-drop-qci65totbyte
sgw-s8-dl-drop-qci65totpkt
sgw-s8-dl-drop-qci66totbyte
sgw-s8-dl-drop-qci66totpkt
sgw-s8-dl-drop-qci69totbyte
sgw-s8-dl-drop-qci69totpkt
sgw-s8-dl-drop-qci70totbyte
sgw-s8-dl-drop-qci70totpkt
sgw-s5s8-ul-qci65totbyte
sgw-s5s8-ul-qci65totpkt
sgw-s5s8-ul-qci66totbyte
sgw-s5s8-ul-qci66totpkt
sgw-s5s8-ul-qci69totbyte
sgw-s5s8-ul-qci69totpkt
sgw-s5s8-ul-qci70totbyte
sgw-s5s8-ul-qci70totpkt
sgw-s5s8-ul-drop-qci65totbyte
sgw-s5s8-ul-drop-qci65totpkt
sgw-s5s8-ul-drop-qci66totbyte
sgw-s5s8-ul-drop-qci66totpkt
```

```
sgw-s5s8-ul-drop-qci69totbyte
sgw-s5s8-ul-drop-qci69totpkt
sgw-s5s8-ul-drop-qci70totbyte
sgw-s5s8-ul-drop-qci70totpkt
sgw-s5s8-dl-qci65totbyte
sgw-s5s8-dl-qci65totpkt
sgw-s5s8-dl-qci66totbyte
sgw-s5s8-dl-qci66totpkt
sgw-s5s8-dl-qci69totbyte
sgw-s5s8-dl-qci69totpkt
sgw-s5s8-dl-qci70totbyte
sgw-s5s8-dl-qci70totpkt
sgw-s5s8-dl-drop-qci65totbyte
sgw-s5s8-dl-drop-qci65totpkt
sgw-s5s8-dl-drop-qci66totbyte
sgw-s5s8-dl-drop-qci66totpkt
sgw-s5s8-dl-drop-qci69totbyte
sgw-s5s8-dl-drop-qci69totpkt
sgw-s5s8-dl-drop-qci70totbyte
sgw-s5s8-dl-drop-qci70totpkt
pgw-subqosstat-bearact-qci65
pgw-subqosstat-bearact-qci66
pgw-subqosstat-bearact-qci69
pgw-subqosstat-bearact-qci70
pgw-subqosstat-bearset-qci65
pgw-subqosstat-bearset-qci66
pgw-subqosstat-bearset-qci69
pgw-subqosstat-bearset-qci70
pgw-subqosstat-bearrel-qci65
pgw-subqosstat-bearrel-qci66
pgw-subqosstat-bearrel-qci69
pgw-subqosstat-bearrel-qci70
pgw-subdatastat-ulpktfwd-qci65
pgw-subdatastat-ulpktfwd-qci66
pgw-subdatastat-ulpktfwd-qci69
pgw-subdatastat-ulpktfwd-qci70
pgw-subdatastat-ulbytefwd-qci65
pgw-subdatastat-ulbytefwd-qci66
pgw-subdatastat-ulbytefwd-qci69
pgw-subdatastat-ulbytefwd-qci70
pgw-subdatastat-dlpktfwd-qci65
pgw-subdatastat-dlpktfwd-qci66
pgw-subdatastat-dlpktfwd-qci69
pgw-subdatastat-dlpktfwd-qci70
pgw-subdatastat-dlbytefwd-qci65
pgw-subdatastat-dlbytefwd-qci66
pgw-subdatastat-dlbytefwd-qci69
pgw-subdatastat-dlbytefwd-qci70
pgw-subdatastat-ulpktdrop-qci65
pgw-subdatastat-ulpktdrop-qci66
pgw-subdatastat-ulpktdrop-qci69
pgw-subdatastat-ulpktdrop-qci70
pgw-subdatastat-ulbytedrop-qci65
pgw-subdatastat-ulbytedrop-qci66
pgw-subdatastat-ulbytedrop-qci69
pgw-subdatastat-ulbytedrop-qci70
pgw-subdatastat-dlpktdrop-qci65
pgw-subdatastat-dlpktdrop-qci66
pgw-subdatastat-dlpktdrop-qci69
pgw-subdatastat-dlpktdrop-qci70
pgw-subdatastat-dlbytedrop-qci65
pgw-subdatastat-dlbytedrop-qci66
pgw-subdatastat-dlbytedrop-qci69
pgw-subdatastat-dlbytedrop-qci70
```

```
pgw-subdatastat-ulpktdropmbrexc-qci65
pgw-subdatastat-ulpktdropmbrexc-qci66
pgw-subdatastat-ulpktdropmbrexc-qci69
pgw-subdatastat-ulpktdropmbrexc-qci70
pgw-subdatastat-ulbytedropmbrexc-qci65
pgw-subdatastat-ulbytedropmbrexc-qci66
pgw-subdatastat-ulbytedropmbrexc-qci69
pgw-subdatastat-ulbytedropmbrexc-qci70
pgw-subdatastat-dlpktdropmbrexc-qci65
pgw-subdatastat-dlpktdropmbrexc-qci66
pgw-subdatastat-dlpktdropmbrexc-qci69
pgw-subdatastat-dlpktdropmbrexc-qci70
pgw-subdatastat-dlbytedropmbrexc-qci65
pgw-subdatastat-dlbytedropmbrexc-qci66
pgw-subdatastat-dlbytedropmbrexc-qci69
pgw-subdatastat-dlbytedropmbrexc-qci70
collapsed-subdatastat-ulpktfwd-qci65
collapsed-subdatastat-ulpktfwd-qci66
collapsed-subdatastat-ulpktfwd-qci69
collapsed-subdatastat-ulpktfwd-qci70
collapsed-subdatastat-ulbytefwd-qci65
collapsed-subdatastat-ulbytefwd-qci66
collapsed-subdatastat-ulbytefwd-qci69
collapsed-subdatastat-ulbytefwd-qci70
collapsed-subdatastat-dlpktfwd-qci65
collapsed-subdatastat-dlpktfwd-qci66
collapsed-subdatastat-dlpktfwd-qci69
collapsed-subdatastat-dlpktfwd-qci70
collapsed-subdatastat-dlbytefwd-qci65
collapsed-subdatastat-dlbytefwd-qci66
collapsed-subdatastat-dlbytefwd-qci69
collapsed-subdatastat-dlbytefwd-qci70
collapsed-subdatastat-ulpktdrop-qci65
collapsed-subdatastat-ulpktdrop-qci66
collapsed-subdatastat-ulpktdrop-qci69
collapsed-subdatastat-ulpktdrop-qci70
collapsed-subdatastat-ulbytedrop-qci65
collapsed-subdatastat-ulbytedrop-qci66
collapsed-subdatastat-ulbytedrop-qci69
collapsed-subdatastat-ulbytedrop-qci70
collapsed-subdatastat-dlpktdrop-qci65
collapsed-subdatastat-dlpktdrop-qci66
collapsed-subdatastat-dlpktdrop-qci69
collapsed-subdatastat-dlpktdrop-qci70
collapsed-subdatastat-dlbytedrop-qci65
collapsed-subdatastat-dlbytedrop-qci66
collapsed-subdatastat-dlbytedrop-qci69
collapsed-subdatastat-dlbytedrop-qci70
collapsed-subqosstat-bearact-qci65
collapsed-subqosstat-bearact-qci66
collapsed-subqosstat-bearact-qci69
collapsed-subqosstat-bearact-qci70
collapsed-subqosstat-bearset-qci65
collapsed-subqosstat-bearset-qci66
collapsed-subqosstat-bearset-qci69
collapsed-subqosstat-bearset-qci70
collapsed-subqosstat-bearrel-qci65
collapsed-subqosstat-bearrel-qci66
collapsed-subqosstat-bearrel-qci69
collapsed-subqosstat-bearrel-qci70
saegw-ggsn-subqosstat-bearact-qci65
saegw-ggsn-subqosstat-bearact-qci66
saegw-ggsn-subqosstat-bearact-qci69
saegw-ggsn-subqosstat-bearact-qci70
```

```
saegw-ggsn-subqosstat-bearset-qci65
saegw-ggsn-subqosstat-bearset-qci66
saegw-ggsn-subqosstat-bearset-qci69
saegw-ggsn-subqosstat-bearset-qci70
saegw-ggsn-subqosstat-bearrel-qci65
saegw-ggsn-subqosstat-bearrel-qci66
saegw-ggsn-subqosstat-bearrel-qci69
saegw-ggsn-subqosstat-bearrel-qci70
saegw-ggsn-subdatastat-ulpktfwd-qci65
saegw-ggsn-subdatastat-ulpktfwd-qci66
saegw-ggsn-subdatastat-ulpktfwd-qci69
saegw-ggsn-subdatastat-ulpktfwd-qci70
saegw-ggsn-subdatastat-ulbytefwd-qci65
saegw-ggsn-subdatastat-ulbytefwd-qci66
saegw-ggsn-subdatastat-ulbytefwd-qci69
saegw-ggsn-subdatastat-ulbytefwd-qci70
saegw-ggsn-subdatastat-dlpktfwd-qci65
saegw-ggsn-subdatastat-dlpktfwd-qci66
saegw-ggsn-subdatastat-dlpktfwd-qci69
saegw-ggsn-subdatastat-dlpktfwd-qci70
saegw-ggsn-subdatastat-dlbytefwd-qci65
saegw-ggsn-subdatastat-dlbytefwd-qci66
saegw-ggsn-subdatastat-dlbytefwd-qci69
saegw-ggsn-subdatastat-dlbytefwd-qci70
saegw-ggsn-subdatastat-ulpktdrop-qci65
saegw-ggsn-subdatastat-ulpktdrop-qci66
saegw-ggsn-subdatastat-ulpktdrop-qci69
saegw-ggsn-subdatastat-ulpktdrop-qci70
saegw-ggsn-subdatastat-ulbytedrop-qci65
saegw-ggsn-subdatastat-ulbytedrop-qci66
saegw-ggsn-subdatastat-ulbytedrop-qci69
saegw-ggsn-subdatastat-ulbytedrop-qci70
saegw-ggsn-subdatastat-dlpktdrop-qci65
saegw-ggsn-subdatastat-dlpktdrop-qci66
saegw-ggsn-subdatastat-dlpktdrop-qci69
saegw-ggsn-subdatastat-dlpktdrop-qci70
saegw-ggsn-subdatastat-dlbytedrop-qci65
saegw-ggsn-subdatastat-dlbytedrop-qci66
saegw-ggsn-subdatastat-dlbytedrop-qci69
saegw-ggsn-subdatastat-dlbytedrop-qci70
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci65
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci66
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci69
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci70
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci65
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci66
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci69
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci70
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci65
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci66
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci69
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci70
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci65
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci66
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci69
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci70
```

S-GW Schema

The following bulk statistics have been added to the S-GW schema to support the New Standard QCIs feature.

```
totepsbearactive-qci65
totepsbearactive-qci66
totepsbearactive-qci69
```

```
totepsbearactive-qci70
totepsbearsetup-qci65
totepsbearsetup-qci66
totepsbearsetup-qci69
totepsbearsetup-qci70
totepsbearrel-qci65
totepsbearrel-qci66
totepsbearrel-qci69
totepsbearrel-qci70
totepsbearmod-qci65
totepsbearmod-qci66
totepsbearmod-qci69
totepsbearmod-qci70
totepsbearrel-dedrsn-pgw-qci65
totepsbearrel-dedrsn-pgw-qci66
totepsbearrel-dedrsn-pgw-qci69
totepsbearrel-dedrsn-pgw-qci70
totepsbearrel-dedrsn-s1err-qci65
totepsbearrel-dedrsn-s1err-qci66
totepsbearrel-dedrsn-s1err-qci69
totepsbearrel-dedrsn-s1err-qci70
totepsbearrel-dedrsn-s5err-qci65
totepsbearrel-dedrsn-s5err-qci66
totepsbearrel-dedrsn-s5err-qci69
totepsbearrel-dedrsn-s5err-qci70
totepsbearrel-dedrsn-s4err-qci65
totepsbearrel-dedrsn-s4err-qci66
totepsbearrel-dedrsn-s4err-qci69
totepsbearrel-dedrsn-s4err-qci70
totepsbearrel-dedrsn-s12err-qci65
totepsbearrel-dedrsn-s12err-qci66
totepsbearrel-dedrsn-s12err-qci69
totepsbearrel-dedrsn-s12err-qci70
totepsbearrel-dedrsn-local-qci65
totepsbearrel-dedrsn-local-qci66
totepsbearrel-dedrsn-local-qci69
totepsbearrel-dedrsn-local-qci70
totepsbearrel-dedrsn-pdn-qci65
totepsbearrel-dedrsn-pdn-qci66
totepsbearrel-dedrsn-pdn-qci69
totepsbearrel-dedrsn-pdn-qci70
totepsbearrel-dedrsn-pathfail-s1-u-qci65
totepsbearrel-dedrsn-pathfail-s1-u-qci66
totepsbearrel-dedrsn-pathfail-s1-u-qci69
totepsbearrel-dedrsn-pathfail-s1-u-qci70
totepsbearrel-dedrsn-pathfail-s5-u-qci65
totepsbearrel-dedrsn-pathfail-s5-u-qci66
totepsbearrel-dedrsn-pathfail-s5-u-qci69
totepsbearrel-dedrsn-pathfail-s5-u-qci70
totepsbearrel-dedrsn-pathfail-s5-qci65
totepsbearrel-dedrsn-pathfail-s5-qci66
totepsbearrel-dedrsn-pathfail-s5-qci69
totepsbearrel-dedrsn-pathfail-s5-qci70
totepsbearrel-dedrsn-pathfail-s11-qci65
totepsbearrel-dedrsn-pathfail-s11-qci66
totepsbearrel-dedrsn-pathfail-s11-qci69
totepsbearrel-dedrsn-pathfail-s11-qci70
totepsbearrel-dedrsn-pathfail-s12-qci65
totepsbearrel-dedrsn-pathfail-s12-qci66
totepsbearrel-dedrsn-pathfail-s12-qci69
totepsbearrel-dedrsn-pathfail-s12-qci70
totepsbearrel-dedrsn-pathfail-s4-u-qci65
totepsbearrel-dedrsn-pathfail-s4-u-qci66
totepsbearrel-dedrsn-pathfail-s4-u-qci69
```

```
totepsbearrel-dedrsn-pathfail-s4-u-qci70
totepsbearrel-dedrsn-inactivity-timeout-qci65
totepsbearrel-dedrsn-inactivity-timeout-qci66
totepsbearrel-dedrsn-inactivity-timeout-qci69
totepsbearrel-dedrsn-inactivity-timeout-qci70
totepsbearrel-dedrsn-other-qci65
totepsbearrel-dedrsn-other-qci66
totepsbearrel-dedrsn-other-qci69
totepsbearrel-dedrsn-other-qci70
datastat-uplink-qci65totbyte
datastat-uplink-qci65totpkt
datastat-uplink-qci66totbyte
datastat-uplink-qci66totpkt
datastat-uplink-qci69totbyte
datastat-uplink-qci69totpkt
datastat-uplink-qci70totbyte
datastat-uplink-qci70totpkt
datastat-uplink-dropstat-qci65totbyte
datastat-uplink-dropstat-qci65totpkt
datastat-uplink-dropstat-qci66totbyte
datastat-uplink-dropstat-qci66totpkt
datastat-uplink-dropstat-qci69totbyte
datastat-uplink-dropstat-qci69totpkt
datastat-uplink-dropstat-qci70totbyte
datastat-uplink-dropstat-qci70totpkt
datastat-downlink-qci65totbyte
datastat-downlink-qci65totpkt
datastat-downlink-qci66totbyte
datastat-downlink-qci66totpkt
datastat-downlink-qci69totbyte
datastat-downlink-qci69totpkt
datastat-downlink-qci70totbyte
datastat-downlink-qci70totpkt
datastat-downlink-dropstat-qci65totbyte
datastat-downlink-dropstat-qci65totpkt
datastat-downlink-dropstat-qci66totbyte
datastat-downlink-dropstat-qci66totpkt
datastat-downlink-dropstat-qci69totbyte
datastat-downlink-dropstat-qci69totpkt
datastat-downlink-dropstat-qci70totbyte
datastat-downlink-dropstat-qci70totpkt
s1u-uplnk-qci65totbyte
s1u-uplnk-qci65totpkt
s1u-uplnk-qci66totbyte
s1u-uplnk-qci66totpkt
s1u-uplnk-qci69totbyte
s1u-uplnk-qci69totpkt
s1u-uplnk-qci70totbyte
s1u-uplnk-qci70totpkt
s1u-uplnk-drop-qci65totbyte
s1u-uplnk-drop-qci65totpkt
s1u-uplnk-drop-qci66totbyte
s1u-uplnk-drop-qci66totpkt
s1u-uplnk-drop-qci69totbyte
s1u-uplnk-drop-qci69totpkt
s1u-uplnk-drop-qci70totbyte
s1u-uplnk-drop-qci70totpkt
s1u-downlnk-qci65totbyte
s1u-downlnk-qci65totpkt
s1u-downlnk-qci66totbyte
s1u-downlnk-qci66totpkt
s1u-downlnk-qci69totbyte
s1u-downlnk-qci69totpkt
s1u-downlnk-qci70totbyte
```

```
s1u-downlnk-qci70totpkt
s1u-downlnk-drop-qci65totbyte
s1u-downlnk-drop-qci65totpkt
s1u-downlnk-drop-qci66totbyte
s1u-downlnk-drop-qci66totpkt
s1u-downlnk-drop-qci69totbyte
s1u-downlnk-drop-qci69totpkt
s1u-downlnk-drop-qci70totbyte
s1u-downlnk-drop-qci70totpkt
s4u-uplnk-qci65totbyte
s4u-uplnk-qci65totpkt
s4u-uplnk-qci66totbyte
s4u-uplnk-qci66totpkt
s4u-uplnk-qci69totbyte
s4u-uplnk-qci69totpkt
s4u-uplnk-qci70totbyte
s4u-uplnk-qci70totpkt
s4u-uplnk-drop-qci65totbyte
s4u-uplnk-drop-qci65totpkt
s4u-uplnk-drop-qci66totbyte
s4u-uplnk-drop-qci66totpkt
s4u-uplnk-drop-qci69totbyte
s4u-uplnk-drop-qci69totpkt
s4u-uplnk-drop-qci70totbyte
s4u-uplnk-drop-qci70totpkt
s4u-downlnk-qci65totbyte
s4u-downlnk-qci65totpkt
s4u-downlnk-qci66totbyte
s4u-downlnk-qci66totpkt
s4u-downlnk-qci69totbyte
s4u-downlnk-qci69totpkt
s4u-downlnk-qci70totbyte
s4u-downlnk-qci70totpkt
s4u-downlnk-drop-qci65totbyte
s4u-downlnk-drop-qci65totpkt
s4u-downlnk-drop-qci66totbyte
s4u-downlnk-drop-qci66totpkt
s4u-downlnk-drop-qci69totbyte
s4u-downlnk-drop-qci69totpkt
s4u-downlnk-drop-qci70totbyte
s4u-downlnk-drop-qci70totpkt
s12-uplnk-qci65totbyte
s12-uplnk-qci65totpkt
s12-uplnk-qci66totbyte
s12-uplnk-qci66totpkt
s12-uplnk-qci69totbyte
s12-uplnk-qci69totpkt
s12-uplnk-qci70totbyte
s12-uplnk-qci70totpkt
s12-uplnk-drop-qci65totbyte
s12-uplnk-drop-qci65totpkt
s12-uplnk-drop-qci66totbyte
s12-uplnk-drop-qci66totpkt
s12-uplnk-drop-qci69totbyte
s12-uplnk-drop-qci69totpkt
s12-uplnk-drop-qci70totbyte
s12-uplnk-drop-qci70totpkt
s12-downlnk-qci65totbyte
s12-downlnk-qci65totpkt
s12-downlnk-qci66totbyte
s12-downlnk-qci66totpkt
s12-downlnk-qci69totbyte
s12-downlnk-qci69totpkt
s12-downlnk-qci70totbyte
```

```
s12-downlnk-qci70totpkt
s12-downlnk-drop-qci65totbyte
s12-downlnk-drop-qci65totpkt
s12-downlnk-drop-qci66totbyte
s12-downlnk-drop-qci66totpkt
s12-downlnk-drop-qci69totbyte
s12-downlnk-drop-qci69totpkt
s12-downlnk-drop-qci70totbyte
s12-downlnk-drop-qci70totpkt
s5-uplnk-qci65totbyte
s5-uplnk-qci65totpkt
s5-uplnk-qci66totbyte
s5-uplnk-qci66totpkt
s5-uplnk-qci69totbyte
s5-uplnk-qci69totpkt
s5-uplnk-qci70totbyte
s5-uplnk-qci70totpkt
s5-uplnk-drop-qci65totbyte
s5-uplnk-drop-qci65totpkt
s5-uplnk-drop-qci66totbyte
s5-uplnk-drop-qci66totpkt
s5-uplnk-drop-qci69totbyte
s5-uplnk-drop-qci69totpkt
s5-uplnk-drop-qci70totbyte
s5-uplnk-drop-qci70totpkt
s5-downlnk-qci65totbyte
s5-downlnk-qci65totpkt
s5-downlnk-qci66totbyte
s5-downlnk-qci66totpkt
s5-downlnk-qci69totbyte
s5-downlnk-qci69totpkt
s5-downlnk-qci70totbyte
s5-downlnk-qci70totpkt
s5-downlnk-drop-qci65totbyte
s5-downlnk-drop-qci65totpkt
s5-downlnk-drop-qci66totbyte
s5-downlnk-drop-qci66totpkt
s5-downlnk-drop-qci69totbyte
s5-downlnk-drop-qci69totpkt
s5-downlnk-drop-qci70totbyte
s5-downlnk-drop-qci70totpkt
s8-uplnk-qci65totbyte
s8-uplnk-qci65totpkt
s8-uplnk-qci66totbyte
s8-uplnk-qci66totpkt
s8-uplnk-qci69totbyte
s8-uplnk-qci69totpkt
s8-uplnk-qci70totbyte
s8-uplnk-qci70totpkt
s8-uplnk-drop-qci65totbyte
s8-uplnk-drop-qci65totpkt
s8-uplnk-drop-qci66totbyte
s8-uplnk-drop-qci66totpkt
s8-uplnk-drop-qci69totbyte
s8-uplnk-drop-qci69totpkt
s8-uplnk-drop-qci70totbyte
s8-uplnk-drop-qci70totpkt
s8-downlnk-qci65totbyte
s8-downlnk-qci65totpkt
s8-downlnk-qci66totbyte
s8-downlnk-qci66totpkt
s8-downlnk-qci69totbyte
s8-downlnk-qci69totpkt
s8-downlnk-qci70totbyte
```

```
s8-downlnk-qci70totpkt
s8-downlnk-drop-qci65totbyte
s8-downlnk-drop-qci65totpkt
s8-downlnk-drop-qci66totbyte
s8-downlnk-drop-qci66totpkt
s8-downlnk-drop-qci69totbyte
s8-downlnk-drop-qci69totpkt
s8-downlnk-drop-qci70totbyte
s8-downlnk-drop-qci70totpkt
s5s8-uplnk-qci65totbyte
s5s8-uplnk-qci65totpkt
s5s8-uplnk-qci66totbyte
s5s8-uplnk-qci66totpkt
s5s8-uplnk-qci69totbyte
s5s8-uplnk-qci69totpkt
s5s8-uplnk-qci70totbyte
s5s8-uplnk-qci70totpkt
s5s8-uplnk-drop-qci65totbyte
s5s8-uplnk-drop-qci65totpkt
s5s8-uplnk-drop-qci66totbyte
s5s8-uplnk-drop-qci66totpkt
s5s8-uplnk-drop-qci69totbyte
s5s8-uplnk-drop-qci69totpkt
s5s8-uplnk-drop-qci70totbyte
s5s8-uplnk-drop-qci70totpkt
s5s8-downlnk-qci65totbyte
s5s8-downlnk-qci65totpkt
s5s8-downlnk-qci66totbyte
s5s8-downlnk-qci66totpkt
s5s8-downlnk-qci69totbyte
s5s8-downlnk-qci69totpkt
s5s8-downlnk-qci70totbyte
s5s8-downlnk-qci70totpkt
s5s8-downlnk-drop-qci65totbyte
s5s8-downlnk-drop-qci65totpkt
s5s8-downlnk-drop-qci66totbyte
s5s8-downlnk-drop-qci66totpkt
s5s8-downlnk-drop-qci69totbyte
s5s8-downlnk-drop-qci69totpkt
s5s8-downlnk-drop-qci70totbyte
s5s8-downlnk-drop-qci70totpkt
```

System Schema

The following bulk statistics have been added to the System Schema to support the New Standard QCIs feature.

```
sess-bearerdur-5sec-qci65
sess-bearerdur-10sec-qci65
sess-bearerdur-30sec-qci65
sess-bearerdur-1min-qci65
sess-bearerdur-2min-qci65
sess-bearerdur-5min-qci65
sess-bearerdur-15min-qci65
sess-bearerdur-30min-qci65
sess-bearerdur-1hr-qci65
sess-bearerdur-4hr-qci65
sess-bearerdur-12hr-qci65
sess-bearerdur-24hr-qci65
sess-bearerdur-over24hr-qci65
sess-bearerdur-2day-qci65
sess-bearerdur-4day-qci65
sess-bearerdur-5day-qci65
sess-bearerdur-5sec-qci66
```

```
sess-bearerdur-10sec-qci66
sess-bearerdur-30sec-qci66
sess-bearerdur-1min-qci66
sess-bearerdur-2min-qci66
sess-bearerdur-5min-qci66
sess-bearerdur-15min-qci66
sess-bearerdur-30min-qci66
sess-bearerdur-1hr-qci66
sess-bearerdur-4hr-qci66
sess-bearerdur-12hr-qci66
sess-bearerdur-24hr-qci66
sess-bearerdur-over24hr-qci66
sess-bearerdur-2day-qci66
sess-bearerdur-4day-qci66
sess-bearerdur-5day-qci66
sess-bearerdur-5sec-qci69
sess-bearerdur-10sec-qci69
sess-bearerdur-30sec-qci69
sess-bearerdur-1min-qci69
sess-bearerdur-2min-qci69
sess-bearerdur-5min-qci69
sess-bearerdur-15min-qci69
sess-bearerdur-30min-qci69
sess-bearerdur-1hr-qci69
sess-bearerdur-4hr-qci69
sess-bearerdur-12hr-qci69
sess-bearerdur-24hr-qci69
sess-bearerdur-over24hr-qci69
sess-bearerdur-2day-qci69
sess-bearerdur-4day-qci69
sess-bearerdur-5day-qci69
sess-bearerdur-5sec-qci70
sess-bearerdur-10sec-qci70
sess-bearerdur-30sec-qci70
sess-bearerdur-1min-qci70
sess-bearerdur-2min-qci70
sess-bearerdur-5min-qci70
sess-bearerdur-15min-qci70
sess-bearerdur-30min-qci70
sess-bearerdur-1hr-qci70
sess-bearerdur-4hr-qci70
sess-bearerdur-12hr-qci70
sess-bearerdur-24hr-qci70
sess-bearerdur-over24hr-qci70
sess-bearerdur-2day-qci70
sess-bearerdur-4day-qci70
sess-bearerdur-5day-qci70
```

Show Commands

This section describes the show commands available to monitor the New Standard QCIs feature.

show apn statistics all

The output of this command has been enhanced to show administrative disconnects and bearer statistics for the new standard QCIs 65, 66, 69, and 70. New statistics are highlighted in *italics*.

```
...

4G Bearers Released By Reasons:

                     QCI1   QCI2   QCI3   QCI4   QCI5   QCI6   QCI7   QCI8   QCI9
   Admin disconnect:  0          0          0      0      0      0      0      0
```

```
                     QCI65       QCI66       QCI69       QCI70
   Admin disconnect:         0           0           0           0
...

  QCI 65:
    Bearer Active:                  0   Bearer setup:                           0
    Bearer Released:                0   Bearer Rejected:                        0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:               0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                 0
    Uplink pkts dropped:            0   Downlink pkts dropped:                  0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 66:
    Bearer Active:                  0   Bearer setup:                           0
    Bearer Released:                0   Bearer Rejected:                        0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:               0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                 0
    Uplink pkts dropped:            0   Downlink pkts dropped:                  0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 69:
    Bearer Active:                  0   Bearer setup:                           0
    Bearer Released:                0   Bearer Rejected:                        0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:               0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                 0
    Uplink pkts dropped:            0   Downlink pkts dropped:                  0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 70:
    Bearer Active:                  0   Bearer setup:                           0
    Bearer Released:                0   Bearer Rejected:                        0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:               0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                 0
    Uplink pkts dropped:            0   Downlink pkts dropped:                  0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0
                      0
...
```

show gtpu statistics

The output of this command has been enhanced to provide packet and byte information for QCI values 65, 66, 69, and 70. New statistics are in *italics*.

```
...
    QCI 9:
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0

    QCI 65:
         Uplink Packets:              0  Uplink Bytes:                0
```

```
        Downlink Packets:            0  Downlink Bytes:              0
        Packets Discarded:           0  Bytes Discarded:             0

    QCI 66:
        Uplink Packets:              0  Uplink Bytes:                0
        Downlink Packets:            0  Downlink Bytes:              0
        Packets Discarded:           0  Bytes Discarded:             0


    QCI 69:
        Uplink Packets:              0  Uplink Bytes:                0
        Downlink Packets:            0  Downlink Bytes:              0
        Packets Discarded:           0  Bytes Discarded:             0

    QCI 70:
        Uplink Packets:              0  Uplink Bytes:                0
        Downlink Packets:            0  Downlink Bytes:              0
        Packets Discarded:           0  Bytes Discarded:             0

    Non-Std QCI(Non-GBR):
        Uplink Packets:              0  Uplink Bytes:                0
        Downlink Packets:            0  Downlink Bytes:              0
        Packets Discarded:           0  Bytes Discarded:             0
...
```

show pgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information by QoS characteristics and IPv4v6 PDN Data statistics. New statistics are in *italics*.

```
Bearers By QoS characteristics:
  Active:                                   Setup:
    QCI 1:                             0      QCI 1:                          0
...
    QCI 65:                        0      QCI 65:                        0
    QCI 66:                            0      QCI 66:                         0
    QCI 69:                            0      QCI 69:                         0
    QCI 70:                            0      QCI 70:                         0
...

  Released:
    QCI 1:                             0
...
    QCI 65:                            0
    QCI 66:                            0
    QCI 69:                            0
    QCI 70:                            0
...

  IPv4v6 PDN Data Statistics:
    Uplink :                                Downlink :
...
      Packets:                                Packets:
        QCI 1:                         0        QCI 1:                         0
...
        QCI 65:                    0        QCI 65:                        0
        QCI 66:                        0        QCI 66:                        0
        QCI 69:                        0        QCI 69:                        0
        QCI 70:                        0        QCI 70:                        0
```

show saegw-service statistics all verbose

The output of this command has been enhanced to provide information related to the new standard QCIs. New statistics are in *italics*.

```
...

Bearers By QoS characteristics:
  Active:                                  Setup:
    QCI  1:                          0      QCI  1:                          0
    ...
    QCI  9:                          0      QCI  9:                          0
    QCI 65:                          0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0
  Released:
    QCI  1:                          0
   ...
    QCI  9:                          0
    QCI 65:                          0
    QCI 66:                          0
    QCI 69:                          0
    QCI 70:                          0
    Non-Std QCI:                     0

…
      Std QCI(Non-GBR):              0      Std QCI(Non-GBR):              0
      Std QCI(GBR):                  0      Std QCI(GBR):                  0

    Uplink :                                 Downlink :
      Packets:                                 Packets:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Bytes:                                   Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Dropped Packets:                         Dropped Packets:
        QCI 1:                       0          QCI 1:                       0\
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
```

```
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0
Setup Guard Timer Expired:        0
```

show sgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information. New statistics are highlighted in *italics*.

```
...

Bearers By QoS characteristics:
  Active:                                 Setup:
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                         0     QCI 65:                           0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
...

  Released:                               Modified:
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                         0     QCI 65:                           0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
...

Dedicated Bearers Released By Reason:
  PGW Ini:                          0     PCRF Ini:                         0
    QCI 1:                          0
...
    QCI 65:                         0
    QCI 66:                         0
    QCI 69:                         0
    QCI 70:                         0
    Non-Std QCI:                    0
...
  S1 Error Ind:                     0     S5 Error Ind:                     0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                         0     QCI 65:                           0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
    Non-Std QCI:                    0       Non-Std QCI:                    0

  S4 Error Ind:                     0     S12 Error Ind:                    0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                         0     QCI 65:                           0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
    Non-Std QCI:                    0       Non-Std QCI:                    0

  Local:                            0     PDN Down:                         0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                         0     QCI 65:                           0
    QCI 66:                         0       QCI 66:                         0
```

```
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S1-U:                 0    Path Failure S5-U:                 0
    QCI 1:                           0      QCI 1:                           0
    ...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S5:                   0    Path Failure S11:                  0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S4-U:                 0    Path Failure S12:                  0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Inactivity Timeout:                0    Other:                             0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

 ...
 Data Statistics Per Interface:
  S1-U Total Data Statistics:
    Uplink :                           Downlink :
...
      Packets:                           Packets:
        QCI 1:                       0      QCI 1:                           0
...
        QCI 65:                    0      QCI 65:                          0
        QCI 66:                          0      QCI 66:                          0
        QCI 69:                          0      QCI 69:                          0
        QCI 70:                          0      QCI 70:                          0
        Non-Std QCI:                     0      Non-Std QCI:                     0

      Bytes:                             Bytes:
        QCI 1:                       0      QCI 1:                           0
...
        QCI 65:                    0      QCI 65:                          0
        QCI 66:                          0      QCI 66:                          0
        QCI 69:                          0      QCI 69:                          0
        QCI 70:                          0      QCI 70:                          0
        Non-Std QCI:                     0      Non-Std QCI:                     0

      Dropped Packets:                   Dropped Packets:
```

```
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S4-U Total Data Statistics:
    Uplink :                              Downlink :
      Total Pkts:                     0      Total Pkts:                     0
      Total Bytes:                    0      Total Bytes:                    0
      Dropped Pkts:                   0      Dropped Pkts:                   0
      Dropped Bytes:                  0      Dropped Bytes:                  0

      Packets:                                Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Bytes:                                  Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Packets:                        Dropped Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S12 Total Data Statistics:
    Uplink :                              Downlink :
      Total Pkts:                     0      Total Pkts:                     0
      Total Bytes:                    0      Total Bytes:                    0
```

```
      Dropped Pkts:                     0      Dropped Pkts:                     0
      Dropped Bytes:                    0      Dropped Bytes:                    0

      Packets:                                 Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0

      Bytes:                                   Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0

      Dropped Packets:                         Dropped Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0

    S5-U Total Data Statistics:
      Uplink :                                 Downlink :
      Total Pkts:                     0        Total Pkts:                     0
      Total Bytes:                    0        Total Bytes:                    0
      Dropped Pkts:                   0        Dropped Pkts:                   0
      Dropped Bytes:                  0        Dropped Bytes:                  0

      Packets:                                 Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0

      Bytes:                                   Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                   0            QCI 65:                   0
        QCI 66:                         0          QCI 66:                         0
        QCI 69:                         0          QCI 69:                         0
        QCI 70:                         0          QCI 70:                         0
        Non-Std QCI:                    0          Non-Std QCI:                    0
```

```
      Dropped Packets:                          Dropped Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0

      Dropped Bytes:                            Dropped Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0

  S8-U Total Data Statistics:
    Uplink :                                  Downlink :
      Total Pkts:                     0       Total Pkts:                     0
      Total Bytes:                    0       Total Bytes:                    0
      Dropped Pkts:                   0       Dropped Pkts:                   0
      Dropped Bytes:                  0       Dropped Bytes:                  0

      Packets:                                  Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0

      Bytes:                                    Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0

      Dropped Packets:                          Dropped Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0

      Dropped Bytes:                            Dropped Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                     0         QCI 65:                         0
        QCI 66:                         0         QCI 66:                         0
        QCI 69:                         0         QCI 69:                         0
        QCI 70:                         0         QCI 70:                         0
        Non-Std QCI:                    0         Non-Std QCI:                    0
```

Non-standard QCI Support

This section describes the Non-standard QCI Support feature.

Feature Description

Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. A license, however, allows non-standard QCIs (128-254) to be used on P-GW/GGSN (not standalone GGSN).

Licensing

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128-254. QCI values 0 and 10 to 255 are defined as follows:

- 0: Reserved
- 10-127: Reserved
- 128-254: Operator-specific/Non-standard QCI
- 255: Reserved

Unique operator-specific QCIs (128-254) can be used to differentiate between various services/applications carriers provide to the end users in their network.

Limitations

- Non-standard QCIs can only be supported with S5/S8/S2a/S2b interfaces.
- The Gn interface is not supported.

Standards Compliance

- 3GPP Specification TS 23.203: Policy and charging control architecture
- 3GPP Specification TS 29.212: Policy and Charging Control over Gx reference point

Configuring Non-standard QCI Support

The **operator-defined-qci** command in the QCI-QoS Mapping Configuration Mode configures the non-standard QCIs in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF. Unique DSCP parameters (uplink and downlink) and GBR or Non-GBR can also be configured.

As non-standard QCIs are not supported in GGSN, **pre-rel8-qos-mapping** is used as a reference for mapping the non-standard QCI values to pre-rel8 QoS values during 3G calls or GnGp handovers.

Configuring Non-standard QCI Support in P-GW

Use the following command to configure non-standard QCI support in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF.

```
configure
    qci-qos-mapping name
         operator-defined-qci num { gbr | non-gbr } [ { downlink |
uplink } [ encaps-header { copy-inner | copy-outer | dscp-marking
dscp-marking-value } [ internal-qos priority priority ] | internal-qos priority
 priority | user-datagram dscp-marking dscp-marking-value [ encaps-header {
copy-inner | copy-outer | dscp-marking dscp-marking-value } [ internal-qos
priority priority ] ] | pre-rel8-qos-mapping num ]
         no operator-defined-qci num
         end
```

Notes:

- This command is only visible if the license key supporting non-standard QCIs is installed. Contact your Cisco Account or Support representative for information on how to obtain a license.
- **operator-defined-qci** *num*: Specifies the operator-defined QCI value to be enabled.

  num must be an integer from 128 through 254.

  Standards-based QCI values 1 through 9 are configured through the **qci** command.
- **pre-rel8-qos-mapping** *num*: Maps non-standard QCI to a standard QCI that has the characteristics (TC, THP, SI, TD, SSD) similar to desired pre-rel8 standard QoS values during 3G call or GnGp handover.

  num must be an integer from 1 through 4 for GBR and 5 through 9 for non-GBR. QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

  3G GGSN Call

  If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI under P-GW which is associated with a GGSN, then the 3G call would be rejected.

  GnGp Handoff

  1. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for default bearer, then the handoff would be rejected.
  2. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for dedicated bearer, then only that bearer would be rejected during handoff.
  3. In the following scenario:
     - default bearer with standard QCI or non-standard QCI (with **pre-rel8-qos-mapping** configured)
     - more than one dedicated bearer (some with standard QCI, some with non-standard QCI with **pre-rel8-qos-mapping** configured, and some with non-standard QCI with no mapping)

     During LTE-to-GnGp handoff:

     - UPC Request for all the dedicated bearers with non-standard QCI with no mapping would be rejected
     - handoff will be successful for the remaining bearers

Monitoring Non-standard QCI Support

Bulk Statistics

This section provides information regarding bulk statistics in support of non-standard QCI support.

APN Schema

The following counters have been added in support of non-standard QCIs (GBR and Non-GBR):

- nonstdqci-nongbr-uplinkpkt-drop-mbrexcd
- nonstdqci-nongbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-nongbr-uplinkbyte-drop-mbrexcd
- nonstdqci-nongbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-nongbr-rejbearer
- nonstdqci-gbr-uplinkpkt-drop-mbrexcd
- nonstdqci-gbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-gbr-uplinkbyte-drop-mbrexcd
- nonstdqci-gbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-gbr-rejbearer

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of non-standard QCI support.

show apn statistics

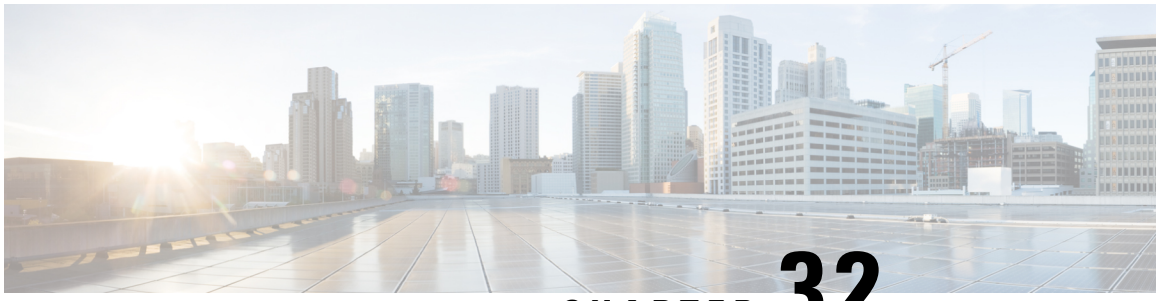
The output of this command has been enhanced to show the following non-standard QCI counters (GBR and Non-GBR):

- Non-Std QCI(Non-GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)
- Non-Std QCI(GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)

show qci-qos-mapping table all

The output of this command has been enhanced to show when non-standard QCI are configured:

- Operator-defined-qci
- pre-rel8-qos-mapping



CHAPTER 32

4G Network Upgrade on Gx Interface

- Feature Summary and Revision History, on page 545
- Feature Description, on page 546
- Configuring DRMP Priority Values , on page 546
- **Origination Time Stamp and Maximum Wait Time**, on page 547
- Monitoring and Trouble Shooting, on page 547

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.23

Feature Description

Diameter Overload Indication Conveyance (DOIC) specification passes overload information during transfer of messages to P-GW server. When there is an overload, there is no specific way to choose the messages that needs to be throttled or discarded which could result in excess traffic in the network. To reduce traffic in the network, Diameter Routing Message Priority (DRMP) is newly introduced. Using DRMP, you can set the priority for messages, based on which messages are throttled or discarded.

DRMP messages can be sent in CCR message and RAA in Gx interface only. The value to be sent in AVP can be configured using the configuration commands for below messages:

Message	Description
CCR -Initial	The CCR message is sent during connection creation.
CCR- Update	The CCR message that is sent during CCR update.
CCR-Termination	The CCR message that is sent during connection deletion.
RAA	ReAuth Answer message that is sent in response to the ReAuth Request from the PCRF.



Note If the DRMP feature is not configured, then no priority is set in the CCR/RAA messages. If DRMP is set without any priority (0 to 15), then the default priority of 10 will be set.

Configuring DRMP Priority Values

Use the following configuration commands to set the priority DRMP value:

```
configure
    context context_name
      ims-auth-service ims_auth_service_name
        policy-control
          [ no ]diameter{ drmp [ ccr-i drmp_value| ccr-t drmp_value| ccr-u
drmp_value |rra  drmp_value]}
  end
```



Note If the DRMP feature is not configured, then no priority is set in the CCR/RAA messages. If DRMP is set without any priority (0 to 15), then the default priority of 10 will be set.

Origination Time Stamp and Maximum Wait Time

Origination-Time-Stamp

Origination-Time-Stamp(1536) is a standard AVP that is added in the CCR-I messages originating from P-GW. This AVP indicates the time (NTP synced) when the request message is sent to PCRF Server from P-GW. The Origination-Time-Stamp(1536)indicates the UTC time at which the originating entity initiated the request and is encoded in the 64-bit NTP timestamp format and here, the binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part is in the last 32 bits.

Maximum-Wait-time

Maximum-Wait-time is a standard AVP (code 1537) of type of Unsigned 32. If message is received and takes a long time to process then the message is dropped by the PCRF and the CCA-I will not be sent by the PCRF. This AVP is used along with origination-timestamp AVP. Max-Wait-time (7103) is the non-standard AVP used in CCR-I messages towards Diameter Gx and it is used along with the Maximum-Wait-Time (1537) standard AVP.

Table 56: Existing AVP's

AVP Name	AVP ID
Origination-Timestamp	7102
Max-Wait-Time	7103

Table 57: New AVP's

AVP Name	AVP ID
Origination-Time-Stamp	1536
Maximum-Wait-Time	1537



Note Both new and existing AVPs are supported in this release.

Monitoring and Trouble Shooting

This section provides information on the show commands and bulk statistics.

Show Command and Output

show ims-authorization service name <service_name>

The following new fields are added to the output of this command:

- Diameter Policy Control
  - DRMP: CCR-I CCR-U CCR-T RAA

show ims-authorization policy-control statistics

The following new fields are added to the output of this command:

- DPCA Experimental Result Code Stats
  - Late Overlapping Request
  - Time Out Request

show session disconnect-reasons

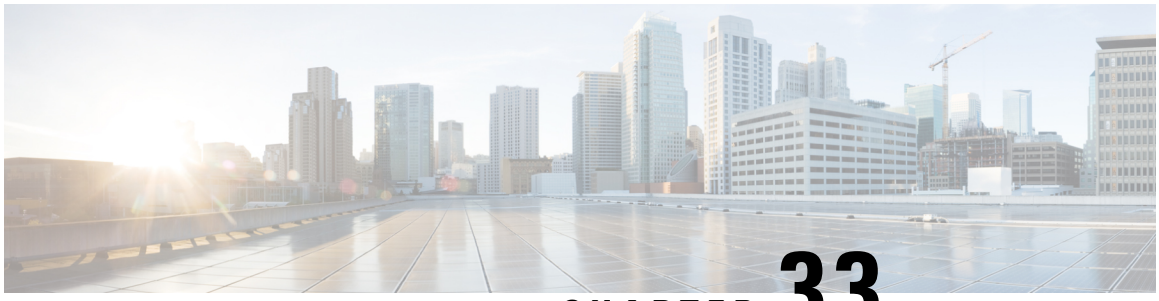
The following new fields are added to the output of this command:

- Disconnect Reason
  - newer-session-detected
  - late-overlapping-request

Bulk Statistics

The following bulk statistics are newly added:

Bulk Statistics	Description
dpca-imsa-exp-late-overlapping-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST(5453) is received in CCA message.
dpca-imsa-exp-timed-out-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_TIME_OUT_REQUEST(5454) is received in CCA message.



CHAPTER 33

GRE Protocol Interface

This chapter provides information on Generic Routing Encapsulation protocol interface support in the GGSN or P-GW service node. 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 GRE protocol 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*.

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.

- Introduction, on page 549
- Supported Standards, on page 550
- Supported Networks and Platforms, on page 551
- Licenses, on page 551
- Services and Application on GRE Interface, on page 551
- How GRE Interface Support Works, on page 551
- GRE Interface Configuration, on page 554
- Verifying Your Configuration, on page 557

Introduction

GRE protocol functionality adds one additional protocol on Cisco's multimedia core platforms (ASR 5500 or higher) to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiator.

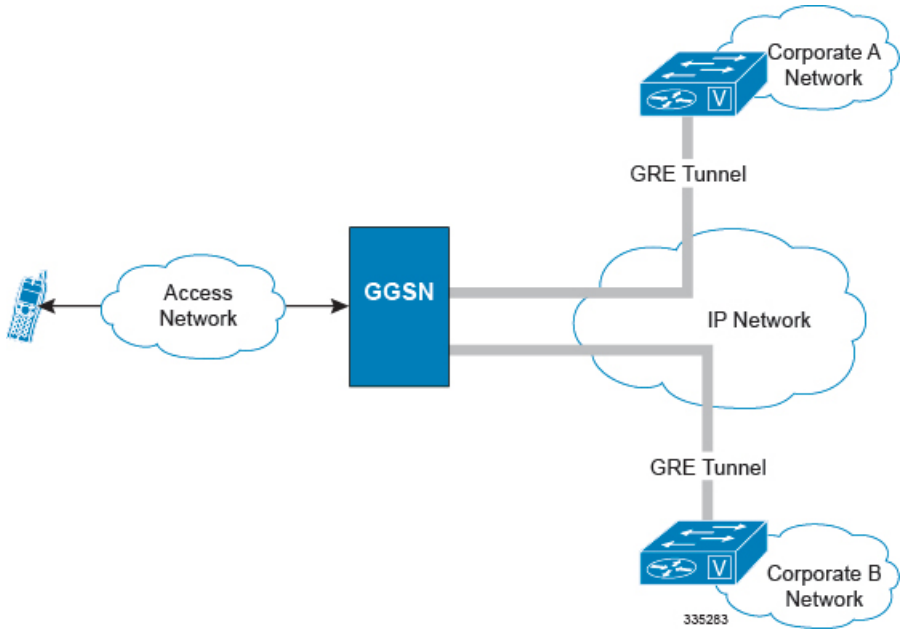
It is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

Figure 40: GRE Interface Deployment Scenario



Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2784, Generic Routing Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE

Supported Networks and Platforms

This feature supports all systems with StarOS Release 9.0 or later running GGSN and/or SGSN service for the core network services. The P-GW service supports this feature with StarOS Release 12.0 or later.

Licenses

GRE protocol 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*.

Services and Application on GRE Interface

GRE interface implementation provides the following functionality with GRE protocol support.

How GRE Interface Support Works

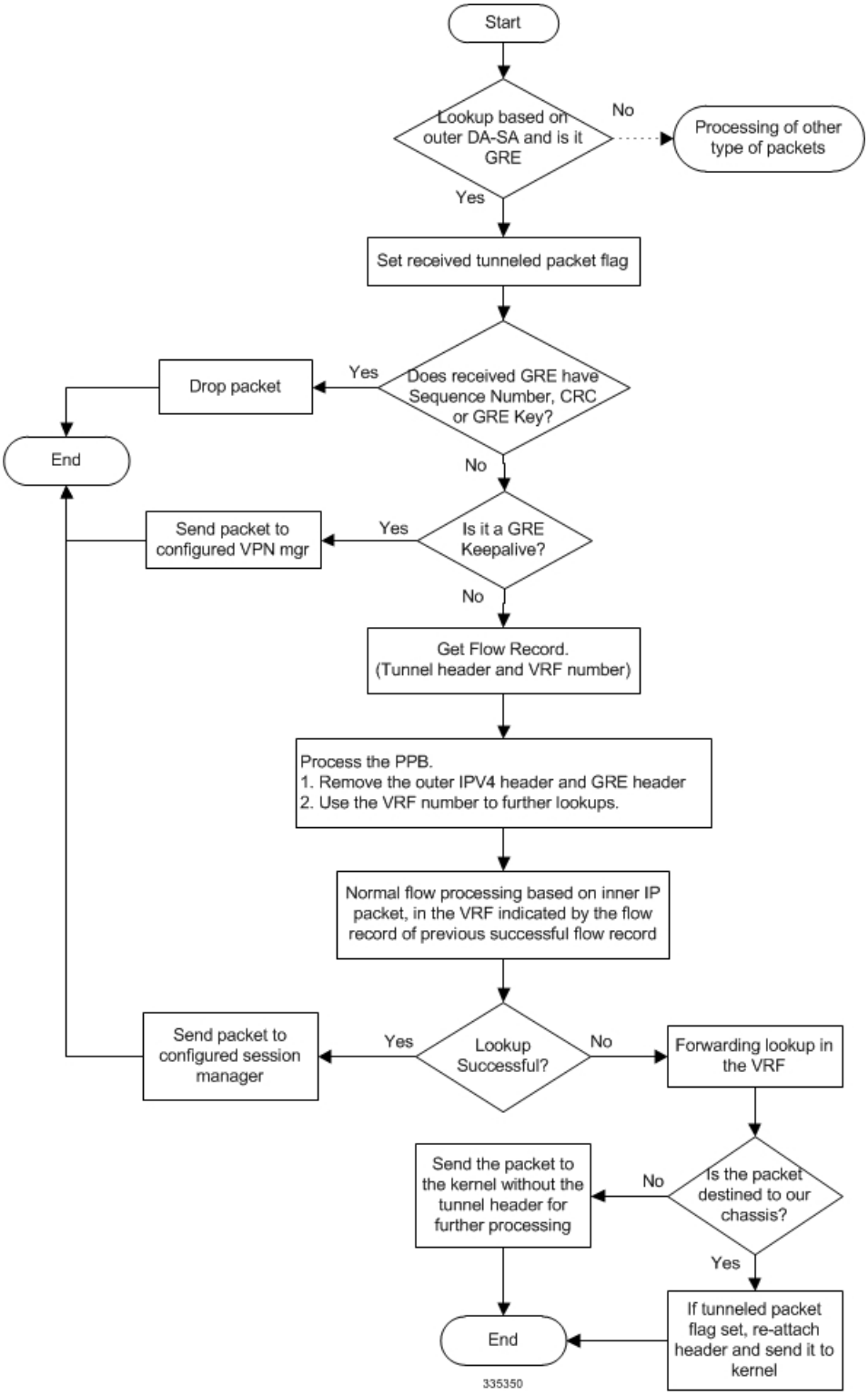
The GRE interface provides two types of data processing; one for ingress packets and another for egress packets.

Ingress Packet Processing on GRE Interface

Figure given below provides a flow of process for incoming packets on GRE interface.

Note that in case the received packet is a GRE keep-alive or a ping packet then the outer IPV4 and GRE header are not stripped off (or get reattached), but instead the packet is forwarded as is to the VPN manager or kernel respectively. In case of all other GRE tunneled packets the IPV4 and GRE header are stripped off before sending the packet for a new flow lookup.

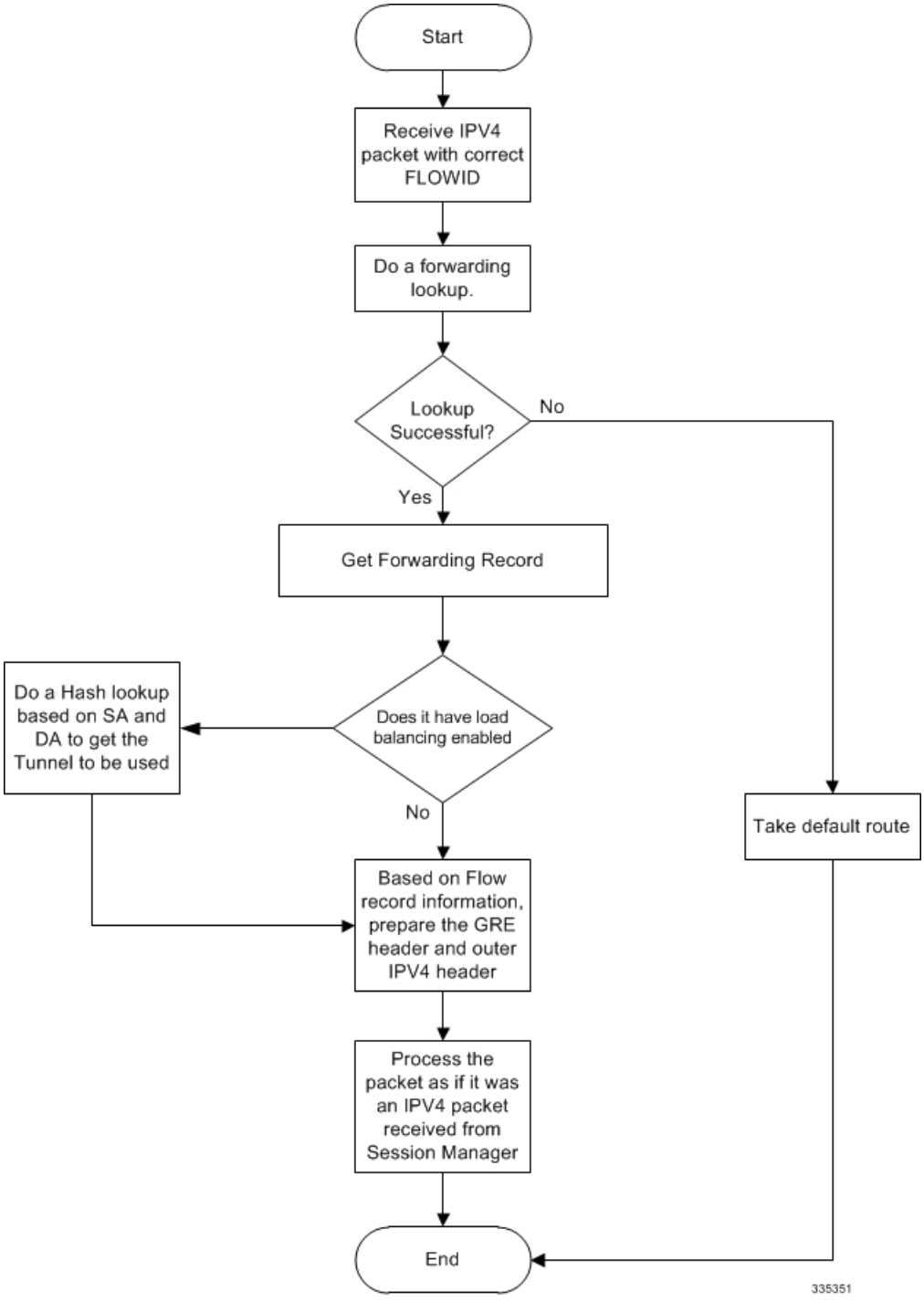
Figure 41: Ingress Packet Processing on GRE Interface



Egress Packet Processing on GRE Interface

Figure given below provides a flow of process for outgoing packets on GRE interface:

Figure 42: Egress Packet Processing on GRE Interface



GRE Interface Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with GRE interface in GGSN or P-GW services.

Important This section provides the minimum instruction set to enable the GRE Protocol Interface support functionality on a GGSN or P-GW. Commands that configure additional functions for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and specific product Administration Guide.

To configure the system to support GRE tunnel interface:

Procedure

Step 1 Configure the virtual routing and forwarding (VRF) in a context by applying the example configurations presented in Virtual Routing And Forwarding (VRF) Configuration, on page 554.

Step 2 Configure the GRE tunnel interface in a context by applying the example configurations presented in GRE Tunnel Interface Configuration, on page 555.

Step 3 Enable OSPF for the VRF and for the given network by applying the example configurations presented in Enabling OSPF for VRF, on page 555.

Step 4 Associate IP pool and AAA server group with VRF by applying the example configurations presented in Associating IP Pool and AAA Group with VRF, on page 556.

Step 5 Associate APN with VRF through AAA server group and IP pool by applying the example configurations presented in Associating APN with VRF, on page 556.

Step 6 Optional. If the route to the server is not learnt from the corporate over OSPFv2, static route can be configured by applying the example configurations presented in Static Route Configuration, on page 557.

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*.

Step 8 Verify configuration of GRE and VRF related parameters by applying the commands provided in Verifying Your Configuration, on page 557.

Virtual Routing And Forwarding (VRF) Configuration

This section provides the configuration example to configure the VRF in a context:

```
configure
   context <vpn_context_name> -noconfirm ]
      ip vrf <vrf_name>
         ip maximum-routes <max_routes>
         end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for VRF. For more information, refer *System Administration Guide*.
- A maximum of 300 VRFs per context and up to 2,048 VRFs per chassis can be configured on system.
- <*vrf_name*> is name of the VRF which is to be associated with various interfaces.
- A maximum of 10000 routes can be configured through **ip maximum-routes** <*max_routes*> command.

GRE Tunnel Interface Configuration

This section provides the configuration example to configure the GRE tunnel interface and associate a VRF with GRE interface:

```
configure
  context <vpn_context_name>
    ip interface <intfc_name> tunnel
      ip vrf forwarding <vrf_name>
        ip address <internal_ip_address/mask>
        tunnel-mode gre
        source interface <non_tunn_intfc_to_corp>
        destination address <global_ip_address>
        keepalive interval <value> num-retry <retry>
        end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for GRE interface configuration. For more information, refer *Command Line Interface Reference*.
- A maximum of 511 GRE tunnels + 1 non-tunnel interface can be configured in one context. System needs at least 1 non-tunnel interface as a default.
- <*intfc_name*> is name of the IP interface which is defined as a tunnel type interface and to be used for GRE tunnel interface.
- <*vrf_name*> is the name of the VRF which is preconfigured in context configuration mode.
- <*internal_ip_address*/mask> is the network IP address with sub-net mask to be used for VRF forwarding.
- <*non_tunn_intfc_to_corp*> is the name a non-tunnel interface which is required by system as source interface and preconfigured. For more information on interface configuration refer *System Administration Guide*.
- <*global_ip_address*> is a globally reachable IP address to be used as a destination address.

Enabling OSPF for VRF

This section provides the configuration example to enable the OSPF for VRF to support GRE tunnel interface:

```
configure
  context <vpn_context_name>
    router ospf
      ip vrf <vrf_name>
      network <internal_ip_address/mask>
      end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for OSPF routing. For more information, refer *Routing* in this guide.
- <*vrf_name*> is the name of the VRF which is preconfigured in context configuration mode.
- <*internal_ip_address/mask*> is the network IP address with sub-net mask to be used for OSPF routing.

Associating IP Pool and AAA Group with VRF

This section provides the configuration example for associating IP pool and AAA groups with VRF:

```
configure
   context <vpn_context_name>
      ip pool <ip_pool_name> <internal_ip_address/mask> vrf <vrf_name>
         exit
      aaa group <aaa_server_group>
         ip vrf <vrf_name>
         end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for IP pool and AAA server group.
- <*ip_pool_name*> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <*aaa_server_group*> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <*vrf_name*> is the name of the VRF which is preconfigured in context configuration mode.
- <*internal_ip_address/mask*> is the network IP address with sub-net mask to be used for IP pool.

Associating APN with VRF

This section provides the configuration example for associating an APN with VRF through AAA group and IP pool:

```
configure
   context <vpn_context_name>
      apn <apn_name>
         aaa group <aaa_server_group>
         ip address pool name <ip_pool_name>
         end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for APN configuration.
- <*ip_pool_name*> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <*aaa_server_group*> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <*vrf_name*> is the name of the VRF which is preconfigured in context configuration mode.

Static Route Configuration

This section provides the optional configuration example for configuring static routes when the route to the server is not learnt from the corporate over OSPFv2:

```
configure
  context <vpn_context_name>
    ip route <internal_ip_address/mask> tunnel <tunnel_intfc_name> vrf <vrf_name>
    end
```

Notes:

- <*vpn_context_name*> is the name of the system context you want to use for static route configuration.
- <*internal_ip_address/mask*> is the network IP address with sub-net mask to be used as static route.
- <*tunnel_intfc_name*> is name of a predefined tunnel type IP interface which is to be used for GRE tunnel interface.
- <*vrf_name*> is the name of the VRF which is preconfigured in context configuration mode.

Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the *System Administration Guide* and also to retrieve errors and warnings within an active configuration for a service.



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

These instructions are used to verify the GRE interface configuration.

Procedure

Step 1 Verify that your interfaces are configured properly by entering the following command in Exec Mode:

`show ip interface`

The output of this command displays the configuration of the all interfaces configured in a context.

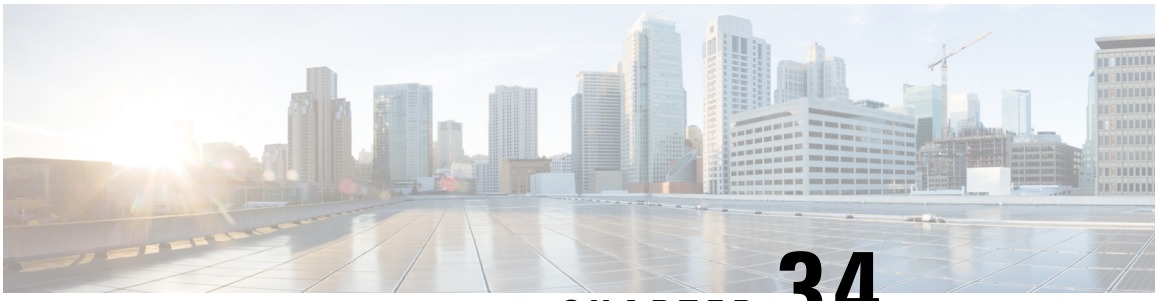
```
Intf Name:     foo1
Intf Type:             Broadcast
Description:
IP State:              UP (Bound to 17/2 untagged, ifIndex 285343745)
IP Address:            209.165.200.225         Subnet Mask:         255.255.255.0
Bcast Address:         209.165.200.254             MTU:                 1500
Resoln Type:           ARP                   ARP timeout:         60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
Intf Name:             foo2
Intf Type:             Tunnel (GRE)
Description:
VRF:                   vrf-tun
IP State:              UP (Bound to local address 209.165.200.225 (foo1), remote address
209.165.200.229)
IP Address:            209.165.200.228              Subnet Mask:         255.255.255.224
```

```
Intf Name:              foo3
Intf Type:              Tunnel (GRE)
Description:
IP State:               DOWN (<state explaining the reason of being down>)
IP Address:             209.165.200.232            Subnet Mask:         255.255.255.224
```

Step 2 Verify that GRE keep alive is configured properly by entering the following command in Exec Mode:

`show ip interface gre-keepalive`

The output of this command displays the configuration of the keepalive for GRE interface configured in a context.



CHAPTER 34

GGSN UPC Collision Handling

• GGSN UPC Collision Handling, on page 559

GGSN UPC Collision Handling

Feature Description

During collision between SGSN-initiated UPC request and GGSN-initiated UPC Request, SGSN-initiated UPC request gets higher priority over Network Operated (NRUPC). With the UPC Collision Handling feature, there is no call or data loss during call establishment or during mid-call phase. This feature can be enabled or disabled using a CLI and is enabled by default.

- When GGSN detects collision between SGSN initiated UPC request and NRUPC on primary PDP context, NRUPC is retried (with different sequence number) after sending UPC Response.
- When GGSN detects collision between SGSN initiated UPC request for Inter-SGSN handoff and NRUPC with TFT and after handoff BCM mode is changed from Mixed mode to MS-Only mode, NRUPC is retried (with different sequence number) after sending UPC Response, but without TFT.
- When GGSN detects collision between an SGSN initiated UPC and a NRUPC on secondary PDP context, NRUPC is aborted and PCRF is notified. When multiple CCR-U support is not enabled on GGSN, CCR-U for aborted NRUPC (on secondary PDP context) is not informed to PCRF. In this case, PCRF will not be aware of this aborted transaction (rule failure).

Note During S2bGTP to LTE handoff procedure, when there is already a pending transaction and a Handoff request is received by SAE-GW, Handoff is rejected with a following message:

```
Rejecting S2b/LTE Handoff as only one pending transaction is supported
```

Limitations

- Behavior for GnGp GGSN has been modified for this feature, in this release. Behavior for GGSN remains unaltered.

- When NRUPC received from Direct Tunnel (due to "Direct Tunnel Error Indication") collides with SGSN initiated UPC request, NRUPC is aborted and not retried. This does not affect the functionality as, when "Direct Tunnel Error Indication" is received from access side, NRUPC is triggered again.
- When a request for handoff to LTE is received before receiving NRUPC response, the behavior remains unchanged. In this case, the pending NRUPC request is aborted. If the NRUPC request received is for rule installation, the request remains in the pending state and the rule is not installed. As there is no static rule and the rule installation request is in pending state, the PDP context stays up without an installed rule.

Configuring GGSN UPC Collision Handling

Operators can use the Command Line Interface (CLI) to configure the collision between SGSN initiated UPC request and network initiated UPC Request.

gtpc handle-collision

This command in the service configuration mode can be used to the collision between SGSN initiated UPC request and network initiated UPC Request.

GGSN Service

```
configure
     context context_name
       ggsn-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

P-GW Service

```
configure
     context context_name
       pgw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

S-GW Service

```
configure
     context context_name
       sgw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

SAEGW Service

```
configure
     context context_name
       saegw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

Notes:

- **no:** Disables collision handling between SGSN initiated UPC and NRUPC request.

- **default:** Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.
- **handle-collision upc nrupc:** Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show configuration verbose**

Please see the *Monitoring and Troubleshooting GGSN UPC Collision Handling* section for the command output.

Monitoring and Troubleshooting GGSN UPC Collision Handling

The following section describes commands available to monitor GGSN UPC Collision Handling.

Show Commands for GGSN UPC Collision Handling

show configuration

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show configuration verbose

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show ggsn-service name *service_name*

This command displays the following output:

```
Service name:                       ggsn-service
Context:                            ingress
…
Suppress NRUPC triggered by UPC:    Disabled
```

```
Collision handling for UPC-NRUPC:  Enabled/Disabled
```

show gtpc statistics

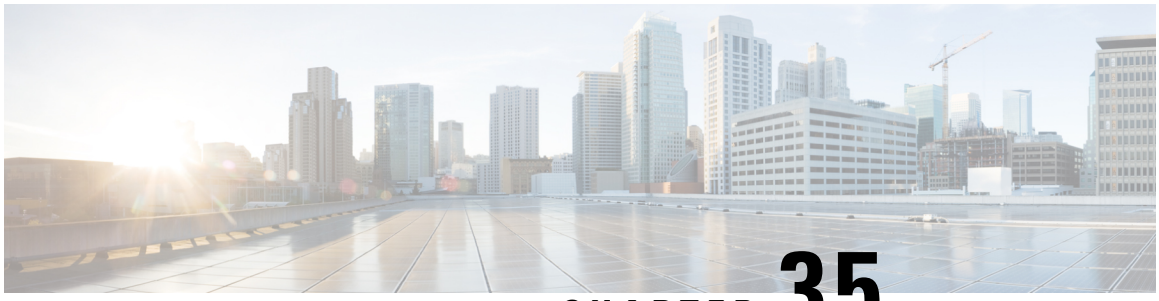
This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:                        1
  2G:                           0
  3G:                           1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:       0   Accepted:                     0
  Denied:                       0   Discarded:                    0

NRUPC UPC Collision:
  Primary PDP ctxt:             3   Secondary PDP ctxt:           0

QoS negotiation:
  CPC QoS Accepted:             3   CPC QoS Downgraded:           0
  UPC QoS Accepted:             3   UPC QoS Downgraded:           0
```

show gtpc statistics [format1 | ggsn-service *service_name* | verbose]

This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:                        1
  2G:                           0
  3G:                           1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:       0   Accepted:                     0
  Denied:                       0   Discarded:                    0

NRUPC UPC Collision:
  Primary PDP ctxt:             3   Secondary PDP ctxt:           0

QoS negotiation:
  CPC QoS Accepted:             3   CPC QoS Downgraded:           0
  UPC QoS Accepted:             3   UPC QoS Downgraded:           0
```



CHAPTER 35

GTP-based S2b Interface Support on the P-GW and SAEGW

This chapter describes the GTP-based S2b interface support feature on the standalone P-GW and the SAEGW.

- Feature Description, on page 563
- How the S2b Architecture Works, on page 565
- How the S2a Architecture Works, on page 587
- Configuring the GTP-based S2b Interface on the P-GW and SAEGW, on page 601
- Monitoring the GTP-based S2b Interface Feature, on page 602
- Monitoring the GTP-based S2a Interface Feature, on page 604

Feature Description

This section describes the GTP-based S2a/S2b interface implementation on the P-GW and SAEGW.

GTP-based S2b Interface Support on the Standalone P-GW and SAEGW

Important GTP-based S2b interface support is a license-controlled feature. Contact your Cisco account or support representative for licensing information.

The S2b interface reference point connects the standalone P-GW with the ePDG and the P-GW of the SAEGW with the ePDG. Communication runs between the non-trusted non-3GPP ePDG (Evolved Packet Data Gateway) and the P-GW uses PMIPv6 (Proxy Mobile IP version 6) for providing access to the EPC. GTPv2-C is the signaling protocol used on the S2b. The S2b interface is based on 3GPP TS 29.274.

The S2b interface uses the PMIPv6 protocol to establish WLAN UE sessions with the P-GW. It also supports the transport of P-CSCF attributes and DNS attributes in PBU (Proxy-MIP Binding Update) and PBA (Proxy-MIP Binding Acknowledgment) messages as part of the P-CSCF discovery performed by the WLAN UEs. When the P-CSCF Address information is missing, P-CSCF Discovery is initiated upon an S4-SGSN-to-LTE (and vice versa) handoff. If the P-CSCF Address information is already available, there is no need to explicitly trigger another P-CSCF Discovery upon S4-SGSN to LTE (and vice versa) handoff.

Example: The UE tries to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports

such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies. So the UE can have independent PDN connections via multiple access types.

The access types supported are 4G and WiFi.

The S2b interface implementation on the P-GW and SAEGW supports the following functionality:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff

GTP-based S2a Interface Support on the Standalone P-GW and SAEGW



Important GTP-Based S2a Interface Support is a licensed-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

GTP-based S2a interface support is available on the P-GW and SAEGW. Operators deployed with the SAEGW are now able to integrate Trusted WiFi network functionality using this feature.

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD. Specifically, the S2a interface supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the standalone P-GW or P-GW of the SAEGW. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

When the WLAN is considered as trusted by the operator, the Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the S2a interface to the P-GW. Support has been extended for WiFi-to-LTE handovers using Make and Break for the SAEGW service. Multi-PDN handovers are also supported as part of this feature.

Supported functionality includes:

- Initial Attach
- WiFi-to-LTE handover
- LTE-to-WiFi handover
- Multi-PDN handovers

Supported protocols include:

- Transport Layer: UDP, TCP
- Tunneling: GRE IPv6
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Relationships to Other Features

This section describes how the GTP-based S2b and S2a interface support feature is related to other features.

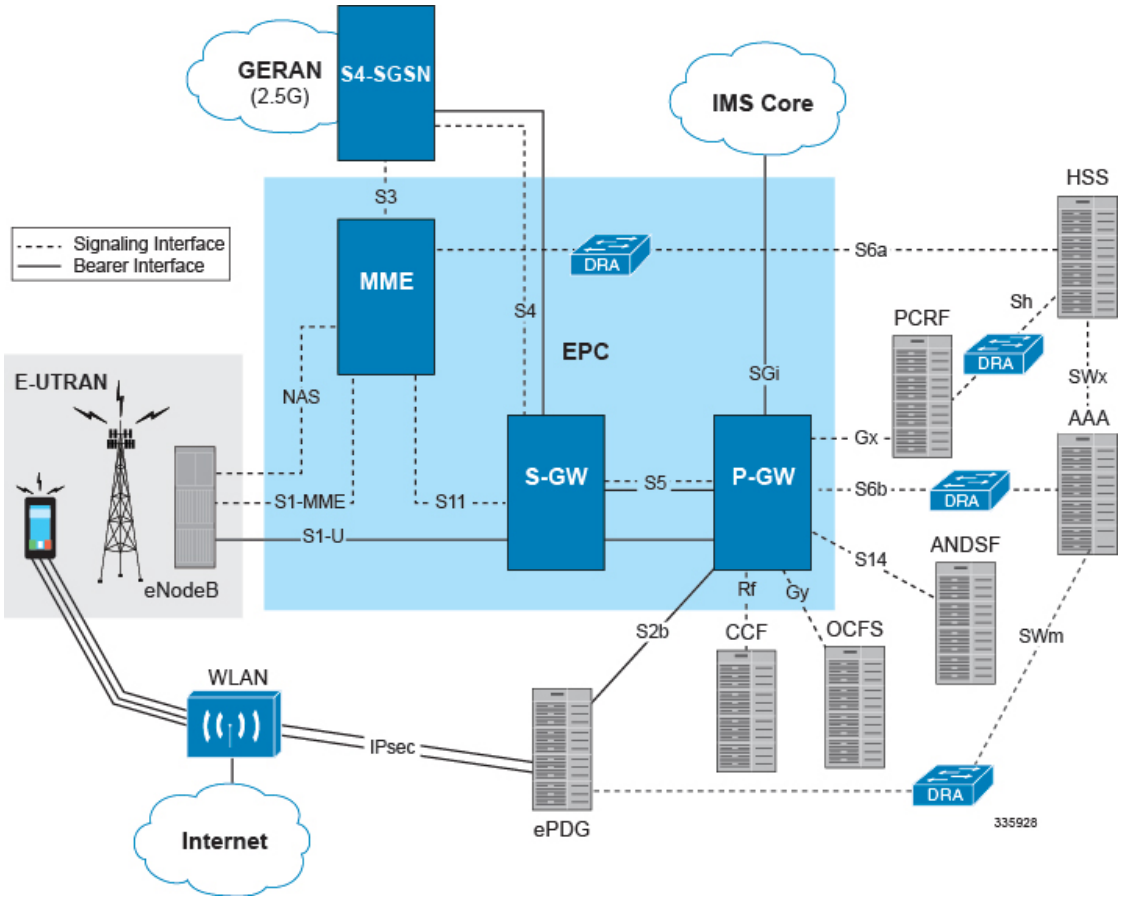
- A P-GW service must be configured and operational before GTP-based s2b interface support can be configured on the standalone P-GW and SAEGW.
- GTP-based S2b interface support must also be configured and operational on the ePDG to support this feature.
- A P-GW service must be configured and operational before GTP-based S2a interface support can be configured on the standalone P-GW and SAEGW.

How the S2b Architecture Works

Standalone P-GW Architecture for S2b Interface Support

The GTP-based S2b interface architecture is part of the P-GW deployment in the E-UTRAN/EPC Network. The P-GW communicates with the ePDG over the S2b interface, and the ePDG connects to the WLAN offload architecture via an IPSec interface.

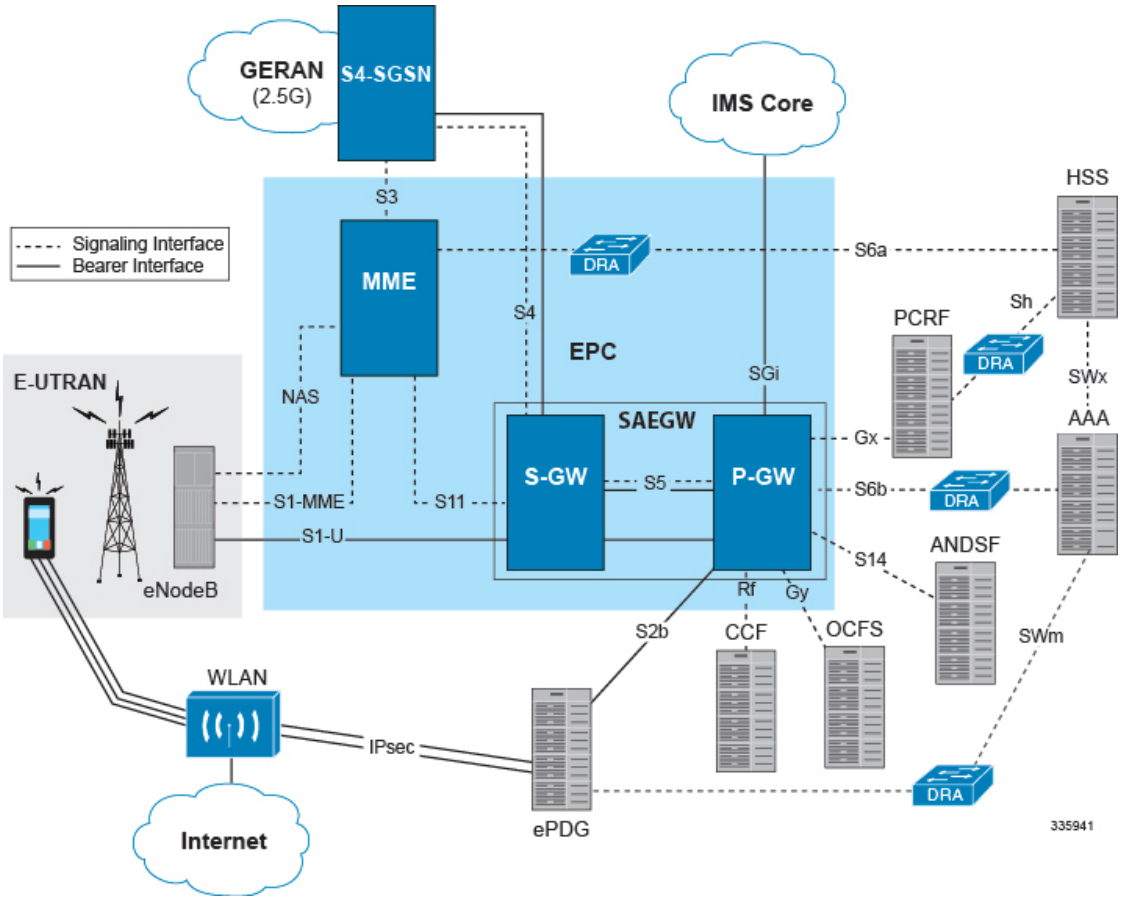
Figure 43: Standalone P-GW: GTP-based S2b Interface Implementation in the E-UTRAN/EPC Network



SAEGW Architecture for S2b Interface Support

The GTP-based S2b interface architecture is part of the SAEGW deployment in the E-UTRAN/EPC Network. The P-GW of the SAEGW communicates with the ePDG over the S2b interface, and the ePDG connects to the WLAN offload architecture via an IPSec interface.

Figure 44: SAEGW: GTP-based S2b Interface Implementation in the E-UTRAN/EPC Network



Limitations on S2b Interface Support for the P-GW and SAEGW

Note the following limitations of the GTP-based S2b interface implementation on the P-GW and SAEGW:

- Only the following interfaces/access types from the WiFi Offload and VLC Flows are supported:
- Access Types:
  - WiFi
  - LTE
- Interfaces:
  - S6b
  - Gy
  - Rf

- Gx
- GTPv2 (S2b)

- Legacy Lawful Intercept is supported on the S2b interface on the standalone P-GW, but is not qualified on the S2b interface on the SAEGW at this time.

Standalone P-GW Call Flows

This section provides call flows that illustrate the basic functionality of the GTP-based S2b interface support on the standalone P-GW.

Figure 45: Initial Attach Call Flow - P-GW

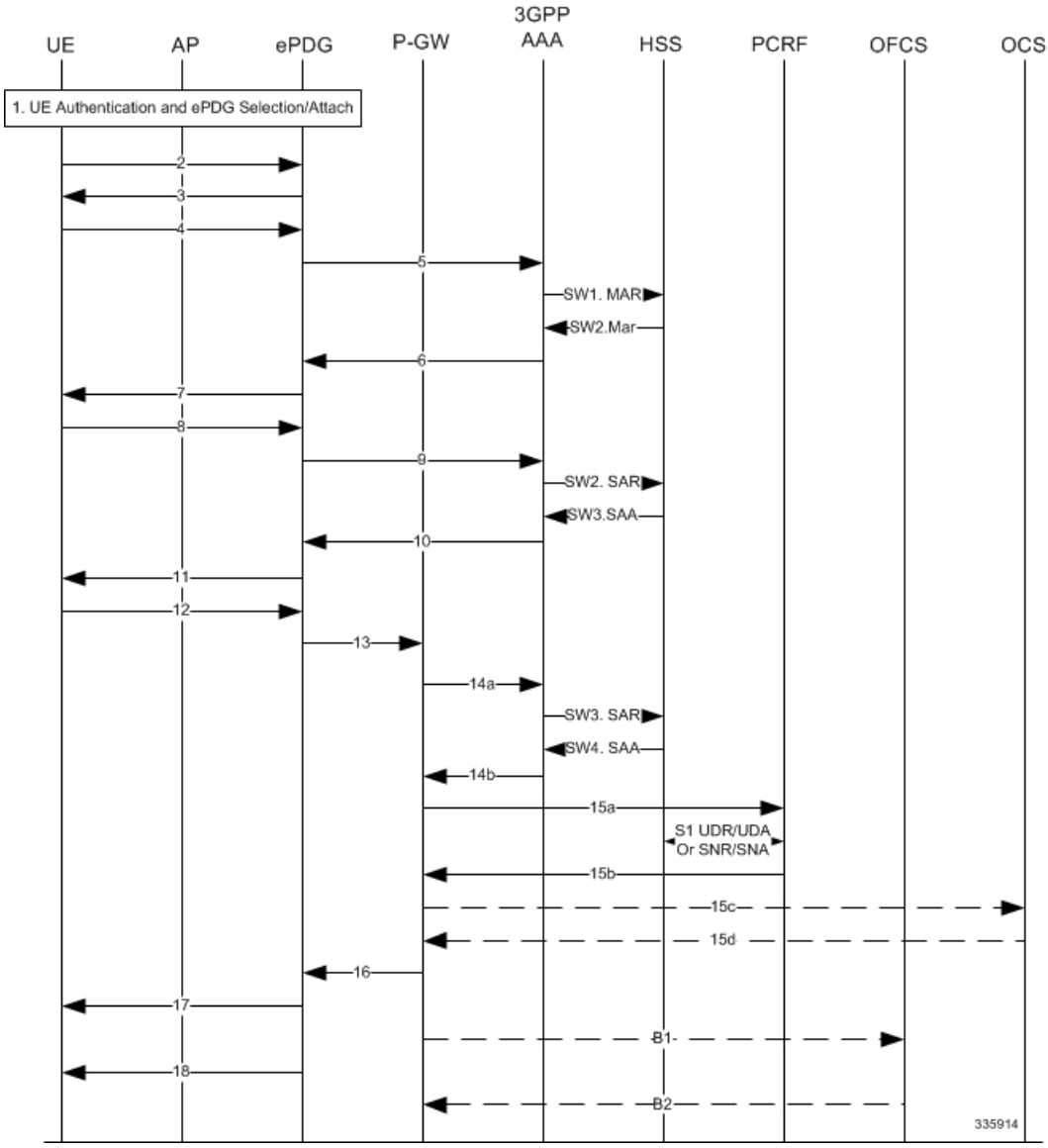


Table 58: Initial Attach - P-GW

Step	Description
1	UE performs initial Access Point association and authentication if necessary.
2 - 11	The UE creates a connection with the ePDG.
12	UE sends IKE_AUTH request (AUTH). The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG selects the P-GW based on Node Selection options. The ePDG sends Create Session Request.
14a	The P-GW sends AAR to the 3GPP AAA to authorize the PDN for the subscriber and to update P-GW address on the HSS for the APN.
SW3	The 3GPP AAA updates the HSS with the P-GW address for the APN and retrieves Subscriber-APN profiles from the HSS.
SW4	The HSS sends Server-Assignment-Answer (Session-Id, Result-Code, Experimental-Result (Vendor-Id, Experimental-Result-Code))
14b	The 3GPP AAA sends AAA.
15a	The P-GW sends an indication of IP-CAN establishment to the PCRF with CCR to indicate establishment of a new IP CAN session.
S1	The PCRF downloads (and caches) user profile (by sending an Sh: UDR (User-Identity, Service-Indication, Data-Reference) and receiving an Sh: UDA (Result-Code, User-Data)).
S2	The PCRF may subscribe to profile update notification.
15b	The PCRF Acknowledges IP CAN Session Establishment with a CCA message.
15c	If the Online AVP is set in the CCA from the PCRF (UC users / CF / RTR), the P-GW shall conditionally send a CCR-Initial.
15d	The OCS responds with a CCA to the P-GW.
16	The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
17	The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
18	ePDG sends Router Advertisement to ensure IP Stack is fully initialized. P-GW disables the Router Advertisement to the UE.
B1	If the Offline AVP is set in the CCA from the PCRF, then after IP-CAN session establishment procedure is complete, the P-GW shall send a ACR-Start to the OFCS.
B2	The OFCS responds with an ACA to the P-GW.

Figure 46: P-GW: LTE to WiFi Handoff Call Flow

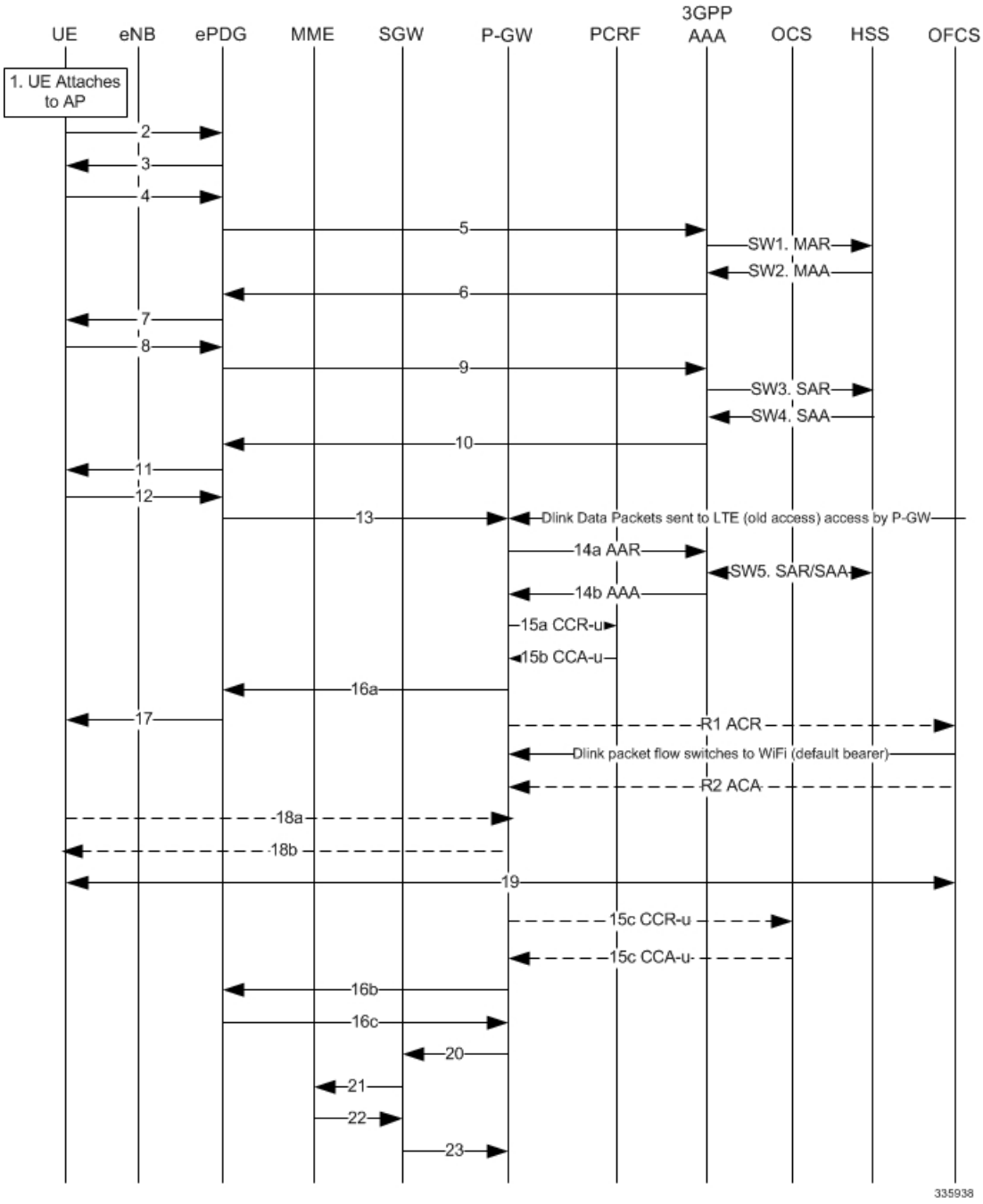


Table 59: P-GW LTE to WiFi Handoff

Step	Description
1	Authentication and ePDG Selection. UE performs initial Access Point association and authentication if necessary.

Step	Description
2	UE to ePDG: IKEv2 SA_INIT. The UE sends IKE_SA_INIT Request.
3	ePDG to UE: INIT Response. The ePDG responds with an IKE_SA_INIT Response. The ePDG will start the IKEv2 setup timer when sending the IKE_SA_INIT Response.
4	UE sends Auth_Request.
5	ePDG to AAA: DER. The ePDG sends the DER message to the 3GPP AAA Server. Note the NAI shall not contain the AP MAC address sent in the username that comes in the IKE message
SW1. MAR	AAA to HSS: MAR. The 3GPP AAA Server fetches the user profile and authentication vectors from HSS over SWx. The 3GPP AAA server look up the IMSI of the authenticated user based on the received user identity and includes the EAP-AKA as requested authentication method in the request sent to the HSS. The AAA sends the Multimedia-Auth-Request MAR, Origin-Host, Origin-Realm, Destination-Realm, Destination-Host, User-Name, RAT-Type, SIP-Auth-Data-Item, SIP-Number-Auth-Items, and Routing-Information).
SW2. MAA	HSS to AAA: MAA. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The HSS sends the Multimedia-Auth-Answer MAA.
6	AAA to ePDG: DEA. The 3GPP AAA Server initiates the authentication challenge and responds with DEA.
7	ePDG to UE: IKE_AUTH. The ePDG responds with IKE_AUTH. The identity is the IP address of the ePDG; the AUTH payload authenticates the first IKE_SA_INIT response. If the UE requested certificates, the CERT is included. The EAP message received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.
8	UE to ePDG: IKE_AUTH Request. The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message IKE_AUTH Request (EAP).
9	ePDG to AAA: DER. The ePDG sends DER (Base AVPs, Auth Request Type, EAP Payload, Auth-Session-State, Service Selection) to the 3GPP AAA Server.
SW3. SAR	AAA to' HSS: SAR. The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the authenticated user. The AAA sends Server-Assignment-Request, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, User-Name (IMSI-NAI), Server-Assignment-Type (REGISTRATION)).
SW4 SAA	HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
10	AAA to ePDG: DEA. The 3GPP AAA Server sends an EAP success. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access before responding with DEA.
11	ePDG to UE: IKE_AUTH_Response. ePDG sends IKE_AUTH_Response (EAP).

Step	Description
12	UE to ePDG: IKE_AUTH_Request. UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG to P-GW: Create Session Request. The ePDG sends Create Session Request to the P-GW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.
14a	P-GW to 3GPP-AAA: AAR. The P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
SW5. SAR/SAA	AAA to HSS: SAR. The 3GPP AAA updates the HSS with the P-GW address for the APN. The AAA sends Server-Assignment-Request.
14b AAA	3GPP AAA to P-GW: AAA. 3GPP AAA sends AAA to the P-GW.
15a CCR-u	P-GW to PCRF: CCR-U. The P-GW sends an indication of IP-CAN modification to the PCRF with CCR to indicate modification of the IP-CAN session.
15b CCA-u	PCRF to P-GW: CCA. The PCRF Acknowledges of IP-CAN Session Modification with a CCA message. This message includes the Policy and Charging rules the P-GW will enforce and triggers for events that must be reported by the P-GW.
16a	P-GW to ePDG: Create Session Response. The P-GW identifies the S5 session and re-allocates the requested IP address session and responds back to the ePDG with a Create Session Response message. The P-CSCF private IE is included if the ePDG had included the P-CSCF request in message 13.
17	ePDG to UE: IKE_AUTH. The ePDG sends IKE_AUTH.
R1 ACR	P-GW to OFCS: ACR. The P-GW sends an ACR-Interim to the OFCS.
R2 ACA	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW.
18a	UE sends a Router Solicitation message.
18b	The P-GW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
19	The UE sends a SIP Re-Register once it successfully identifies it has changed access network to indicate the RAT change to the P-CSCF and assigned IP address is unchanged. UE will include 802.11 a/b/g/n in the PANI header. The SIP re-registration does not impact the way the P-CSCF does charging as charging is not used from the P-CSCF in IMS case.
15c CCR-u	P-GW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
15d CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW.
16b	P-GW to ePDG: Create Bearer Request. The IMS PDN has one or more dedicated bearers established prior to handoff and the P-GW also sends Create Bearer Request to the ePDG. Note that Charging ID is not sent on S2b.

Step	Description
16c	ePDG to P-GW: Create Bearer Response. The ePDG sends Create Bearer Response message
20	P-GW to S-GW: Delete Bearer Request. The P-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the S-GW. This message may be sent any time after message 13, the create session request.
21	S-GW to MME: Delete Bearer Request. The S-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the MME. The MME releases the E-UTRAN bearers if not already released. The MME does not send Notify Request to HSS at this point, as the cause IE is RAT change to Non-3GPP. MME does not page the UE either or initiate any NAS signaling and remove the locally stored PDN state and does S1 context release to the eNodeB if it has not already been triggered by the eNodeB. For last PDN MME removes all locally stored UE state.
22	MME to S-GW: Delete Bearer Response. The MME sends Delete Bearer Response to the S-GW.
23	S-GW to P-GW: Delete Bearer Response. The S-GW sends Delete Bearer Response to the P-GW.

Figure 47: P-GW: WiFi to LTE Handoff

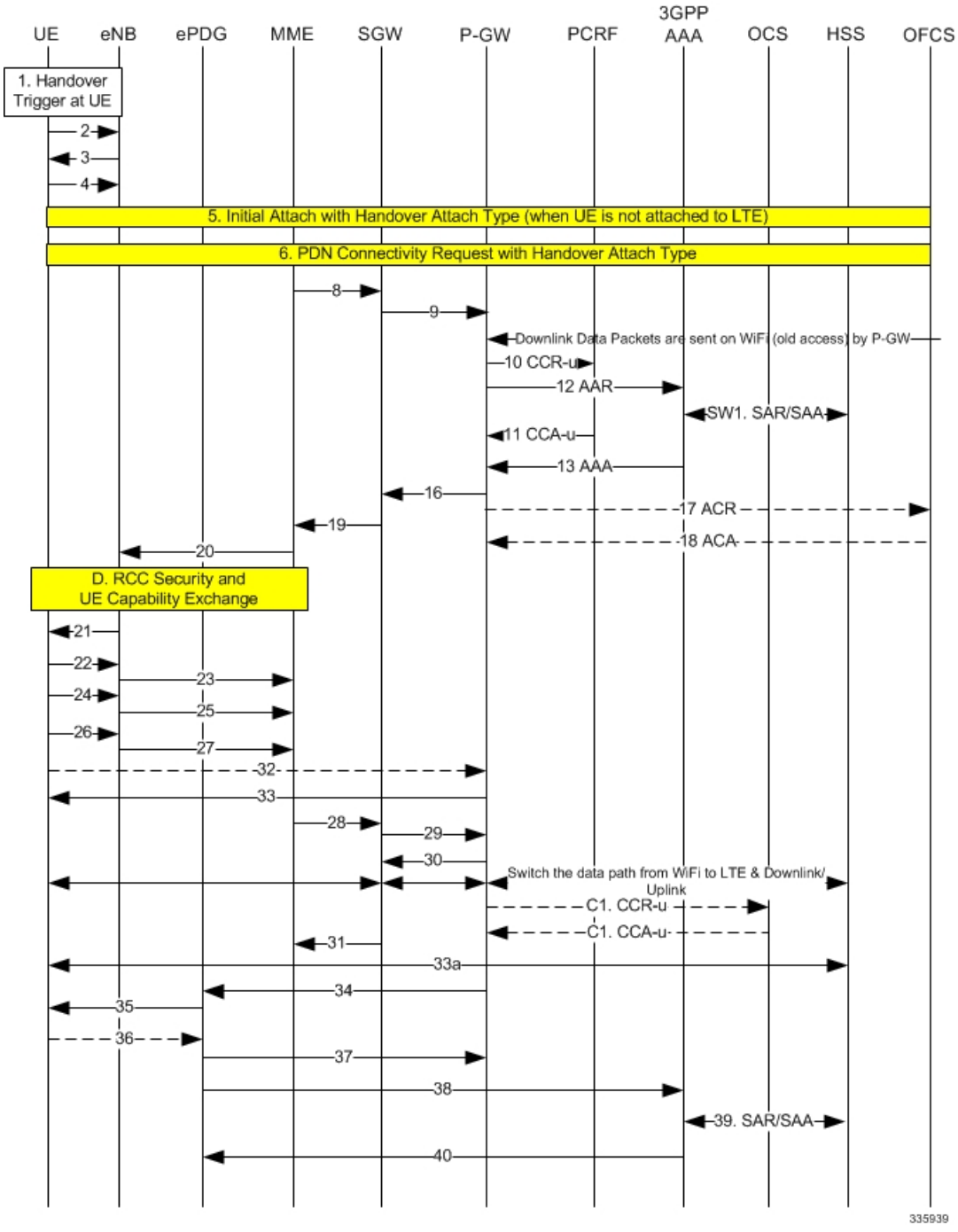


Table 60: P-GW WiFi to LTE Handoff Procedure

Step	Description
1	A handover trigger occurs at the UE.

Step	Description
2, 3	RRC Connection Request/Connection Setup. The UE and eNodeB exchange signaling to set up an RRC connection (5.3.3, TS 36.331).
4	RRC Connection Setup Complete [Attach Request]. The UE sends RRC Connection Setup Complete message to the eNodeB.
5	Attach Request from eNB to MME. The UE indicates in the Attach Request to LTE that this is a Handover Attach. The eNodeB selects the MME. The eNodeB forwards the Attach Request message in an Initial UE Message to the MME.
6	MME selects the same P-GW based on HSS provided PGW FQDN and sends the Create Session request.
8	The MME selects the PGW/SGW. The MME sends a Create Session Request to the SGW with RAT as EUTRAN and the handoff indicator set to TRUE.
9	The SGW sends a Create Session Request to the PDN GW in order to establish the handoff (handoffindicator is set to true). RAT type is E-UTRAN.
10	P-GW to PCRF CCR IP-CAN Session Modification Procedure. The PCEF sends a CC-Request (CCR) Command with CC-Request-Type set to UPDATE_REQUEST. The APN-AMBR is included in the QoS-information AVP.
12	The P-GW sends AAR to 3GPP-AAA and includes the RAT type of the new connection.
SW1. SAR/SAA	The 3GPP-AAA sends SAR to HSS to retrieve the user profile, the HSS returns an SAA. The P-GW-FQDN is not updated as the 3GPP-AAA is not registered for this user.
11	PCRF ' P-GW: CCA IP-CAN Session modification Procedure. On receiving the CCR the PCRF shall send a CC-Answer (CCA) Command to install the PCC rules and event triggers for all configured and established bearers. The QoS-Information AVP contains APN-AMBR-UL and APN-AMBR-DL.
13	The 3GPP-AAA responds with AAA.
16	P-GW to S-GW: Create Session Response + Create Bearer Request. The P-GW responds with a Create Session Response message to the S-GW. The P-GW provides IPv6 Prefix. Subject to operator configuration the P-GW can begin to forward downlink data and the S-GW shall buffer any downlink data packets.
17	P-GW to OFCS: ACR. After the P-GW sends the PBA, the P-GW shall send an ACR-Interim to the OFCS.
18	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW.
19	Create Session Response. The S-GW sends Create Session Response to the MME.
20	Initial Context Setup Request/Attach Accept. The Attach Accept is sent as NAS PDU in the Initial Context Setup Request from MME to eNodeB. Attach Accept message contains new GUTI.

Step	Description
D	These procedures occur independently of the location procedures. These procedures only apply to initial attach scenarios.
21	RRC Connection Re-configuration. The eNodeB sends the RRC Connection Reconfiguration message including the EPS Radio Bearer Identity to the UE, and the Attach Accept message to the UE. The APN is provided to the UE to notify it of the APN for which the activated default bearer is associated.
22	RRC Connection Re-configuration Complete. The UE sends the RRC Connection Reconfiguration Complete message to the eNodeB.
23	Initial Context Setup Response. The eNodeB sends Initial Context Setup Response to the MME.
24	Uplink Information Transfer. The UE sends an Uplink Information Transfer message.
25	Attach Complete. The eNodeB forwards the received Attach Complete message in an Uplink NAS Transport as part of NAS PDU.
26	Uplink Information Transfer. When the UE has received Activate dedicated EPS Bearer Context Request message in the Attach Accept message, the UE sends Activate Dedicated EPS Bearer Context Accept message in a Uplink Information Transfer message.
27	UL NAS Transport. The eNB passes the Activate Dedicated EPS Bearer Context Accept message received in Step 14.b, to the MME in a UL NAS Transport message. At this time, the uplink data can be sent on the dedicated bearer.
32	Router Solicitation. This step may happen any time after step 26. For IPv6 PDN, the UE may send a Router Solicitation to the P-GW.
33	Router Advertisement. This step may happen any time after step 29 if the UE requested IPv4v6 or IPv6 PDN type. On receipt of the RS or prior the P-GW shall send a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
28	Modify Bearer Request / Create Bearer Response. On receiving both Initial Context Setup Response and Attach Complete, the MME sends a Modify Bearer Request message to the S-GW. The MME piggybacks the Modify Bearer Request message on the Create Bearer Response message.
29	The S-GW processes each message independently. The S-GW forwards the Create Bearer Response to the P-GW. At this time, the P-GW can send downlink data on the dedicated bearer for the IMS traffic. Since Handover Indication is set to TRUE in the Modify Bearer Request, the S-GW sends Modify Bearer Request to the P-GW separately. Based on TS 23.401, the P-GW switches the downlink traffic to S5 upon receiving this message. However, subject to operator configuration, this switching occurs at Create Session Request above (C3).
30	The P-GW sends Modify Bearer Response (Cause) message to the S-GW.

Step	Description
C1. CCR-u	P-GW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
C1. CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW.
31	The S-GW sends Modify Bearer Response to the MME. The S1 S-GW F-TEID is the same as the S1-U S-GW F-TEID sent in Create Session Response from the S-GW to the MME. The S-GW can now start sending downlink packets to eNB and the switching of the data path from WiFi to LTE occurs after the Modify Bearer Response.
33a	SIP Re-registration RAT Change. The UE sends a SIP Re-Register to the P-CSCF to indicate that it detected a RAT change and assigned IP address remained unchanged.
34	P-GW to ePDG: Delete Bearer Request. The P-GW sends Delete Bearer Request to ePDG to disconnect the session.
35	ePDG to UE: IKEv2 Information Delete Request. The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
34	UE to ePDG: IKEv2 Informational Delete Response. UE responds with IKEv2 Information Delete Response () and initiates air interface resource release. This step is conditional and UE may not send this response.
37	ePDG to P-GW: Delete Bearer Response. The ePDG sends Delete Bearer Response to the P-GW.
38	ePDG to AAA: Session Termination Request. The ePDG sends STR to the 3GPP AAA.
39	AAA to HSS: Server Assignment Request. The AAA sends Server-Assignment-Request to de-register. HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
40	AAA to ePDG: Session Termination Answer. The AAA sends STA to the ePDG.

SAEGW GTP-based S2b Call Flows

This section provides call flows that illustrate the basic functionality of the GTP-based S2b interface support on the SAEGW.

Figure 48: Initial Attach Call Flow - SAEGW

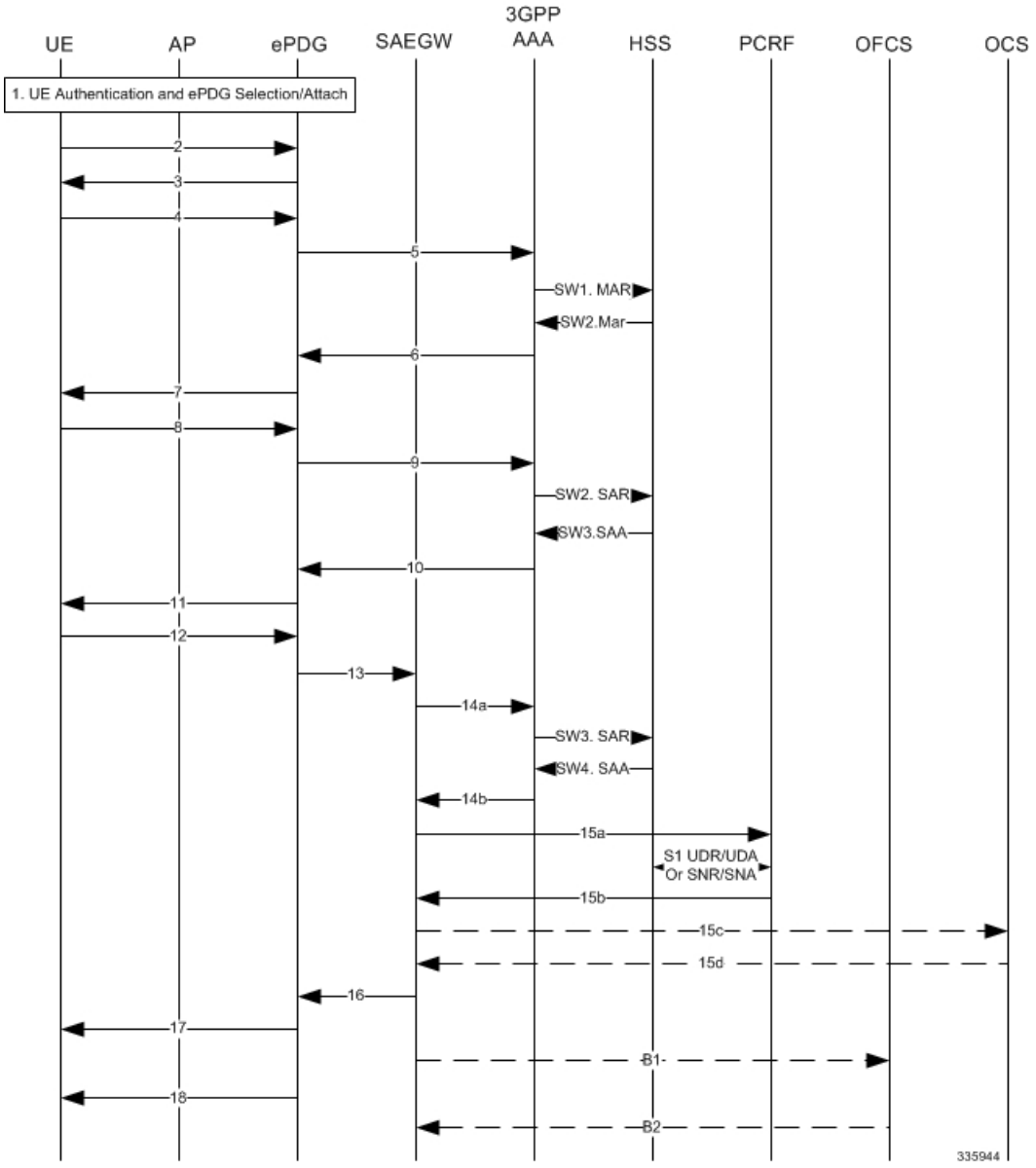


Table 61: Initial Attach - SAEGW

Step	Description
1	UE performs initial Access Point association and authentication if necessary.
2 - 11	The UE creates a connection with the ePDG.
12	UE sends IKE_AUTH request (AUTH). The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.

Step	Description
13	ePDG selects the P-GW of the SAEGW based on Node Selection options. The ePDG sends Create Session Request.
14a	The P-GW of the SAEGW sends AAR to the 3GPP AAA to authorize the PDN for the subscriber and to update P-GW address on the HSS for the APN.
SW3	The 3GPP AAA updates the HSS with the P-GW address of the SAEGW for the APN and retrieves Subscriber-APN profiles from the HSS.
SW4	The HSS sends Server-Assignment-Answer (Session-Id, Result-Code, Experimental-Result (Vendor-Id, Experimental-Result-Code))
14b	The 3GPP AAA sends AAA.
15a	The P-GW of the SAEGW sends an indication of IP-CAN establishment to the PCRF with CCR to indicate establishment of a new IP CAN session.
S1	The PCRF downloads (and caches) user profile (by sending an Sh: UDR (User-Identity, Service-Indication, Data-Reference) and receiving an Sh: UDA (Result-Code, User-Data)).
S2	The PCRF may subscribe to profile update notification.
15b	The PCRF Acknowledges IP CAN Session Establishment with a CCA message.
15c	If the Online AVP is set in the CCA from the PCRF (UC users / CF / RTR), the P-GW shall conditionally send a CCR-Initial.
15d	The OCS responds with a CCA to the P-GW.
16	The P-GW of the SAEGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
17	The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
18	ePDG sends Router Advertisement to ensure IP Stack is fully initialized. The P-GW of the SAEGW disables the Router Advertisement to the UE.
B1	If the Offline AVP is set in the CCA from the PCRF, then after IP-CAN session establishment procedure is complete, the P-GW of the SAEGW shall send a ACR-Start to the OFCS.
B2	The OFCS responds with an ACA to the P-GW of the SAEGW.

Figure 49: SAEGW: LTE to WiFi Handoff Call Flow

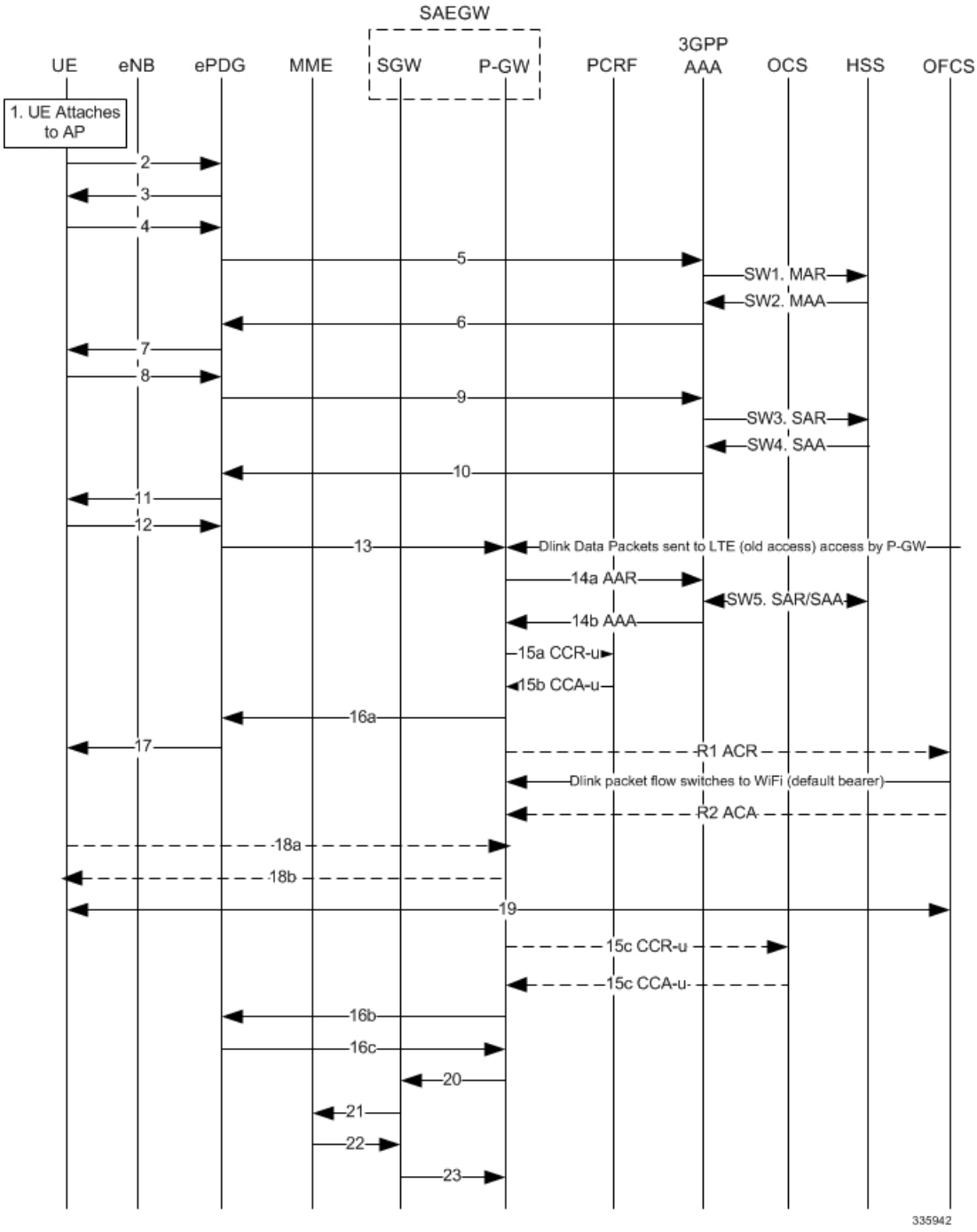


Table 62: SAEGW LTE to WiFi Handoff

Step	Description
1	Authentication and ePDG Selection. UE performs initial Access Point association and authentication if necessary.

Step	Description
2	UE to ePDG: IKEv2 SA_INIT. The UE sends IKE_SA_INIT Request.
3	ePDG to UE: INIT Response. The ePDG responds with an IKE_SA_INIT Response. The ePDG will start the IKEv2 setup timer when sending the IKE_SA_INIT Response.
4	UE sends Auth_Request.
5	ePDG to AAA: DER. The ePDG sends the DER message to the 3GPP AAA Server. Note the NAI shall not contain the AP MAC address sent in the username that comes in the IKE message
SW1. MAR	AAA to HSS: MAR. The 3GPP AAA Server fetches the user profile and authentication vectors from HSS over SWx. The 3GPP AAA server look up the IMSI of the authenticated user based on the received user identity and includes the EAP-AKA as requested authentication method in the request sent to the HSS. The AAA sends the Multimedia-Auth-Request MAR, Origin-Host, Origin-Realm, Destination-Realm, Destination-Host, User-Name, RAT-Type, SIP-Auth-Data-Item, SIP-Number-Auth-Items, and Routing-Information).
SW2. MAA	HSS to AAA: MAA. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The HSS sends the Multimedia-Auth-Answer MAA.
6	AAA to ePDG: DEA. The 3GPP AAA Server initiates the authentication challenge and responds with DEA.
7	ePDG to UE: IKE_AUTH. The ePDG responds with IKE_AUTH. The identity is the IP address of the ePDG; the AUTH payload authenticates the first IKE_SA_INIT response. If the UE requested certificates, the CERT is included. The EAP message received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.
8	UE to ePDG: IKE_AUTH Request. The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message IKE_AUTH Request (EAP).
9	ePDG to AAA: DER. The ePDG sends DER (Base AVPs, Auth Request Type, EAP Payload, Auth-Session-State, Service Selection) to the 3GPP AAA Server.
SW3. SAR	AAA to' HSS: SAR. The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the authenticated user. The AAA sends Server-Assignment-Request, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, User-Name (IMSI-NAI), Server-Assignment-Type (REGISTRATION)).
SW4 SAA	HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
10	AAA to ePDG: DEA. The 3GPP AAA Server sends an EAP success. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access before responding with DEA.
11	ePDG to UE: IKE_AUTH_Response. ePDG sends IKE_AUTH_Response (EAP).

Step	Description
12	UE to ePDG: IKE_AUTH_Request. UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG to P-GW of SAEGW: Create Session Request. The ePDG sends Create Session Request to the P-GW of SAEGW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.
14a	P-GW to 3GPP-AAA: AAR. The P-GW of SAEGW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
SW5. SAR/SAA	AAA to HSS: SAR. The 3GPP AAA updates the HSS with the P-GW address for the APN. The AAA sends Server-Assignment-Request.
14b AAA	3GPP AAA to P-GW: AAA. 3GPP AAA sends AAA to the P-GW of SAEGW.
15a CCR-u	P-GW of SAEGW to PCRF: CCR-U. The P-GW sends an indication of IP-CAN modification to the PCRF with CCR to indicate modification of the IP-CAN session.
15b CCA-u	PCRF to P-GW of SA: CCA. The PCRF Acknowledges of IP-CAN Session Modification with a CCA message. This message includes the Policy and Charging rules the P-GW will enforce and triggers for events that must be reported by the P-GW.
16a	P-GW of SAEGW to ePDG: Create Session Response. The P-GW of SAEGW identifies the S5 session and re-allocates the requested IP address session and responds back to the ePDG with a Create Session Response message. The P-CSCF private IE is included if the ePDG had included the P-CSCF request in message 13.
17	ePDG to UE: IKE_AUTH. The ePDG sends IKE_AUTH.
R1 ACR	P-GW to OFCS: ACR. The P-GW sends an ACR-Interim to the OFCS.
R2 ACA	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW of SAEGW.
18a	UE sends a Router Solicitation message.
18b	The P-GW of SAEGW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
19	The UE sends a SIP Re-Register once it successfully identifies it has changed access network to indicate the RAT change to the P-CSCF and assigned IP address is unchanged. UE will include 802.11 a/b/g/n in the PANI header. The SIP re-registration does not impact the way the P-CSCF does charging as charging is not used from the P-CSCF in IMS case.
15c CCR-u	P-GW of SAEGW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
15d CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW of SAEGW.

Step	Description
16b	P-GW of SAEGW to ePDG: Create Bearer Request. The IMS PDN has one or more dedicated bearers established prior to handoff and the P-GW of SAEGW also sends Create Bearer Request to the ePDG. Note that Charging ID is not sent on S2b. **Note** If there is a collision and already one transaction is pending and handoff request is received, then handoff is rejected with message "Rejecting S2b/LTE Handoff as only one pending transaction is supported".
16c	ePDG to P-GW: Create Bearer Response. The ePDG sends Create Bearer Response message
20	P-GW of SAEGW to S-GW of SAEGW: Delete Bearer Request. The P-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the S-GW. This message may be sent any time after message 13, the create session request.
21	S-GW of SAEGW to MME: Delete Bearer Request. The S-GW of SAEGW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the MME. The MME releases the E-UTRAN bearers if not already released. The MME does not send Notify Request to HSS at this point, as the cause IE is RAT change to Non-3GPP. MME does not page the UE either or initiate any NAS signaling and remove the locally stored PDN state and does S1 context release to the eNodeB if it has not already been triggered by the eNodeB. For last PDN MME removes all locally stored UE state.
22	MME to S-GW of SAEGW: Delete Bearer Response. The MME sends Delete Bearer Response to the S-GW of SAEGW.
23	S-GW of SAEGW to P-GW of SAEGW: Delete Bearer Response. The S-GW of SAEGW sends Delete Bearer Response to the P-GW of SAEGW.

Figure 50: SAEGW WiFi to LTE Handoff

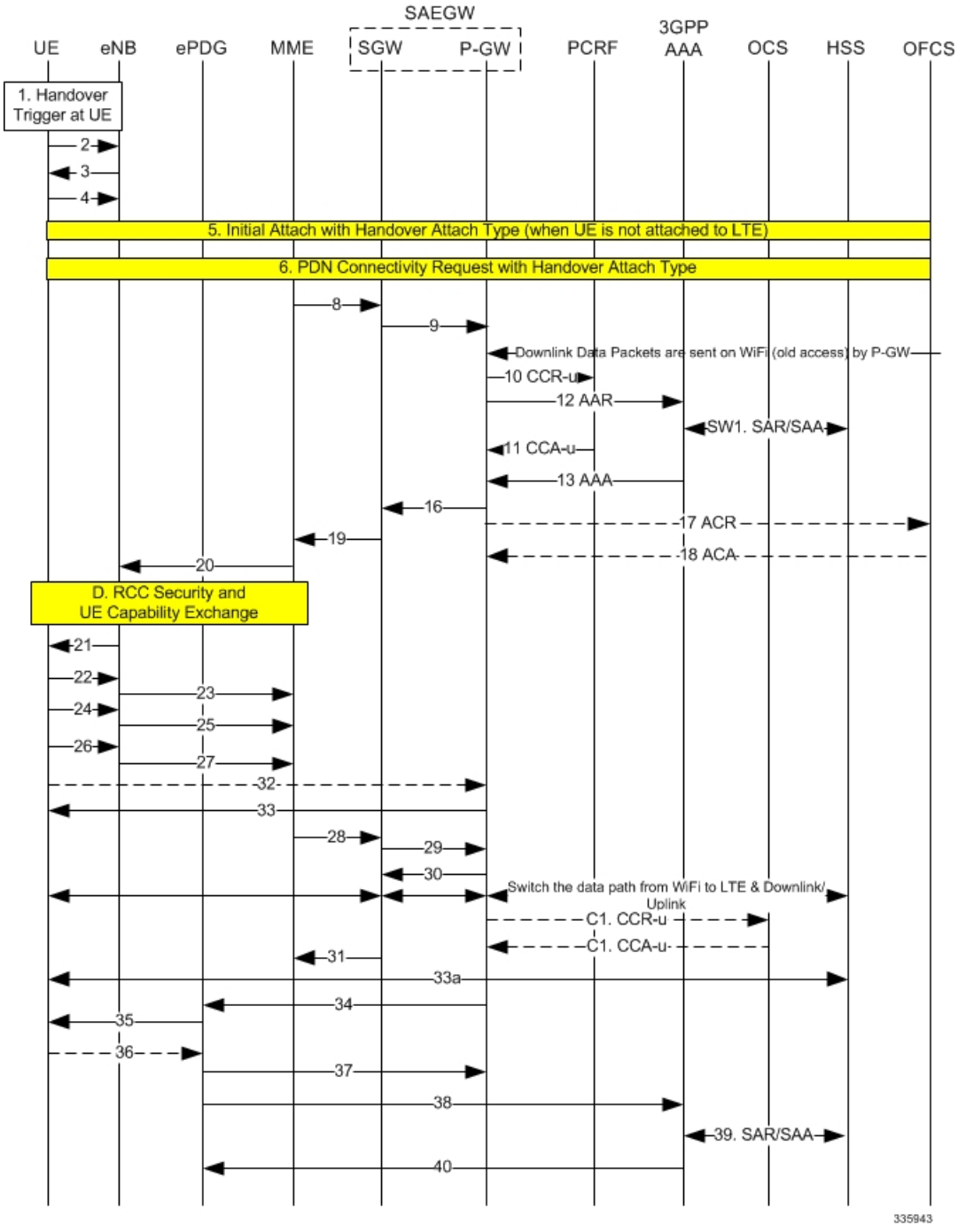


Table 63: SAEGW WiFi to LTE Handoff Procedure

Step	Description
1	A handover trigger occurs at the UE.

Step	Description
2, 3	RRC Connection Request/Connection Setup. The UE and eNodeB exchange signaling to set up an RRC connection (5.3.3, TS 36.331).
4	RRC Connection Setup Complete [Attach Request]. The UE sends RRC Connection Setup Complete message to the eNodeB.
5	Attach Request from eNB to MME. The UE indicates in the Attach Request to LTE that this is a Handover Attach. The eNodeB selects the MME. The eNodeB forwards the Attach Request message in an Initial UE Message to the MME.
6	MME selects the same P-GW of SAEGW based on HSS provided PGW FQDN and sends the Create Session request.
8	The MME selects the PGW/SGW of SAEGW. The MME sends a Create Session Request to the SGW of SAEGW with RAT as EUTRAN and the handoff indicator set to TRUE.
9	The SGW of SAEGW sends a Create Session Request to the PDN GW in order to establish the handoff (handoffindicator is set to true). RAT type is E-UTRAN.
10	P-GW of SAEGW to PCRF CCR IP-CAN Session Modification Procedure. The PCEF sends a CC-Request (CCR) Command with CC-Request-Type set to UPDATE_REQUEST. The APN-AMBR is included in the QoS-information AVP.
12	The P-GW of SAEGW sends AAR to 3GPP-AAA and includes the RAT type of the new connection.
SW1. SAR/SAA	The 3GPP-AAA sends SAR to HSS to retrieve the user profile, the HSS returns an SAA. The P-GW-FQDN is not updated as the 3GPP-AAA is not registered for this user.
11	PCRF to P-GW of SAEGW: CCA IP-CAN Session modification Procedure. On receiving the CCR the PCRF shall send a CC-Answer (CCA) Command to install the PCC rules and event triggers for all configured and established bearers. The QoS-Information AVP contains APN-AMBR-UL and APN-AMBR-DL.
13	The 3GPP-AAA responds with AAA.
16	P-GW of SAEGW to S-GW of SAEGW: Create Session Response + Create Bearer Request. The P-GW of SAEGW responds with a Create Session Response message to the S-GW of SAEGW. The P-GW of SAEGW provides IPv6 Prefix. Subject to operator configuration the P-GW of SAEGW can begin to forward downlink data and the S-GW of SAEGW buffers any downlink data packets.
17	P-GW of SAEGW to OFCS: ACR. After the P-GW of SAEGW sends the PBA, the P-GW of SAEGW sends an ACR-Interim to the OFCS.
18	OFCS to P-GW of SAEGW: ACA. The OFCS responds with an ACA to the P-GW.
19	Create Session Response. The S-GW of SAEGW sends Create Session Response to the MME.

Step	Description
20	Initial Context Setup Request/Attach Accept. The Attach Accept is sent as NAS PDU in the Initial Context Setup Request from MME to eNodeB. Attach Accept message contains new GUTI.
D	These procedures occur independently of the location procedures. These procedures only apply to initial attach scenarios.
21	RRC Connection Re-configuration. The eNodeB sends the RRC Connection Reconfiguration message including the EPS Radio Bearer Identity to the UE, and the Attach Accept message to the UE. The APN is provided to the UE to notify it of the APN for which the activated default bearer is associated.
22	RRC Connection Re-configuration Complete. The UE sends the RRC Connection Reconfiguration Complete message to the eNodeB.
23	Initial Context Setup Response. The eNodeB sends Initial Context Setup Response to the MME.
24	Uplink Information Transfer. The UE sends an Uplink Information Transfer message.
25	Attach Complete. The eNodeB forwards the received Attach Complete message in an Uplink NAS Transport as part of NAS PDU.
26	Uplink Information Transfer. When the UE has received Activate dedicated EPS Bearer Context Request message in the Attach Accept message, the UE sends Activate Dedicated EPS Bearer Context Accept message in a Uplink Information Transfer message.
27	UL NAS Transport. The eNB passes the Activate Dedicated EPS Bearer Context Accept message received in Step 14.b, to the MME in a UL NAS Transport message. At this time, the uplink data can be sent on the dedicated bearer.
32	Router Solicitation. This step may happen any time after step 26. For IPv6 PDN, the UE may send a Router Solicitation to the P-GW.
33	Router Advertisement. This step may happen any time after step 29 if the UE requested IPv4v6 or IPv6 PDN type. On receipt of the RS or prior the P-GW of SAEGW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
28	Modify Bearer Request / Create Bearer Response. On receiving both Initial Context Setup Response and Attach Complete, the MME sends a Modify Bearer Request message to the S-GW of SAEGW. The MME piggybacks the Modify Bearer Request message on the Create Bearer Response message.

Step	Description
29	The S-GW of SAEGW processes each message independently. The S-GW of SAEGW forwards the Create Bearer Response to the P-GW. At this time, the P-GW of SAEGW can send downlink data on the dedicated bearer for the IMS traffic. Since Handover Indication is set to TRUE in the Modify Bearer Request, the S-GW of SAEGW sends Modify Bearer Request to the P-GW of SAEGW separately. Based on TS 23.401, the P-GW of SAEGW switches the downlink traffic to S5 upon receiving this message. However, subject to operator configuration, this switching occurs at Create Session Request above (C3).
30	The P-GW of SAEGW sends Modify Bearer Response (Cause) message to the S-GW.
C1. CCR-u	P-GW of SAEGW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW of SAEGW conditionally sends a CCR-Update to the OCS to request online charging quota for the PDN session.
C1. CCA-u	OCS to P-GW of SAEGW: CCA. The OCS responds with a CCA to the P-GW of SAEGW.
31	The S-GW of SAEGW sends Modify Bearer Response to the MME. The S1 S-GW F-TEID is the same as the S1-U S-GW F-TEID sent in Create Session Response from the S-GW of SAEGW to the MME. The S-GW of SAEGW can now start sending downlink packets to eNB and the switching of the data path from WiFi to LTE occurs after the Modify Bearer Response.
33a	SIP Re-registration RAT Change. The UE sends a SIP Re-Register to the P-CSCF to indicate that it detected a RAT change and assigned IP address remained unchanged.
34	P-GW of SAEGW to ePDG: Delete Bearer Request. The P-GW of SAEGW sends Delete Bearer Request to ePDG to disconnect the session.
35	ePDG to UE: IKEv2 Information Delete Request. The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
34	UE to ePDG: IKEv2 Informational Delete Response. UE responds with IKEv2 Information Delete Response () and initiates air interface resource release. This step is conditional and UE may not send this response.
37	ePDG to P-GW of SAEGW: Delete Bearer Response. The ePDG sends Delete Bearer Response to the P-GW.
38	ePDG to AAA: Session Termination Request. The ePDG sends STR to the 3GPP AAA.
39	AAA to HSS: Server Assignment Request. The AAA sends Server-Assignment-Request to de-register. HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
40	AAA to ePDG: Session Termination Answer. The AAA sends STA to the ePDG.

Standards Compliance

This section lists the industry-standards and references that were used in developing the GTP-based S2b interface implementation on the P-GW and SAEGW:

The following standards and references were used in developing the GTP-based S2b interface support feature.

- 3GPP TS 23.003-a.1.0 Numbering, addressing and identification
- 3GPP TS 23.234-a.0.0, 3GPP system to Wireless Local Area Network (WLAN) Interworking
- 3GPP TS 23.261-a.1.0, IP flow mobility and seamless Wireless Local Area Network (WLAN) Offload
- 3GPP TS 23.401: GPRS Enhancement for E-UTRAN Access
- 3GPP TS 23.402-a.4.0 Architecture Enhancements for non-3GPP Accesses
- 3GPP TS 24.302-a.4.0: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks.
- 3GPP TS 24.312-a.3.0 Access Network Discovery and Selection Function (ANDSF) Management Object (MO)
- 3GPP TS 29.273-a.3.0 Evolved Packet System (EPS); 3GPP EPS AAA interfaces
- 3GPP TS 29.274- Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 33.234-a.0.0 Wireless Local Area Network (WLAN) interworking security
- 3GPP TS 33.402-a.0.0 Security aspects of non-3GPP accesses
- IETF RFC 3588: Diameter Base Protocol.
- IETF RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPSec
- IETF RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- IETF RFC 3748: Extensible Authentication Protocol (EAP)
- IETF RFC 3948: UDP Encapsulation of IPSec ESP Packets.
- IETF RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- IETF RFC 4303: IP Encapsulating Security Payload (ESP).
- IETF RFC 4306: Internet Key Exchange Protocol Version 2
- IETF RFC 4739: Multiple Authentication Exchange in IKEv2 protocol
- IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)

How the S2a Architecture Works

This section provides information that describes the S2a interface architecture on the standalone P-GW and SAEGW.

Standalone P-GW and SAEGW Architecture for S2a Interface Support

Diagrams for the S2a interface architecture for the standalone P-GW and SAEGW appear below.

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD. Specifically, the S2a interface supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the standalone P-GW or P-GW of the SAEGW. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

Figure 51: S2a Interface Architecture for the Standalone P-GW

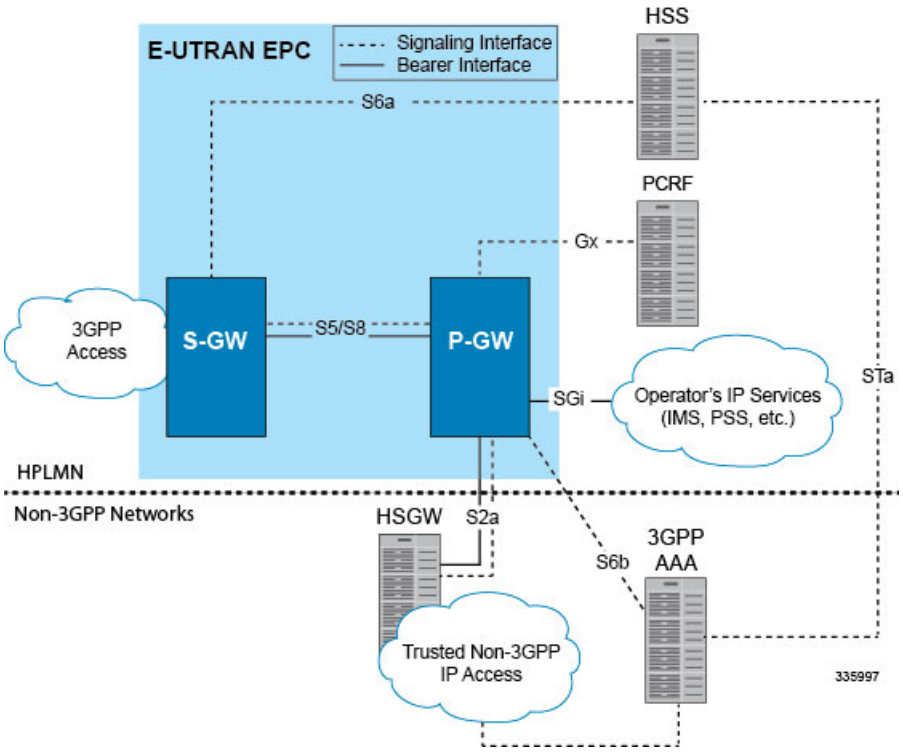
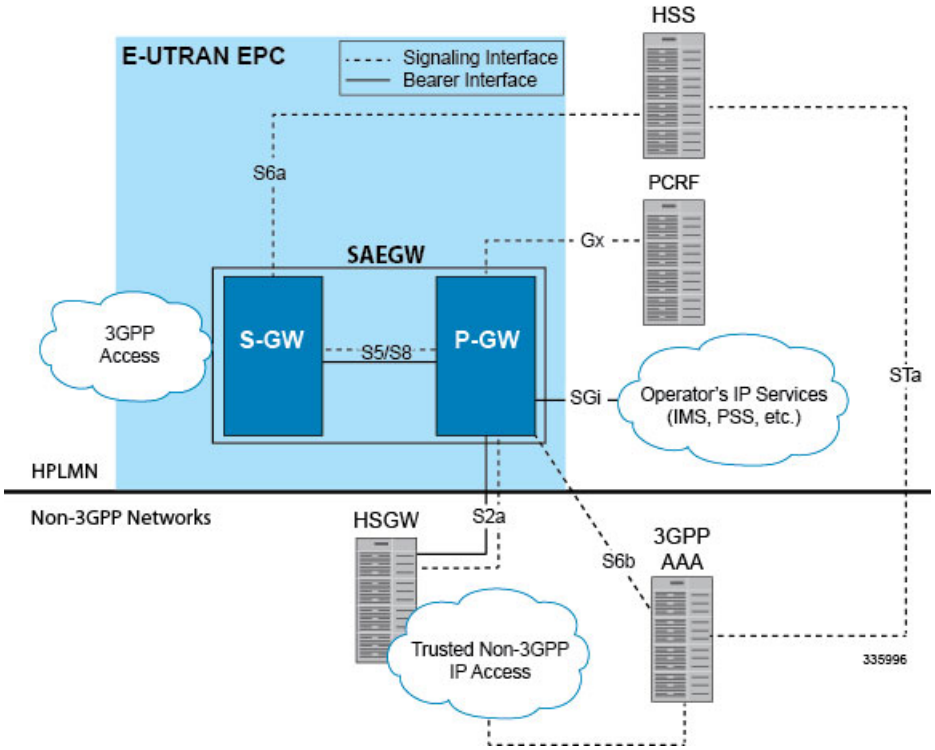


Figure 52: S2a Interface Architecture for the SAEGW



Limitations on S2a Interface Support on the P-GW and SAEGW

Note the following limitations of the GTP-based S2a interface implementation on the P-GW and SAEGW:

- Access Type technologies supported are WiFi and LTE.
- Interfaces supported include:
  - S6b
  - Gy
  - Rf
  - Gx
  - GTPv2

Standalone P-GW S2a Call Flows

The following call flow diagrams describe the basic functionality of the S2a interface when deployed in a standalone P-GW architecture.

Figure 53: S2a Initial Attach on Standalone P-GW

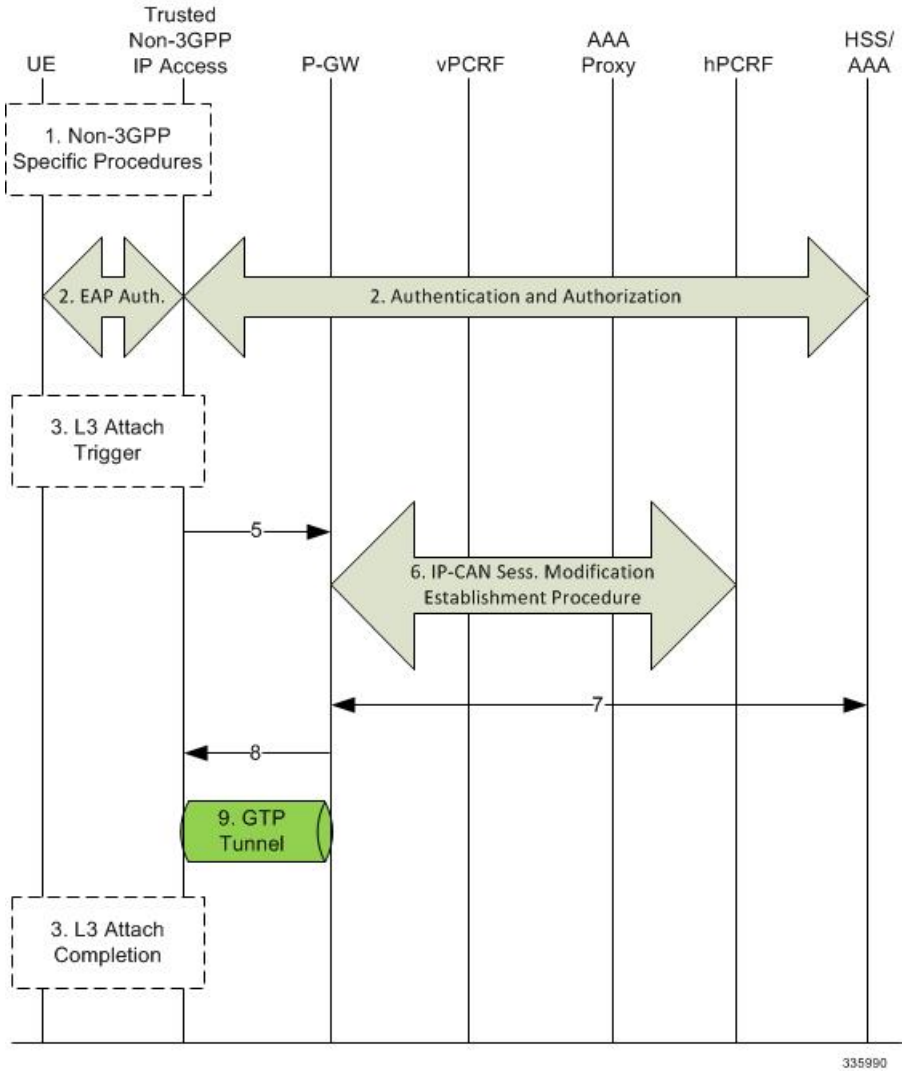


Table 64: S2a Initial Attach on Standalone P-GW

Step	Description
1	
2	
3	
4	

Step	Description
5	The Trusted non-3GPP IP Access sends a Create Session Request message to the P-GW. The RAT type indicates the non-3GPP IP access technology type. The PDN type shall be set based on the requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach.
6	The P-GW initiates the IP-CAN Session Establishment Procedure with the PCRF.
7	The selected P-GW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS.
8	The P-GW returns a Create Session Response message to the TWAN, including the IP address(es) allocated for the UE.
9	The GTP tunnel is set up between the TWAN and the P-GW.
10	Initial Attach is complete.

Figure 54: S2a LTE-to-WiFi Handover on Standalone P-GW

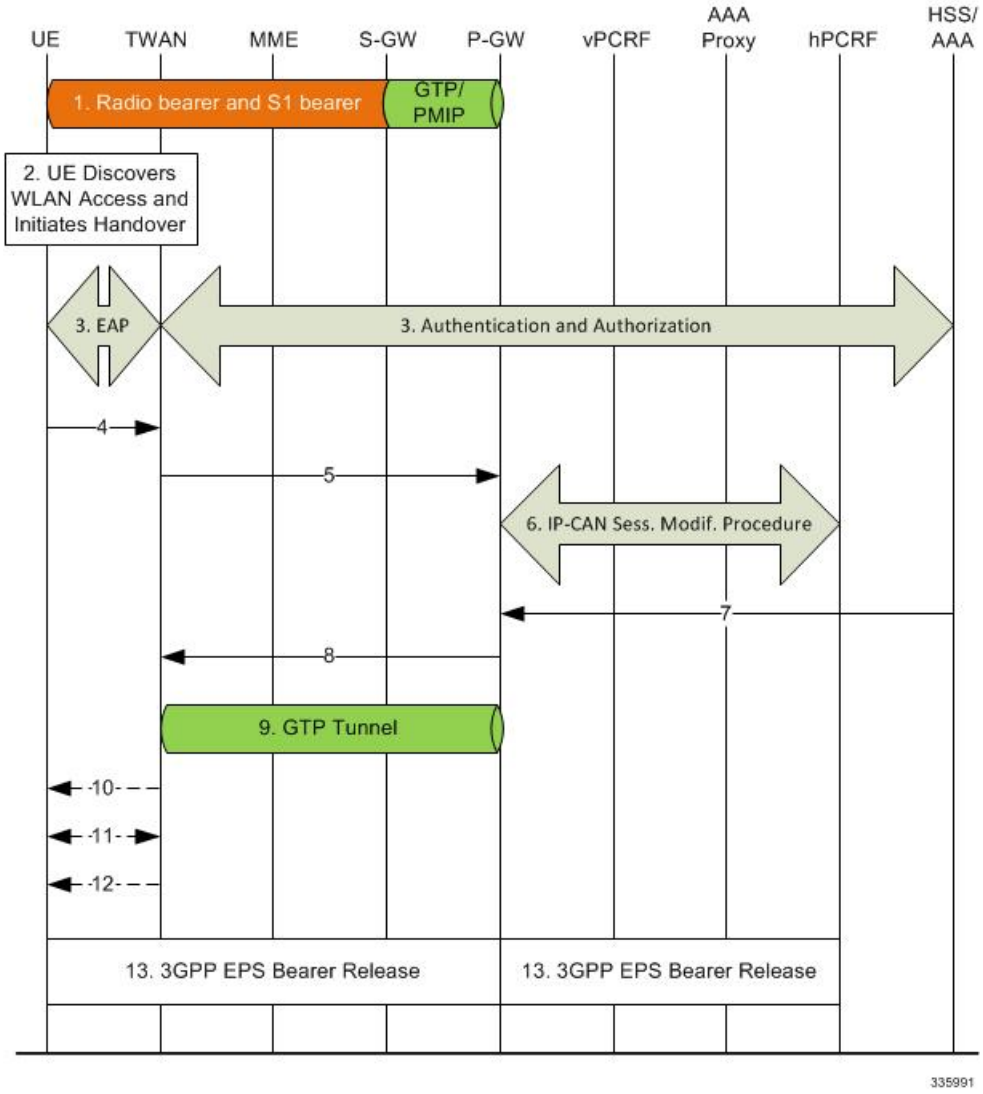


Table 65: S2a WiFi-to-LTE Handover on Standalone P-GW

Step	Description
1	
2 - 4	The UE discovers WLAN access and initiates a handover. The TWAN takes authorization from the AAA server.

Step	Description
5	The TWAN sends a Create Session Request (IMSI, APN, RAT type) message to the the P-GW. The RAT type WLAN indicates the non-3GPP IP access technology type. The TWAN does not set the 'Handover Indication' bit. Instead, based on the IMSI, APN and RAT type the P-GW determines that it is potential handover from the TWAN. The P-GW re-allocates the same IPv4 address and/or IPv6 address that was assigned to the UE while it was connected to 3GPP IP access.
6	The P-GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF with the RAT type as WLAN.
7	The P-GW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN and obtains authorization information from the 3GPP AAA Server. The 3GPP AAA Server decides whether or not to update the P-GW identification according to the UE capability, which has been provided at the authentication phase.
8	The P-GW responds with a Create Session Response to the TWAN. The Create Session Response contains the IPv4 address and/or the IPv6 address assigned to the UE while it was connected to the 3GPP IP access.
9	The GTP tunnel is setup between TWAN and the P-GW.
10	
11	
12	
13	The P-GW initiates the P-GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1 for GTP-S5/S8.

Figure 55: S2a WiFi-to-LTE Handover on Standalone P-GW

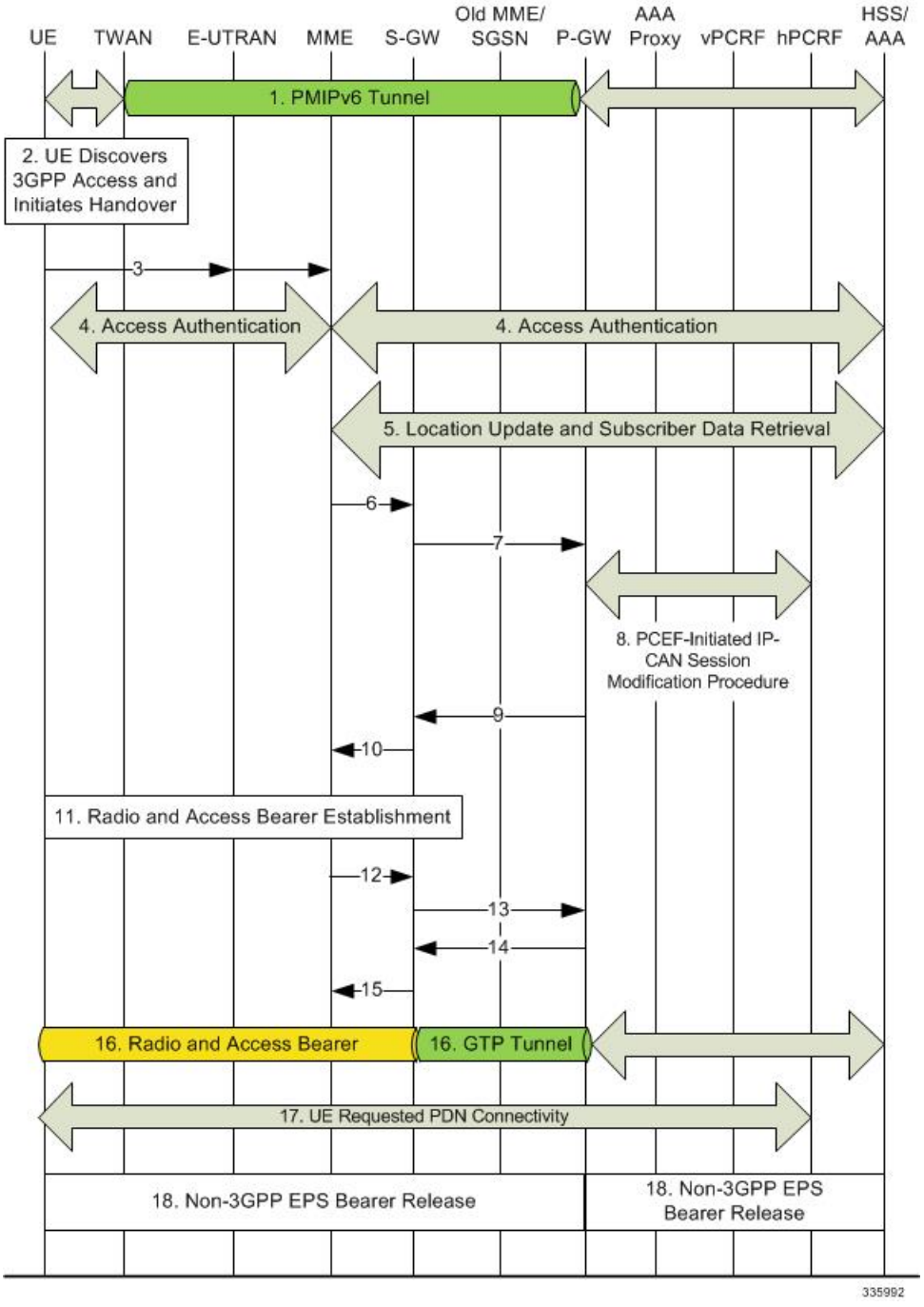


Table 66: S2a WiFi-to-LTE Handover on Standalone P-GW

Step	Description
1	

Step	Description
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

SAEGW S2a Call Flows

The call flow diagrams in this section describe the basic functionality of S2a interface support on the SAEGW, including:

- Initial Attach
- LTE-to-WiFi Handover
- WiFi-to-LTE Handover

Figure 56: S2a Initial Attach on the SAEGW

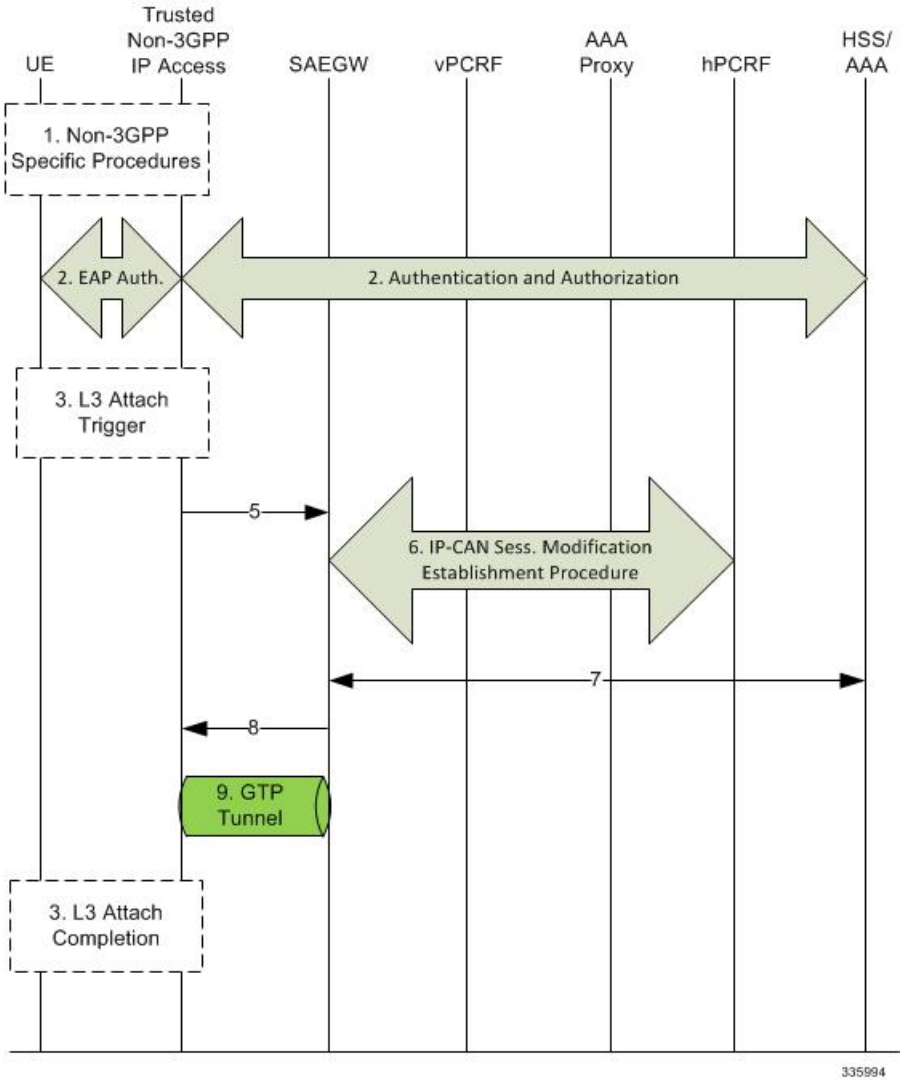


Table 67: S2a Initial Attach on the SAEGW

Step	Description
1	
2	
3	
4	

Step	Description
5	The Trusted non-3GPP IP Access sends a Create Session Request (CSReq) message to the P-GW of the SAEGW. The RAT type indicates the non-3GPP IP access technology type. The PDN type shall be set based on the requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach. The P-GW of the SAEGW creates a new entry in its bearer context table and generates a Charging Id. The new entry allows the P-GW of the SAEGW to route user plane PDUs between the Trusted non-3GPP IP Access Network and the packet data network and to start the charging process.
6	The P-GW initiates the IP-CAN Session Establishment Procedure with the PCRF.
7	The selected P-GW of the SAEGW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the P-GW is located. This information is registered in the HSS.
8	The P-GW returns a Create Session Response (CSResp) message to the TWAN, including the IP address(es) allocated for the UE.
9	The GTP tunnel is set up between the TWAN and the P-GW. Initial Attach is completed.

Figure 57: S2a LTE-to-WiFi Handover on the SAEGW

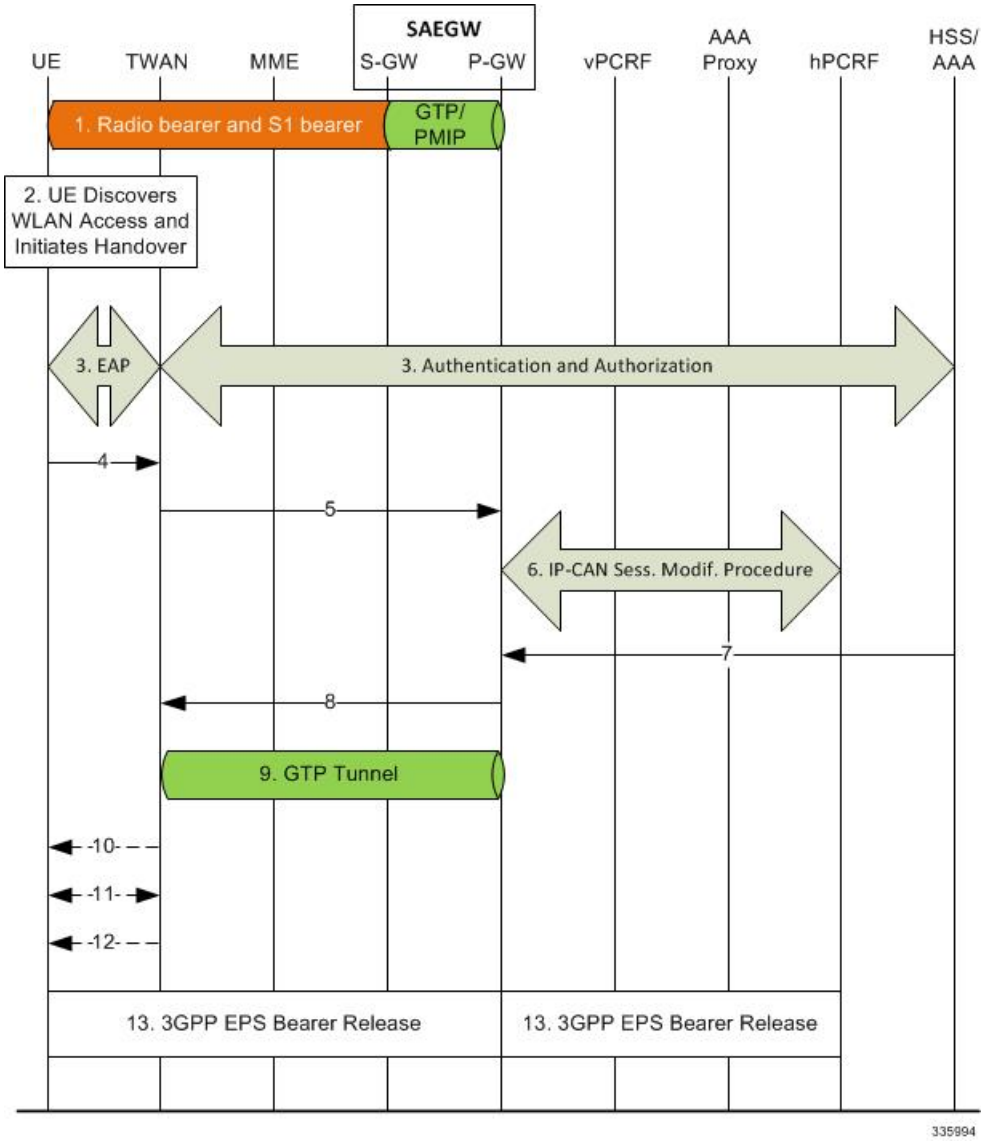


Table 68: S2a LTE-to-WiFi Handover on the SAEGW

Step	Description
1	
2 - 4	In Steps 2-4, the UE discovers WLAN access and initiates a handover. The TWAN takes authorization from the AAA server.

Step	Description
5	The TWAN sends a Create Session Request (including IMSI, APN, RAT type) message to the P-GW of the SAEGW The RAT type WLAN indicates the non-3GPP IP access technology type. The TWAN does not set the 'Handover Indication' bit. Instead, based on the IMSI, APN and RAT type the P-GW of the SAEGW determines that it is a potential handover from the TWAN. The P-GW of the SAEGW re-allocates the same IPv4 address and/or IPv6 address assigned to the UE while it was connected to 3GPP IP access.
6	The P-GW of the SAEGW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF with RAT type as WLAN.
7	The P-GW of the SAEGW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN and obtains authorization information from the 3GPP AAA Server. The 3GPP AAA Server decides whether or not to update PDN GW identification according to the UE capability, which was provided at the authentication phase.
8	The P-GW of the SAEGW responds with a Create Session Response to the TWAN. The Create Session Response contains the IPv4 address and/or the IPv6 address assigned to the UE while it was connected to the 3GPP IP access.
9	A GTP tunnel is setup between TWAN and the P-GW of the SAEGW.
10	
11	
12	
13	The P-GW of the SAEGW begins the P-GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1 for GTP-S5/S8 interfaces.

Figure 58: S2a WiFi-to-LTE Handover on the SAEGW

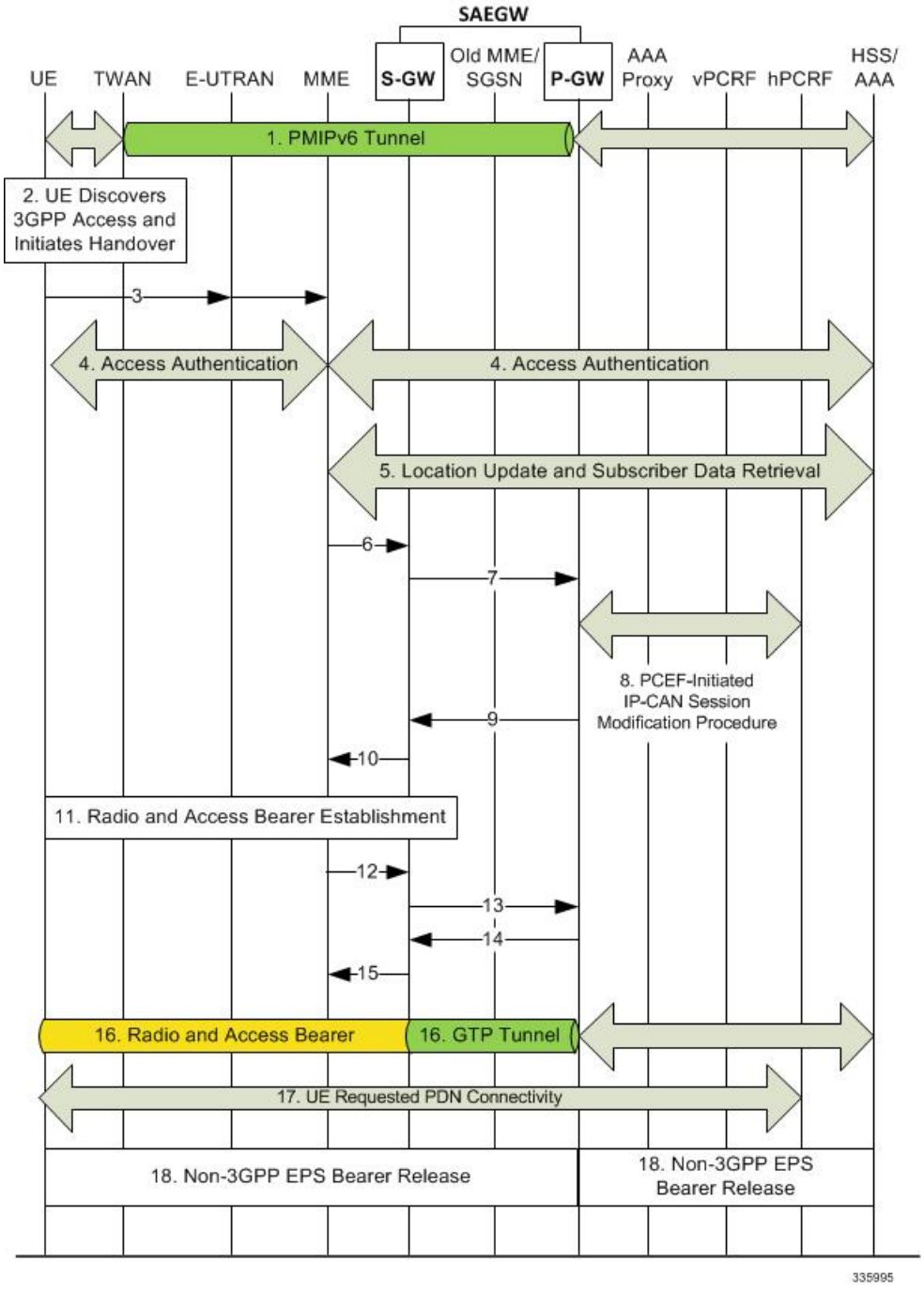


Table 69: S2a WiFi-to-LTE Handover on the SAEGW

Step	Description
1	

Step	Description
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

Configuring the GTP-based S2b Interface on the P-GW and SAEGW

This section describes how to configure the GTP-based S2b interface support feature.

Configuring GTP-based S2b Interface Support

Use the following example to configure GTP-based S2b interface support on the P-GW and SAEGW.



Important GTP-based S2a/S2b interface support on the P-GW and SAEGW is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress s2b
         end
```

Disable S2b interface support by entering the following commands:

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress
         end
```

Verifying the Configuration

This section describes how to verify the GTP-based S2a/S2b interface configuration on the P-GW and SAEGW.

Use the **show configuration** command from Exec Mode to verify that the configuration is active. Look for the eGTP service configuration section in the output:

```
egtp-service EGTP
   interface-type interface-pgw-ingress s2a s2b
```

Once the S2b license is installed and active, run a WiFi Initial Attach Call to check that a successful call is setup. From Exec Mode, use the **show subscribers all** command to verify that the call was successful.

Monitoring the GTP-based S2b Interface Feature

This section provides commands that operators can use to monitor the GTP-based S2b interface feature on the P-GW and SAEGW.

GTP-based S2b Interface Show Commands

This section provides information regarding show commands and/or their outputs for GTP-based S2b interface support.

show pgw-service statistics all

For S2b interface support on the standalone P-GW: This command provides statistics on the number of attempts, failures, and successes for the following S2b interface functions:

- S2bGTP-to-LTE handovers
- LTE-to-S2bGTP handovers

show subscribers epdg-address

This command provides information on the S2b P-GW subscribers connected to the ePDG over the S2b interface.

show subscribers saegw-only epdg-address

This command shows information related to subscribers of the P-GW of the SAEGW connected to a specific ePDG over the S2b interface.

show subscribers saegw-only interface-type S2bGTP

This command shows information related to GTP P-GW subscribers of the SAEGW connected via the S2b interface.

show subscribers summary pgw-address

This command provides information on the number of Active and Dormant GTP S2b IPv4 and IPv6 subscribers.

show subscribers pgw-only full all

For S2b interface support on the standalone P-GW: Use this command to view S2b call related information for P-GW subscribers. The output will provide the following S2b specific information:

- Interface Type (S2b PGW GTP-C interface)
- MAC Address
- ePDG c-teid (ePDG control tunnel endpoint identifier)
- ePDG u-teid (ePDG bearer tunnel endpoint identifier)
- ePDG c-addr (ePDG control IP address)
- ePDG u-addr (ePDG bearer IP address)

show subscribers pgw-only epdg-address

For S2b interface support on the standalone P-GW: Use this command to view all S2b information for all the subscribers' sessions that exist on the P-GW for a specific ePDG. The ePDG is specified by the epdg-address (in IPv4 or IPv6 address format).

show subscribers summary epdg-address

For S2b interface support on the standalone P-GW: Use this command to view statistics for all the subscribers' sessions that exists on the P-GW that belong to the S2b interface on a specific ePDG. The ePDG is specified by the epdg-address.

show subscribers summary interface-type S2bGTP

For S2b interface support on the standalone P-GW: View the number of active and dormant subscriber sessions on the P-GW that belong to the S2b interface.

show subscribers saegw-only full all

For S2b interface support on the SAEGW: This command provides S2b call-related information for P-GW subscribers, including:

- Access Tech
- Interface Type
- Access Point MAC Address
- sgw c-teid
- ePDG c-teid
- sgw c-addr
- ePDG c-addr
- sgw u-teid
- ePDG u-teid
- sgw u-addr
- ePDG u-addr

show saegw-service statistics all function pgw

For S2b interface support on the SAEGW: This command provides statistics related to successes, failures and attempts for various S2bGTP handovers for all P-GW SAEGW services, including:

- S2bGTP-to-LTE handover
  - Attempted
  - Succeeded
  - Failed
- LTE-to-S2bGTP handover
  - Attempted
  - Succeeded
  - Failed

Monitoring the GTP-based S2a Interface Feature

This section provides information on how to monitor the GTP-based S2a interface feature.

GTP-based S2a Interface Show Commands

This section provides information regarding show commands and/or their outputs for GTP-based S2a interface support.

show pgw-service statistics all

The output of this command has been enhanced to provide statistics on S2aGTP-to-LTE and LTE-to-S2aGTP handovers. It records the total number of handover attempts, and the number of attempts that succeeded and failed.

show saegw-service statistics all

The output of this command provides information related to subscribers, bearers, and PDNs on the S2a interface.

show saegw-service statistics all function-pgw

The output of this command provides subscriber, PDN and handover statistics for the P-GW function of the SAEGW on the S2a interface.

show session-subsystem facility sessmgr service-type pgw-ingress

The output of this command has been enhanced to provide S2a interface session information to troubleshoot subscriber session problems and for general monitoring for orphaned sessions. If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

show subscribers pgw-only full all

The output of this command has been enhanced to show S2a call-related information, including access technology, TWAN, and TEID information.

show subscribers saegw-only full all

The output of this command contains subscriber information related to the S2a interface, including subscriber ID information, TEID and address information, and input/output packets recorded and dropped.

show subscribers saegw-only interface-type S2aGTP

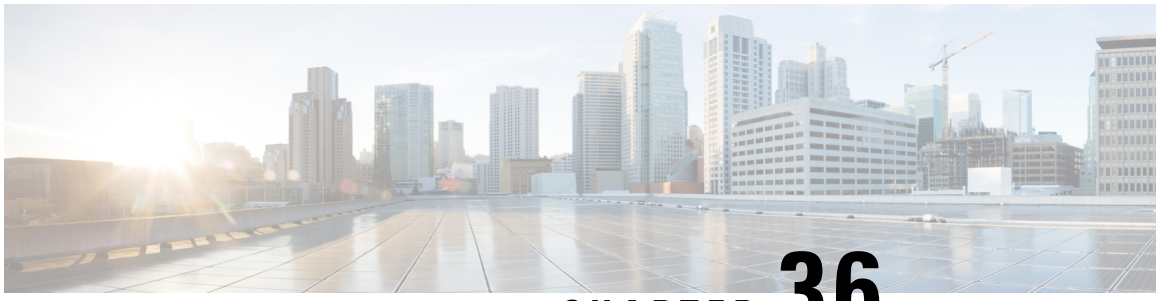
The **S2aGTP** keyword has been added to this command to enable operators to view detailed information for S2a subscriber sessions, including call code, CALLID, IMSI/IMEI, APN and Time-Idle.

show subscribers summary interface-type S2aGTP

The output provides interface type details on subscribers connected via the S2a interface. The output provides interface type details on subscribers connected via the S2a interface. Information is given for both IPv4, IPv6, and IPv4v6 interfaces.

show subscribers summary pgw-address

The output of this command contains S2a subscriber information for the specified P-GW. Interface information is included for IPv4, IPv6 and IPv4v6 interfaces.



CHAPTER 36

GTPv2 Cause Code Change for S6b Interface

- Feature Summary and Revision History, on page 607
- Feature Description, on page 608
- Configuring S6b Retry Code, on page 608
- Monitoring and Troubleshooting, on page 608

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

When the S6b service is unreachable or connections are unstable while sending the Create Session Response, the S6b interface modifies the existing GTPv2 cause code 92/0x5C (user authentication failed) to cause code 73/0x49 (no resources available).

Configuring S6b Retry Code

Use the following configuration to apply S6b retry code from Diameter:

```
configure
   context context_name
      pgw-service service_name
         egtp { reject-cause { no-resource [ s6b-link-failure ] {
s6b-retry-code } }
         [ no | default ] egtp reject-cause no-resource
         end
```

NOTES:

- **reject-cause**: Configures options for handling response with reject-cause.
- **no-resource**: Configures handling for Create Session Response with cause code no-resource.
- **s6b-link-failure**: Responds with no-resource for S6b server unreachability during authentication.
- **s6b-retry-code**: Responds with no-resource for S6b diameter result-codes—3002, 3004, 3005 and 5198.

Monitoring and Troubleshooting

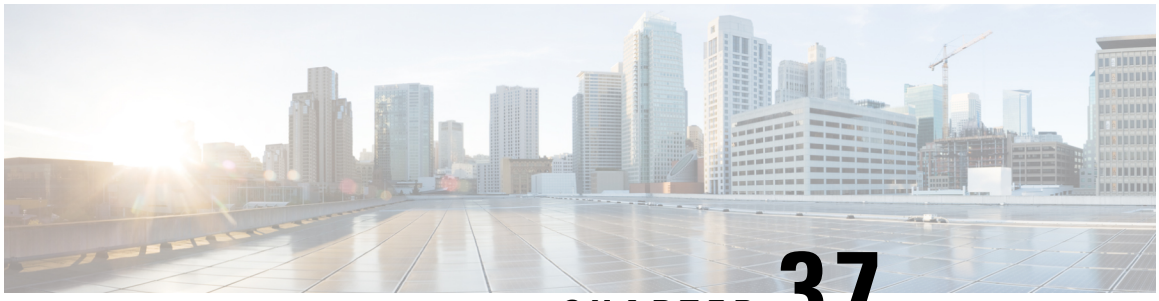
This section provides information regarding show commands and/or their outputs.

Show Command and Output

show pgw-service name <pgw_service_name>

The output of this command is enhanced to include the following fields. These fields indicate whether EGTP-C cause code mapping for S6b Link Failure and S6b Retry Code is enabled or disabled.

- EGTP-C Cause Code Mapping (S6b Link Failure) : Enabled or Disabled
- EGTP-C Cause Code Mapping (S6b Retry Code) : Enabled or Disabled



CHAPTER 37

3GPP R12 GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW

This chapter describes the 3GPP Release 12 GTP-C Load and Overload Control feature on the P-GW, SAEGW, and S-GW.

- Feature Description, on page 609
- How It Works, on page 610
- Creating and Configuring a 3GPP R12 GTP-C Load Control Profile, on page 611
- Creating and Configuring a 3GPP R12 GTP-C Overload Control Profile, on page 616
- Monitoring and Troubleshooting the 3GPP R12 GTP-C Load and Overload Control Feature, on page 624

Feature Description

This section describes the 3GPP R12 GTP-C Load and Overload Control feature.

Important Use of the 3GPP R12 Load and Overload Control feature requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

The 3GPP R12 GTP-C Load and Overload Control feature is a licensed, optional feature which allows a GTP control plane node to send its load information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of overload control information in order to mitigate overload situations for the overloaded node through actions taken by the peer node(s). This feature is supported over the S4, S11, S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes, may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the overload control information provides guidance to the receiving node to decide upon the correct actions, which leads to mitigation towards the sender of the information.

To summarize, load control and overload control can be described in this manner:

- **Load Control**: Load control enables a GTP-C entity (for example, an P-GW/SAEGW/S-GW) to send its load information to a GTP-C peer (for example, an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- **Overload Control**: Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Load and Overload Factor Calculation Enhancement

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

A new CLI command, **gtpc-system-param-poll interval**, is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.

Relationships to Other Features

Note the following before configuring the GTPP R12 GTP-C Load and Overload Control feature:

- One of the following services must be configured on the node before GTP-C Load and Overload Control can be configured.
  - P-GW
  - SAEGW
  - S-GW
- Once configured, the GTP-C Load and Overload Control profiles must be associated with a P-GW, SAEGW, or S-GW service to function properly in the network.

How It Works

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization, and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load/overload control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, [(number of active sessions per service / max session allowed for the service license) * 100].

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

Creating and Configuring a 3GPP R12 GTP-C Load Control Profile

This section describes how to create and configure a 3GPP R12 GTP-C load control profile.

Configuration Overview

Creating and configuring a 3GPP R12 GTP-C load control profile consists of the following procedures:

Procedure

Step 1 Create a load control profile. Refer to Creating the GTPP R12 Load Control Profile, on page 611.

Step 2 Configure the load control weightage settings. Refer to Configuring the 3GPP R12 Load Control Profile Weightage Settings, on page 612.

Step 3 Configure the load control inclusion frequency. Refer to Configuring the 3GPP R12 Load Control Profile Inclusion Frequency, on page 612.

Step 4 P-GW Only. Configure the load control threshold. Refer to Configuring the 3GPP R12 Load Control Threshold, on page 613.

Step 5 Configure load control information handling. Refer to Configuring 3GPP R12 Load Control Information Handling, on page 613.

Step 6 Configure load control information publishing. Refer to Configuring 3GPP R12 Load Control Information Publishing, on page 613.

Step 7 Configure the 3GPP R12 GTP-C Polling Parameter Interval. Refer to Configuring the 3GPP R12 GTP-C Polling Parameter Interval, on page 614

Step 8 Associate the load control profile with a P-GW, SAEGW, or S-GW service. Refer to Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service., on page 615.

Step 9 Verify the configuration settings. Refer to Verifying the 3GPP R12 Load Control Configuration , on page 615.

Step 10 Save the configuration. Refer to Saving the Configuration, on page 616.

Creating the GTPP R12 Load Control Profile

Use the following example to create a load control profile on the P-GW/SAEGW/S-GW:

```
config
   gtpc-load-control-profile profile_name
   end
```

Notes:

- The profile name must be an alphanumeric string from 1 to 64 characters in length.
- Once you have created the load control profile, you will enter *GTP-C Load Control Profile Configuration Mode*.

Configuring the 3GPP R12 Load Control Profile Weightage Settings

This section describes how to set weightage percentages for system CPU, memory, and license session utilization as part of a GTP-C load control profile configuration. These settings constitute the basic load control profile for this network element. These parameters allow the P-GW/S-GW/SAEGW to send its load information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedures for the P-GW and S-GW. Load information reflects the operating status of the resources of the originating GTP control plane node.

Use the following example to configure the load control profile weightage settings on the P-GW/SAEGW/S-GW:

```
config
   gtpc-load-control-profile profile_name
   weightage system-cpu-utilization percentage system-memory-utilization
 percentage license-session-utilization percentage
   end
```

Notes:

- **system-cpu-utilization** *percentage*: Configures system CPU utilization weightage as a percentage of 100.

  percentage must be an integer from 0 to 100. The default is 40.

- **system-memory-utilization** *percentage*: Configures system memory utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.

- **license-session-utilization** *percentage*: Configures license session utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.



Important All parameters must be specified. The total of all three parameter settings should equal, but not exceed, 100.

Configuring the 3GPP R12 Load Control Profile Inclusion Frequency

This section describes how to set the parameters that determine the inclusion frequency of the Load Control Information Element (LCI) for a GTP-C Load Control Profile configuration. The LCI is a 3GPP-specific Information Element that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send this information to the node's peers.

Use the following example to configure the load control profile inclusion frequency on the P-GW/SAEGW/S-GW.

```
config
   gtpc-load-control-profile profile_name
      inclusion-frequency { advertisement-interval interval_in_seconds |
```

```
change-factor change_factor  }
      end
```

Notes:

- **inclusion frequency**: Configures parameters to determine the inclusion frequency of the LCI.
- **advertisement-interval** *interval_in_seconds*: Configures advertisement-interval for the LCI in seconds. This specifies how often load control information should be sent to the peers. If configured to 0, the node will send load control information in each and every outgoing message to the peers. *interval_in_seconds* must be an integer from 0 to 3600. The default is 300.
- **change-factor** *change_factor*: Configures the change factor for the load control profile. If the load control change factor changes by the configured factor, whether it is an increase or decrease in load, the load control information is sent to the peers. This information is only sent to the peers when the load factor changes by the factor configured. *change_factor* must be an integer from 1 to 20. The default is 5.

Configuring the 3GPP R12 Load Control Threshold

This section describes how to configure the minimum threshold value above which P-GW-provided load control information should be utilized for calculating the P-GW effective weight during initial node selection.

Use the following example to configure Load Control Profile threshold on the P-GW.

```
config
   gtpc-load-control-profile profile_name
      threshold time_in_seconds
      end
```

Notes:

- The default threshold value is 50.

Configuring 3GPP R12 Load Control Information Handling

The handling of load control information for the home or visited PLMN can be enabled/disabled via this procedure.

Use the following example to enable/disable load control profile information handling on the SAEGW/S-GW/P-GW.

```
config
   gtpc-load-control-profile  profile_name
      load-control-handling { home | visited }
      no load-control-handling { home | visited }
      end
```

Notes:

- **no** disables load-control-handling for the specified option.

Configuring 3GPP R12 Load Control Information Publishing

The publishing of load control information can be enabled/disabled for the home or visited PLMN.

Use the following example to enable/disable load control profile information publishing on the P-GW/SAEGW/S-GW.

```
config
   gtpc-load-control-profile profile_name
      load-control-publishing { home | visited }
      no load-control-publishing { home | visited }
      end
```

Notes:

- **no** disables load control profile information publishing for the specified option.

Configuring the 3GPP R12 GTP-C Polling Parameter Interval

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

Beginning with StarOS release 21, a new CLI command, **gtpc-system-param-poll interval**, is introduced in *Context Configuration Mode* to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements. This command sets the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager.

To configure the GTP-C polling parameter interval:

```
config
   context context_name
      gtpc-system-param-poll interval seconds
      default gtpc-system-param-poll interval
      end
```

- Where *seconds* is the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager. Valid entries are from 15 to 300 seconds. The default setting is 30 seconds.
- **default** returns the setting to its default value of 30 seconds.



Caution Setting the time interval to a low value may impact system performance.

Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service.

Once the 3GPP R12 GTP-C load control profile is created, it must be associated with an existing P-GW, SAEGW, or S-GW service.

Use the following examples to associate the GTP-C load control profile with an existing P-GW, SAEGW, or S-GW service.

P-GW Service Association:

```
configure
   context  context_name
      pgw-service pgw_service_name
         associate gtpc-load-control-profile profile_name
         no associate gtpc-load-control-profile
         end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

S-GW Service Association:

```
configure
   context  context_name
      sgw-service sgw_service_name
         associate gtpc-load-control-profile profile_name
         no associate gtpc-load-control-profile
         end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

SAEGW Service Association::

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-load-control-profile profile_name
         exit
      pgw-service pgw_service_name
         associate gtpc-load-control-profile profile_name
         exit
      saegw-service saegw_service_name
         associate sgw-service sgw_service_name
         associate pgw-service pgw_service_name
         exit
```

Verifying the 3GPP R12 Load Control Configuration

Use the following command to view the load control profile configuration settings:

```
show gtpc-overload-control-profile full name load_control_profile_name
```

The output of this command provides the configuration settings of all load control parameters, including:

- Weightage
- Inclusion Frequency
- Load control information handling
- Load control information publishing
- Load threshold

Saving the Configuration

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

Creating and Configuring a 3GPP R12 GTP-C Overload Control Profile

This section describes how to create and configure a 3GPP R12 GTP-C overload control profile on the P-GW/SAEGW/S-GW.

Configuration Overview

Procedure

Step 1 Create the GTP-C overload control profile. Refer to Creating the GTPP R12 Overload Control Profile, on page 617.

Step 2 Configure the weightage settings. Refer to Configuring 3GPP R12 Overload Control Weightage Settings, on page 617.

Step 3 Configure the inclusion frequency. Refer to Configuring the 3GPP R12 Overload Control Inclusion Frequency, on page 618.

Step 4 Configure the validity period. Refer to Configuring the 3GPP R12 Overload Control Validity Period, on page 618.

Step 5 Configure the tolerance settings. Refer to Configuring 3GPP R12 Overload Control Tolerance Limits, on page 619.

Step 6 Configure the throttling behavior for the node. Refer to Configuring 3GPP R12 Overload Control Throttling Behavior, on page 619.

Step 7 Configure the message prioritization. Refer to Configuring 3GPP R12 Overload Control Message Prioritization, on page 620.

Step 8 Configure self-protection behavior for the node. Refer to Configuring 3GPP R12 Overload Control Self-Protection Behavior, on page 620.

Step 9 Configure overload control information handling. Refer to Configuring 3GPP R12 Overload Control Information Handling, on page 621.

Step 10 Configure overload control information publishing. Refer to Configuring 3GPP R12 Overload Control Information Publishing, on page 621.

Step 11 Configure the GTP-C polling parameter interval . Refer to Configuring the 3GPP R12 GTP-C Polling Parameter Interval, on page 614.

Step 12 Associate the overload control configuration with an existing P-GW/SAEGW/S-GW service. Refer to Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service, on page 622.

Step 13 Verify the overload control configuration. Refer to Verifying the 3GPP R12 Overload Control Configuration , on page 623.

Step 14 Save the configuration. Refer to Saving the 3GPP R12 Overload Control Configuration, on page 624.

Creating the GTPP R12 Overload Control Profile

Use the following example to create the GTP-C Overload Control Profile:

```
configure
   gtpc-overload-control-profile  profile_name
   no gtpc-overload-control-profile  profile_name
   end
```

Notes:

- **no**: Removes specified GTP-C Overload Control profile.
- *profile_name* must be an alphanumeric string from 1 to 64 characters in length.

Configuring 3GPP R12 Overload Control Weightage Settings

This section describes how to configure GTP-C Overload Control weightage parameters. These parameters constitute the basic settings for this GTP-C Overload Control Profile. Communication of these parameters indicate to peers when this network element is becoming or being overloaded. When this occurs, the NE will be able to instruct its peers to gracefully reduce its incoming signaling load by instructing the peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Use the following example to configure the GTP-C Overload Control Weightage settings on the P-GW/SAEGW/S-GW.

```
configure
   gtpc-overload-control-profile  profile_name
      weightage system-cpu-utilization percentage system-memory-utilization
 percentage license-session-utilization percentage.
      default weightage
      end
```

Notes:

- Total weightage for all parameters should be 100.
- **system-cpu-utilization** *percentage*: Configures system cpu utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 40.
- **system-memory-utilization** *percentage*: Configures system memory utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.
- **license-session utilization** *percentage*: Configures license session utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.

Configuring the 3GPP R12 Overload Control Inclusion Frequency

This section describes how to set the parameters that determine the inclusion frequency of the Overload Control Information Element (OCI) for a GTP-C Load Control Profile configuration. The OCI is a 3GPP-specific IE that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send this information to the peers.

Use the following example to configure the overload control profile inclusion frequency on the P-GW/SAEGW/S-GW.

```
configure
   gtpc-overload-control-profile  profile_name
      inclusion-frequency { advertisement-interval interval_in_seconds |
change-factor change_factor }
     default inclusion-frequency { advertisement-interval | change-factor
 }
      end
```

Notes:

- **inclusion frequency**: Configures parameters to decide inclusion frequency of the OCI information element.
- **advertisement-interval** *interval_in_seconds*: Configures the advertisement-interval for overload control in seconds. Specifies how often overload control information should be sent to the peers. If configured to 0, the node will send overload control information in each and every outgoing message to the peers.*interval_in_seconds* must be an integer from 0 to 3600. The default is 300.
- **change-factor** *change_factor*: P-GW only. Configures the change factor for overload control. If the overload control factor changes by a configured factor, whether by an increase or decrease, the overload control information should be sent to the peers. This information is only sent to the peers when the overload factor changes by the factor configured.*change_factor* must be an integer from 1 to 20. The default is 5.

Configuring the 3GPP R12 Overload Control Validity Period

This section describes how to configure the overload control validity period. The validity period is the length of time during which the overload condition specified by the overload control information element is to be considered as valid, unless overridden by subsequent new overload control information.

Use the following example to configure the GTP-C Overload Control validity period on the P-GW/SAEGW/S-GW.

```
configure
   gtpc-overload-control-profile profile_name
      validity-period seconds
      default validity-period
      end
```

Notes:

- **validity-period** *seconds*: Configures the validity of overload control information. *seconds* must be an integer from 1 to 3600. The default is 600 seconds.

Configuring 3GPP R12 Overload Control Tolerance Limits

Use this example to configure GTP-C Overload Control Tolerance limits.

```
configure
   gtpc-overlaod-control-profile  profile_name
      tolerance { initial-reduction-metric percentage | threshold
report-reduction-metric percentage self-protection-limit percentage  }
      default tolerance { initial-reduction-metric | threshold }
      end
```

Notes:

- **initial-reduction-metric** *percentage*: Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit. When reaching the configured minimum threshold, this parameter specifies how much the node wants the peers to reduce incoming traffic.*percentage* must be an integer from 1 to 100. The default is 10.
- **threshold report-reduction-metric** *percentage*: Configures the minimum overload tolerance threshold for advertising overload reduction metric to the peer. When the minimum threshold is reached, the node will report this information to peers. When the maximum limit is reached, the node will go into self-protection mode. *percentage* must be an integer from 1 to 100. The default is 80.
- The **threshold report-reduction-metric** should always be lower than the **self-protection-limit**.
- **self-protection-limit** *percentage*: Configures the maximum overload tolerance threshold after which node will move to self protection mode. When the maximum limit is reached, the node will start rejecting all incoming messages, except for delete messages. The node will not initiate any new messages to the peers. This is to mitigate the overload condition.*percentage* must be an integer from 1 to 100. The default is 95.

Configuring 3GPP R12 Overload Control Throttling Behavior

Use this command to configure throttling behavior based on peer's overload reduction-metric by excluding some or all emergency events and/or messages with configured EARP. Message throttling applies only to initial messages. Triggered request or response messages should not be throttled since that would result in the retransmission of the corresponding request message by the sender.

If **throttling-behavior** is configured, the profile can be associated with an S-GW or P-GW service. If a P-GW specific keyword is configured, and the profile is associated with an S-GW service, the S-GW will ignore the P-GW specific configuration. Only the parameters specific to S-GW or P-GW will be utilized.

Use this example to configure GTP-C overload control throttling behavior on the P-GW/SAEGW/S-GW.

```
configure
   gtpc-overlaod-control-profile  profile_name
      throttling-behavior { earp [ 1 | 2 | 3 | 4 | 5 | 6 | 7 |8 | 9 | 10
 | 11 | 12 | 13 | 14 | 15 ]* exclude } | emergency-events exclude }
      no throttling-behavior [ earp [ 1 |2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
 10 | 11 | 12 | 13 | 14 | 15 ]* exclude | emergency-events exclude ]
      end
```

Notes:

- **throttling-behavior**: Configures throttling behavior based on peer's overload reduction-metric.

- **earp**: Excludes the specified messages with configured earp from throttling due to peer's overload-reduction metric. If a bearer with configured EARP is created or updated, it will be excluded from throttling.
- *****: Indicates that more than one of the keywords can be entered within a single command.
- **emergency-events exclude**: P-GW Only. Excludes all emergency events from throttling due to the peer's overload reduction-metric. While reducing messages towards the peer based on the overload information received from the peer, the P-GW will exclude events sent for emergency sessions.

Configuring 3GPP R12 Overload Control Message Prioritization

In the R12 GTP-C Load Overload control feature, it is possible to apply message throttling, (when a peer indicates it is overloaded), based on message priority. To apply message prioritization it is necessary to configure the percentage of two groups of messages that each node (P-GW or ePDG) is expected to generate. The operator can define the expected number of messages as a percentage for each message group.

Use the following example to configure message prioritization.

```
configure
   gtpc-overload-control-profile profile_name
      message-prioritization  group1 percentage group2 percentage
      no message-prioritization
      default message-prioritization
      end
```

Notes:

- **group1** specifies the message priority percentage for the following messages:
  - Update Bearer Request message for default bearer generated from P-GW ingress
  - Update Bearer Request message for dedicated bearer generated from P-GW ingress
  - Handoff Create Session Request message generated from ePDG egress.
- **group2** specifies the message priority percentage for the following messages:
  - Create Bearer Request message for default bearer generated from P-GW ingress
  - PDN connection requested Create Session Request message from ePDG egress
- The total percentage for the message groups should equal 100.
- **group1** messages will have the highest priority (1) and are dropped last. **group2** messages will have the lowest priority (2) and are dropped first.
- **default** returns the group message priority settings to their default value. The default for each group is 50.
- The default behavior for this command is enabled. To disable the command use the **no** option.

Configuring 3GPP R12 Overload Control Self-Protection Behavior

This functionality enables the operator to configure APN names and EARP priority level values for self-protection mode so that incoming request messages for emergency packet data node (PDN) connections and/or configured EARP priority values are not rejected even if the system is under self-protection mode.

Use this example to configure GTP-C overload control self-protection behavior.

```
configure
   gtpc-overload-control-profile profile_name
      self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 | 3
| 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude } }
      no self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 |
 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude } }
      end
```

Notes:

- **apn** configures up to three APN names to be allowed under self-protection behavior.
- **earp** configures up to three EARP priority level values so that incoming request messages for the configured evolved ARP priority values are not rejected even if the system is under self-protection mode.
- **no** disables the specified options.

Configuring 3GPP R12 Overload Control Information Handling

Use this command to enable/disable the handling of overload control information for the home or visited PLMN.

```
configure
   gtpc-load-control-profile profile_name
      overload-control-handling { home | visited }
      no overload-control-handling { home | visited }
      default overload-control-handling
      end
```

Notes:

- **home**: Enables the handling of load control information for the home PLMN.
- **visited** enables the handling of load control information for the visited PLMN.
- **default**: Returns load control handling to its default behavior (enabled).

Configuring 3GPP R12 Overload Control Information Publishing

Enables or disables the publishing of load control information towards the home or visited PLMN.

```
configure
   gtpc-overload-control-profile profile_name
      overload-control-publishing { home | visited }
      no overload-control-publishing { home | visited }
      default overload-control-publishing
      end
```

Notes:

- **home**: Enables the publishing of load control information towards the home PLMN.
- **visited**: Enables the publishing of load control information towards the visited PLMN.
- **default**: Returns load control handling to its default behavior (enabled).

Configuring the 3GPP R12 GTP-C Polling Parameter Interval

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

Beginning with StarOS release 21, a new CLI command, **gtpc-system-param-poll interval**, is introduced in *Context Configuration Mode* to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements. This command sets the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager.

To configure the GTP-C polling parameter interval:

```
config
  context context_name
    gtpc-system-param-poll interval seconds
    default gtpc-system-param-poll interval
    end
```

- Where *seconds* is the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager. Valid entries are from 15 to 300 seconds. The default setting is 30 seconds.
- **default** returns the setting to its default value of 30 seconds.

⚠

Caution Setting the time interval to a low value may impact system performance.

Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service

Once the 3GPP R12 overload control profile has been configured, it must be associated with an existing P-GW, SAEGW, or S-GW service.

Use the following examples to associate the overload control configuration to an existing service.

P-GW Service Association:

```
configure
   context context_name
      pgw-service pgw_service_name
         associate gtpc-overload-control-profile profile_name
         no associate gtpc-overload-control-profile
         end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

S-GW Service Association:

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-overload-control-profile profile_name
         no associate gtpc-overload-control-profile
         end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

SAEGW Service Association::

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-overload-control-profile profile_name
         exit
      pgw-service pgw_service_name
         associate gtpc-overload-control-profile profile_name
         exit
      saegw-service saegw_service_name
         associate sgw-service sgw_service_name
         associate pgw-service pgw_service_name
         exit
```

Verifying the 3GPP R12 Overload Control Configuration

Use the following command to view the overload control configuration settings.

show gtpc-overload-control-profile full name *overload_control_profile_name*

The output of this command provides all overload control profile configuration settings, including:

- Weightage
- Tolerance
- Inclusion Frequency
- Validity Period
- Throttling Profile
- Self-Protection Behavior
- Overload control information Handling
- Overload control information Publishing
- Message Prioritization

Saving the 3GPP R12 Overload Control Configuration

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*.

Monitoring and Troubleshooting the 3GPP R12 GTP-C Load and Overload Control Feature

This section provides information to assist operators in monitoring the 3GPP R12 GTP-C Load and Overload Control feature.

3GPP R12 GTP-C Load and Overload Show Commands

This section provides information regarding show commands in support of the 3GPP R12 Load and Overload Control feature.

show egtpc statistics egtp-service <egtp-service name>

The output of this command provides detailed granular statistics for 3GPP R12 load and overload control profile statistics that have been transmitted (TX) and received (RX). Statistics are provided on a per egtp-service basis.

show gtpc-load-control-profile full all

The output of this command provides all configuration settings for all 3GPP R12 load control profiles configured on the node. Use this command to determine if the load control profile is configured as intended.

show gtpc-load-control-profile full name <name>

Use this command to view all configuration settings for the specified 3GPP R12 load control profile.

show gtpc-overload-control-profile full all

The output of this command provides all configuration settings for all 3GPP R12 overload control profiles configured on the node. Use this command to determine if the overload control profile is configured as intended.

show gtpc-overload-control full name <name>

The output of this command provides all configuration settings for all 3GPP R12 Overload Control Profiles configured on the node. Use this command to determine if the Overload Control Profile is configured as intended.

show pgw-service all

Use this command to obtain the names of all 3GPP R12 load control and 3GPP R12 overload control profiles configured on the P-GW.

show sgw-service all

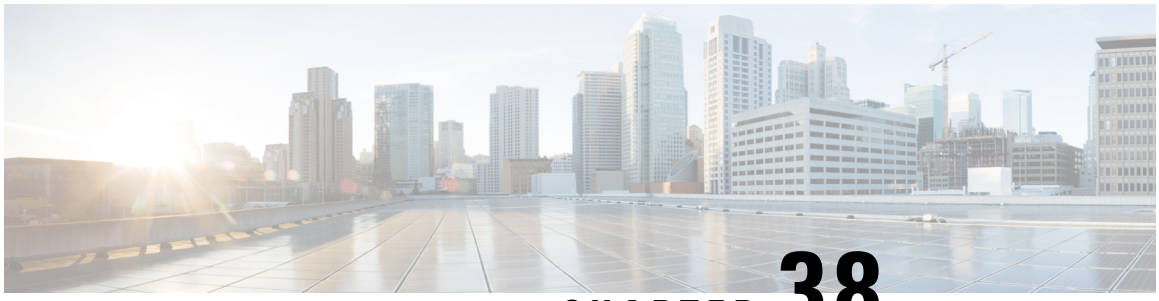
Use this command to obtain the names of all 3GPP R12 Load Control and Overload Control profiles configured on the S-GW.

eGTP-C Bulk Statistics

The following statistics are included in the eGTP-C Schema in support of the 3GPP R12 Load and Overload Control feature:

- load-overload-own-lci
- load-overload-own-oci
- load-overload-num-msg-throttled
- load-overload-num-ovrload-cond-reached

For descriptions of these variables, see "eGTP Schema Statistics" in the *Statistics and Counters Reference*.



CHAPTER 38

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, on page 627
- Rel. 8 Gx Interface, on page 652
- Rel. 9 Gx Interface, on page 673
- Rel. 10 Gx Interface, on page 681
- Supported Gx Features, on page 688

Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR chassis for the following products:

- GGSN
- IPSG

This section describes the following topics:

- Introduction, on page 628
- Terminology and Definitions, on page 630
- How Rel. 7 Gx Works, on page 644
- Configuring Rel. 7 Gx Interface, on page 647
- Gathering Statistics, on page 652

Introduction

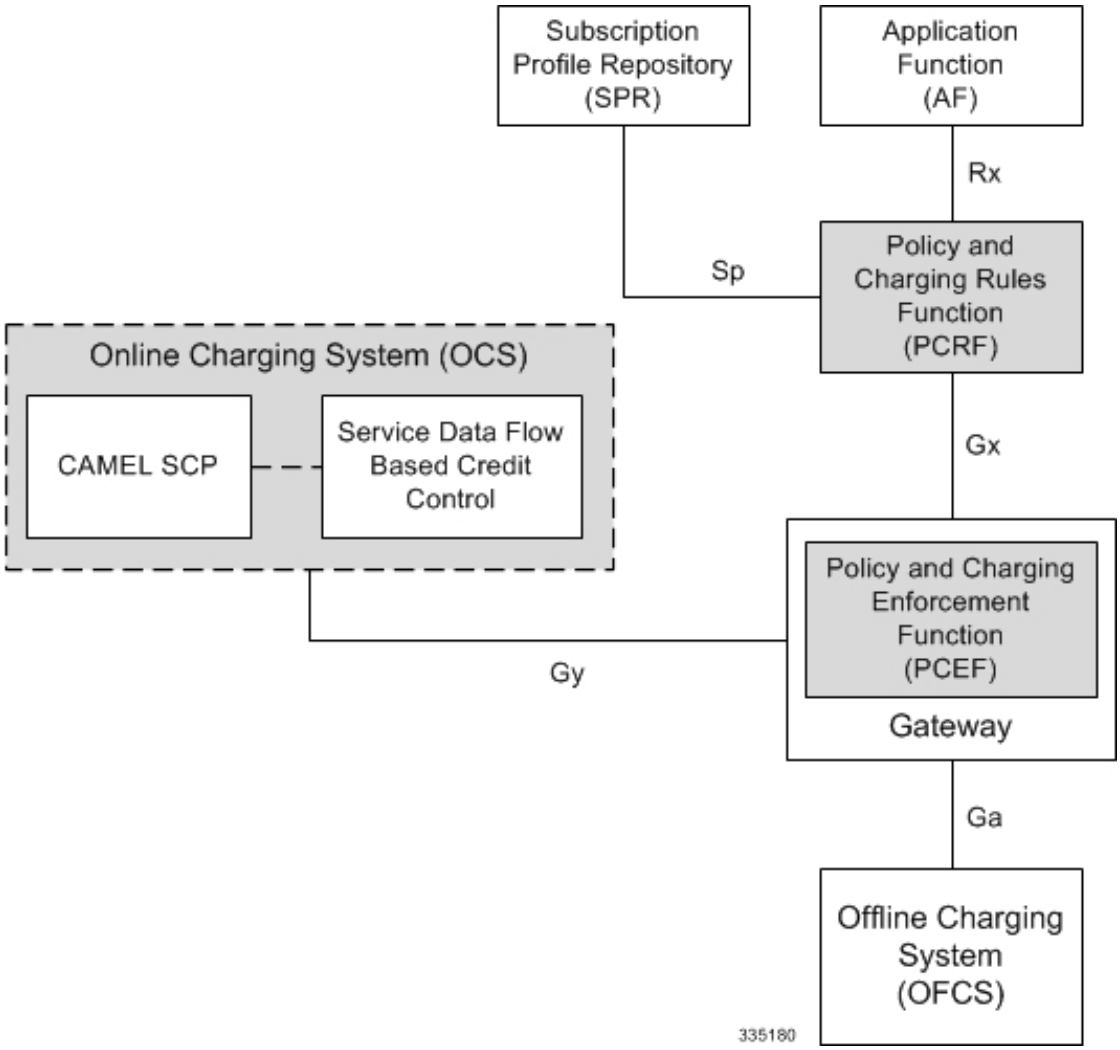
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is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

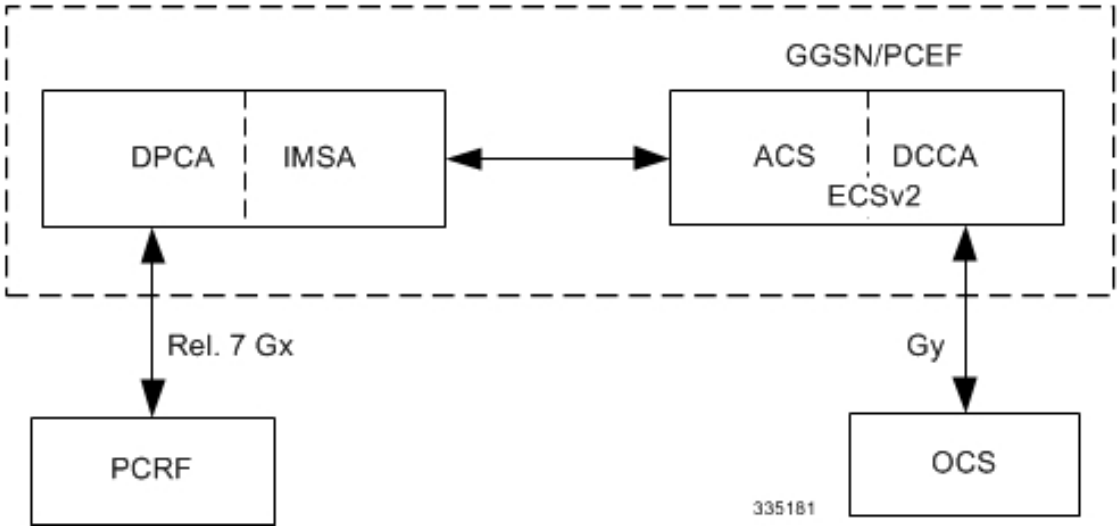
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, 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 59: 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 60: PCC Architecture within Cisco PCEF



Supported Networks and Platforms

This feature is supported on all chassis 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.

  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.

  The 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.

    The RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS.

- 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.

  SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger will be sent under the following conditions:

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

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



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

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



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

Supported Features:

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



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

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



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

  - Policy Enforcement for Authorized QoS per QCI: The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values.

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

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

      In the following scenarios UE_ONLY is chosen as the BCM:

Scenario 1:

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

Scenario 2:

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

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

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

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

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

  The 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 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.

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 ECS uses the entire ARP byte 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, 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.

There are 24 PCC rules that can be recovered per bearer in the event of a session manager crash. Also, up to 24 PCC rules can be recovered post ICSR.

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 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.

During 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 IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value.

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.

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 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.

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.

The usage reporting on bearer termination and uplink/downlink level reporting are 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. Monitoring key at session level is supported.

  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.

  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.

  An 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

  An 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.

If threshold breach happens for multiple monitoring keys at the same time, 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, 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. The usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  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: 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.

- 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. This is configurable in the standard implementation.

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.

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 651.

ICSR Support for Volume Reporting over Gx (VoRoGx)

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 The DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 61: Rel. 7 Gx IMS Authorization Call Flow

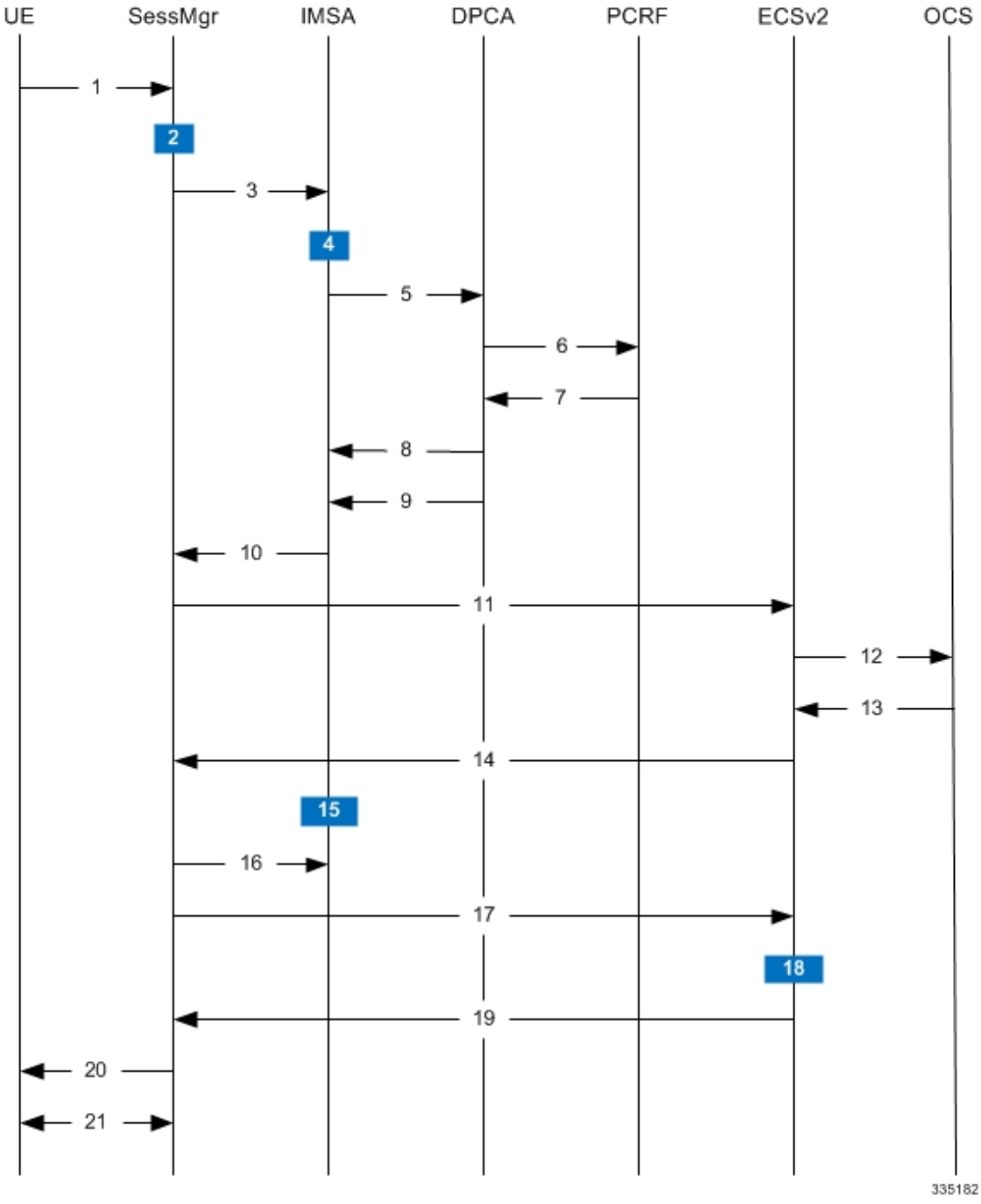


Table 70: Rel. 7 Gx IMS Authorization Call flow Description

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.
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 the RAR messages are allowed before the session is established. Also note that 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.

Step	Description
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.
21	Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).

Configuring Rel. 7 Gx Interface

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

To configure Rel. 7 Gx interface functionality:

Procedure

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 648.

Step 2 Verify your configuration as described in Verifying the Configuration, on page 650.

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 650.

Step 4 Verify your configuration as described in Verifying Subscriber Configuration, on page 651.

Step 5 *Optional:* Configure the Volume Reporting over Gx feature as described in Configuring Volume Reporting over Gx, on page 651.

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.
- 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.

  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.

  A maximum of 128 rows can be added to the MSISDN prefix range table.

  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:
- *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:

Procedure

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 647.

```
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 is available to enable volume 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 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 71: 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**

Rel. 8 Gx Interface

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

This section describes the following topics:

- HA/PDSN Rel. 8 Gx Interface Support, on page 652
- P-GW Rel. 8 Gx Interface Support, on page 668

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, on page 653
- Terminology and Definitions, on page 655
- How it Works, on page 662
- Configuring HA/PDSN Rel. 8 Gx Interface Support, on page 665
- Gathering Statistics, on page 667

Introduction

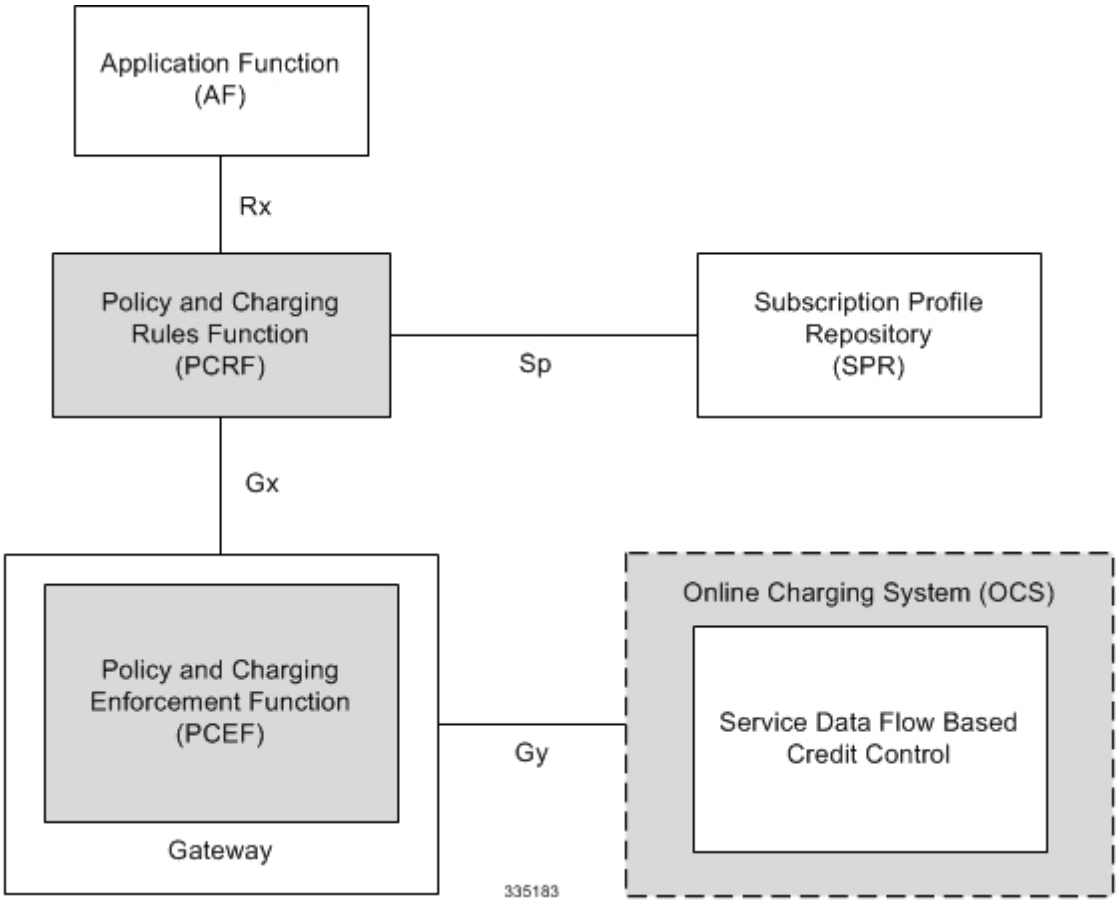
For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished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

The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

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

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

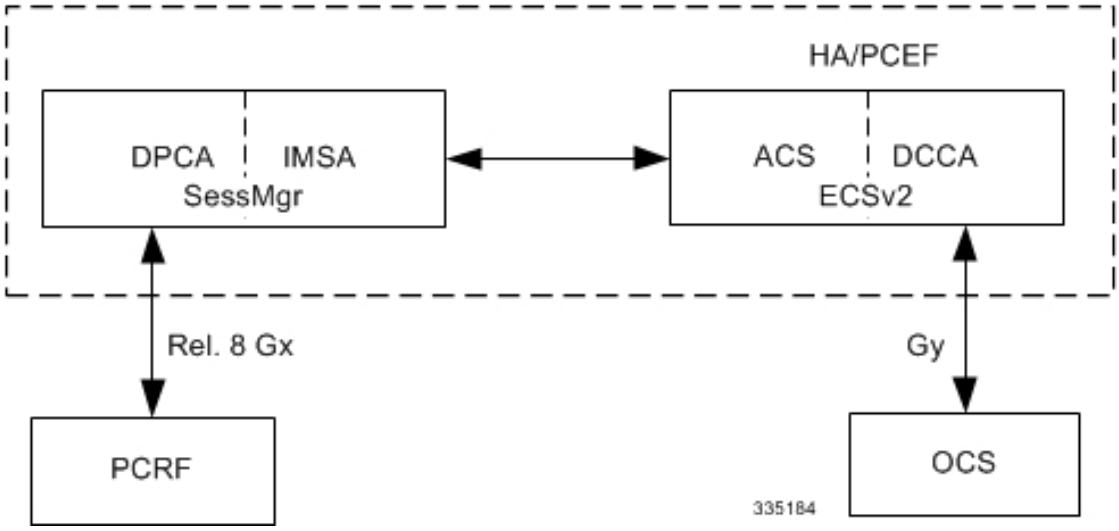
Figure 62: HA/PDSN Rel. 8 Gx PCC Logical Architecture



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 63: 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.

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.

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.

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 the event of a session manager crash, 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.

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 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.

During 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 The DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 64: HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

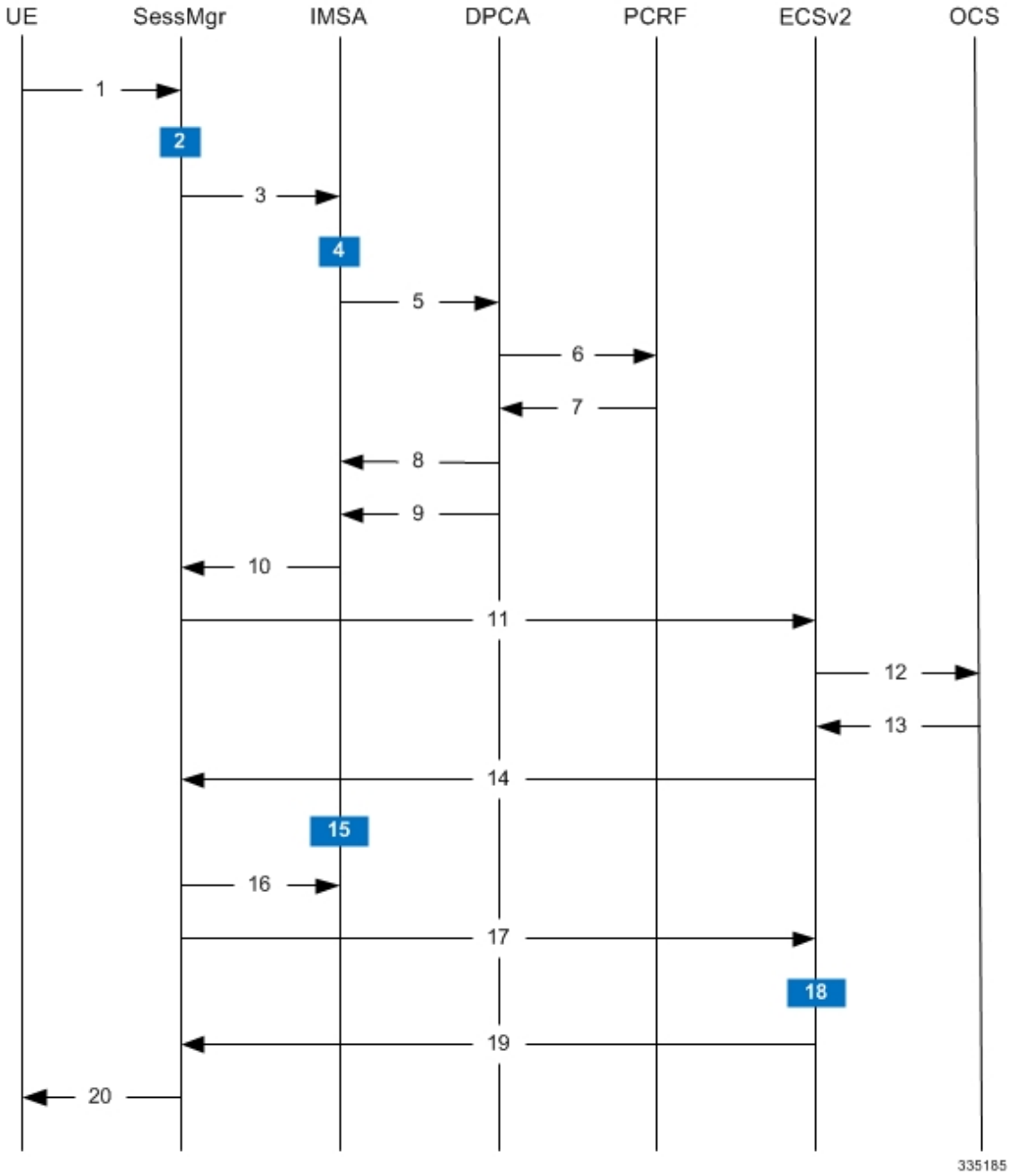


Table 72: HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

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

Step	Description
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 665.
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 667.
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.
- 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 665.

```
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 73: 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**

Statistics/Information	Action to perform
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**

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 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.

Volume Reporting supports both the total data usage reporting and the uplink/downlink level reporting

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.

It supports usage reporting on bearer termination.

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. PCRF supports Monitoring Key at session level.

  PCRF supports to enable and disable session usage in a single message. This is supported only if the monitoring key is associated at session level.

  PCRF supports the monitoring of usage based on input/output octet threshold levels. 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.

  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

  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.

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, 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. Usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  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: 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.

- The 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. This is configurable in the standard implementation.

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.

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 651.

ICSR Support for Volume Reporting over Gx (VoRoGx)

Volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post ICSR 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.

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 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.

Volume Reporting over GX supports both the total data usage reporting and uplink/downlink level reporting.

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.

The 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. PCRF supports Monitoring Key at session level.

  PCRF supports to enable and disable session usage in a single message. This is supported only if the monitoring key is associated at session level.

  PCRF supports the monitoring of usage based on input/output octet threshold levels. 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.

  An 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

  An 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.

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, 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. Usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  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: 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.

- The 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. This is configurable in the standard implementation.

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.

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 651 section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

Volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post ICSR 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 678
- Configuring Rel.9 Compliant AVPs, on page 679
- Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule, on page 680

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.

This section describes the following topic:

• P-GW Rel. 10 Gx Interface Support, on page 681

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 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.

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.

The 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. PCRF supports the Monitoring Key at session level.

  PCRF supports to enable and disable session usage in a single message. This is supported only if the monitoring key is associated at session level.

  PCRF supports the monitoring of usage based on input/output octet threshold levels. 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.

  An 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

  An 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.

When threshold breach happens for multiple monitoring keys at the same time, 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, 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. The usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  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: 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.

- The 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. This is configurable in the standard implementation.

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.

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 651.

ICSR Support for Volume Reporting over Gx (VoRoGx)

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.

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.

There are 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.

Sponsored connectivity is supported with "dpca-custom8" Gx dictionary. When a session is enabled for sponsored connectivity from PCRF and offline charging is enabled using aaa-custom4 dictionary, sponsored connectivity AVPs are reported in ACR interim and ACR Stop packets to the CDF server. The AVPs Sponsor-Identity and Application-Service-Provider-Identity are sent under grouped AVP Service-Data-Container in ACR packets.

This feature supports dynanic rules and Gx dictionary—dpca-custom 15 and dpca-custom8.

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

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.

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".

The 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.

The following behaviors was 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.

After 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.

The gateway (GW) node and PCRF 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:

Procedure

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 691.

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 692.

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 693.

Step 4 Verify your configuration as described in the Verifying Local Policy Service Configuration, on page 693.

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, 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 696.

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

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

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

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

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

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

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

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

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

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

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

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
```

```
[ default ] max-outstanding-ccr-u value
end
```

Notes:

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

Support for RAN/NAS Cause IE on Gx Interface

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

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

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

Configuring Supported Feature Netloc-RAN-NAS-Cause

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

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

                  end
```

Notes:

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

To disable this supported feature, use the following command:

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

Support ADC Rules over Gx Interface

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

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

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

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

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

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

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



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

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

- TDF-Application-Identifier: It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.
- Redirect-Information: This indicates whether the detected application traffic should be redirected to another controlled address.
- Mute-Notification: This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.
- Application Detection Information: If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

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

Limitations

The limitations for the ADC over Gx feature are:

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

Configuring ADC Rules over Gx

The following configuration enables ADC rules over Gx interface.

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

Notes:

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

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

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

GoR Name Support in TDF-Application-Identifier

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

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

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

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

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

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

- The following AVPs will be modified and applied when received from PCRF:
  - Precedence
  - Rating-Group/Service-Identifier/Sponsor-Identity (mandatory depending on the Reporting-Level)
  - Metering-Method
  - Online/Offline
  - QoS-Information
  - Monitoring-Key
  - Redirect-Information

- Dynamic route will be updated for all protocols of rules that are part of TDF-Application-Identifier GoR.
- Any change in dynamic rule priority or TDF-Application-Identifier value will lead to sending of APP-START and APP-STOP event notifications as new rule match. If an APP-START notification was sent already before rule modification, the corresponding APP-STOP notification will not be sent.
- Runtime deletion of associated GoR will take immediate effect and APP-STOP notification will not be sent if an APP-START was already sent. Addition of GoR at service level will need to have rules to be re-installed for the new addition to take effect for both dynamic and predefined ADC rules.

ADC Mute Customization

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

- A Gx message might contain both Standards based MUTE and the custom MUTE.
- Standards based MUTE is given preference over the custom MUTE/UNMUTE.
- A dynamic ADC rule can be installed and modified with a custom MUTE.
- Custom-Mute-Notification AVP can be sent by the PCRF in CCA-I and RAR.
- A dynamic ADC rule can be modified with a custom UNMUTE.
- On a custom MUTE for a given dynamic ADC rule, PCEF sends a single APPLICATION_START/ APPLICATION_STOP response for the entire application traffic rather the per flow APPLICATION_START /APPLICATION_STOP response.
- On a custom MUTE for a given dynamic ADC rule, if no APPLICATION_START has been sent prior to the custom MUTE then a single APPLICATION_START is sent on the next flow packet that hits the dynamic rule.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with the flow's 5-tuple information.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with TDF-Application-Instance-Identifier = 0.
- On a custom MUTE for a given dynamic rule, a single APPLICATION_STOP is sent when the last flow associated with the given dynamic rule is terminated. Such an APPLICATION_STOP will not contain 5-tuple information of the last flow and is sent with TDF-Application-Instance-Identifier = 0.
- On a custom UNMUTE for a given dynamic rule, APPLICATION STARTs response is matched with the given dynamic rule and then sent to all the forthcoming flows.
- There is no change in behavior for a custom UNMUTE, which has not been custom MUTED or standard MUTED before UNMUTING. APPLICATION_STARTs and APPLICATION_STOPs is continued to be sent per flow as before.
- On a custom UNMUTE, PCEF sends an APPLICATION_STOP each for all flows that terminate then onwards.
- A given dynamic rule is recovered in both SR and ICSR including the Custom MUTE/UNMUTE status. The APPLICATION_START status for a given dynamic rule is check-pointed and recovered. This ensures that an extra APPLICATION_START is not sent to the PCRF post recoveries.

Enhancement to the ADC Custom Mute/Unmute Functionality

Feature Information

Summary Data

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

Revision History



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

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

Feature Changes

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

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

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

Limitations

Following are the limitations of this feature:

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

How it Works

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

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

Following are some important points:

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

Configuring the ADC Notifications

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

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

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

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

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

For configuring single notification use the following command:

```
adc notify once
```

Notes:

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

Support for TAI and ECGI Change Reporting

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

This section discusses the following topics for this feature:

- Feature Description, on page 705
- How it Works, on page 706
- Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature, on page 707

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). 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.

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
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: ULI_CHANGE + TAI/ECGI CHANGE ULI_Type: TAI+ECGI

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
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 708
- How it Works, on page 708
- Configuring Location Based Local Policy Rule Enforcement Feature, on page 710
- Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature, on page 712

Feature Description

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

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

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

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

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

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

Relationships to Other Features

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

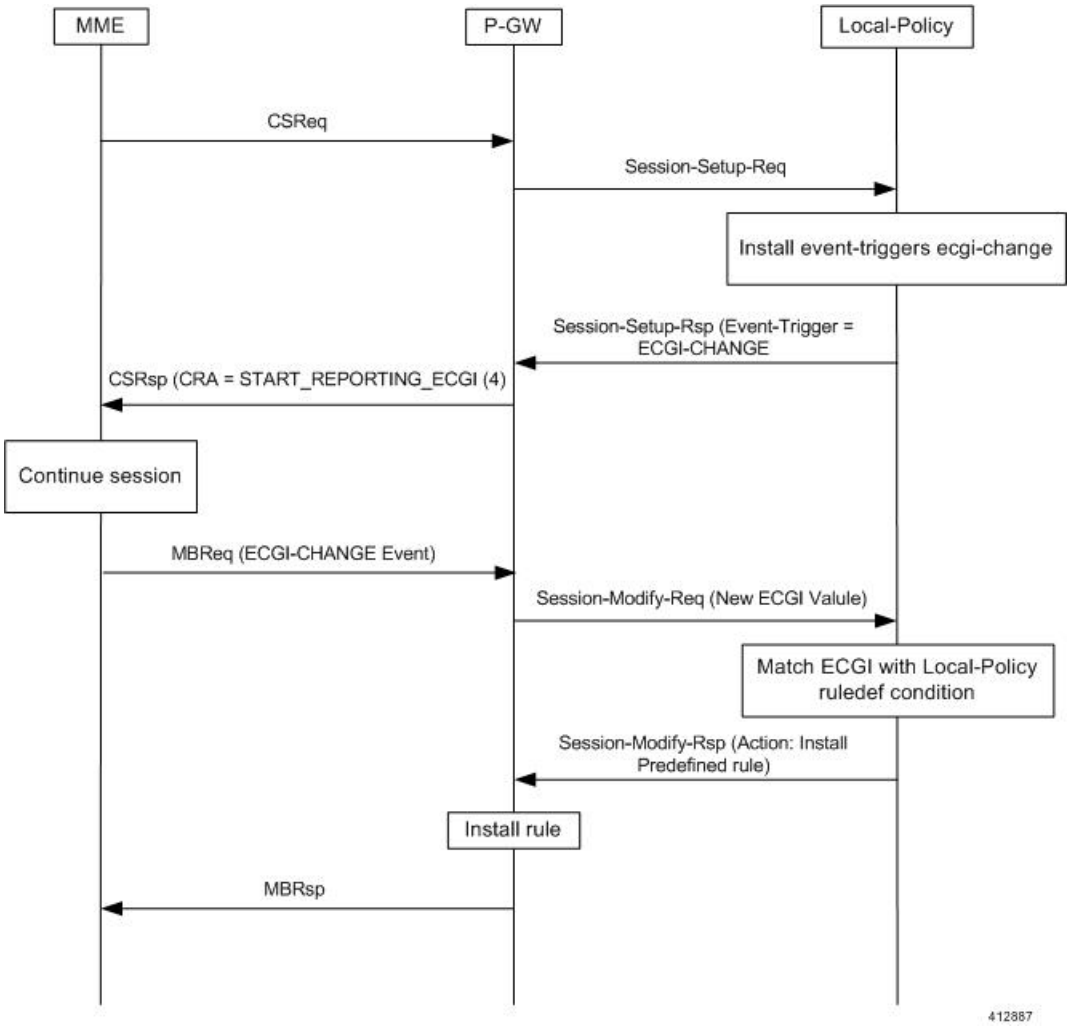
How it Works

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

Flows

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

Figure 65: ECGI-CHANGE Event Handling



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

Limitations

This section identifies the known limitations of this feature.

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

Configuring Location Based Local Policy Rule Enforcement Feature

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

Configuring ECGI Change Trigger

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

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

Notes:

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

Applying Rules for ECGI-Change Event

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

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

Notes:

- **priority** *priority*: Specifies a priority for the specified rule. *priority* must be unique and an integer from 1 to 2048.
- **ruledef** *ruledef_name*: Associates the rule with a specific ruledef. *ruledef_name* must be an existing ruledef within this local QoS policy service.
- **actiondef** *actiondef_name*: Associates the rule with a specific actiondef. *actiondef_name* must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.
- **ecgi-change**: Enables a new event to detect ECGI-CHANGE and applies specific action for the ECGI-CHANGE event as defined in actiondef configuration.

- **continue**: Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Enforcing Local Policy Rule based on ECGI Value

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

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

Notes:

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

Verifying the Location Based LP Rule Enforcement Configuration

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

```
show configuration context
```



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

Here is an example configuration for this feature.

```
configure
   context source
      apn corporate-apn
         ims-auth-service LocalPolicy_1
      exit
   exit
end
```

```
configure
   local-policy-service LocalPolicy_1
      ruledef any-imsi
         condition priority 1 imsi match *
```

```
      exit
      ruledef ecgi-group
         condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
      exit
      actiondef ecgi-trigger
         action priority 1 event-triggers ecgi-change
      exit
      actiondef ecgi-redirect-rule
         action priority 1 activate-rule namerule-1
      exit
      eventbase default
        rule priority 1 event new-call ruledef any-imsi actiondef ecgi-trigger

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

Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature

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

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

show configuration context

logging filter active facility local-policy level debug

show local-policy statistics

show active-charging sessions full

show local-policy statistics summary

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

- Event Statistics:
  - ECGI Change - Displays the number of ECGI-CHANGE event triggers that has been received by Local-Policy.
- Variable Matching Statistics
  - ECGI - Displays the number of times the ECGI is matched and the specific action is applied based on the event.

Gx Support for GTP based S2a/S2b

The Gx support for GTP based S2a/S2 interface is extended to all customers for WiFi integration in P-GW. 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 713
- Configuring Gx based Virtual APN Selection Feature , on page 714
- Monitoring and Troubleshooting the Gx based Virtual APN Selection, on page 714

Feature Description

Overview

The current implementation supports Virtual APN (VAPN) Selection through RADIUS or local configuration. The 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 the StarOS Gx architecture, every Diameter session is associated with a primary and secondary peer when the host selection is configured at the IMSA service.

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

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

```
configure
   context test
      diameter endpoint Gx
         ...
         peer DRA1 realm realmName address 192.168.23.3
         peer DRA2 realm realmName address 192.168.23.3 port 3869
         peer DRA3 realm realmName address 192.168.23.3 port 3870
         exit
```

```
      ims-auth-service imsa-Gx
         policy-control
            diameter host-select row-precedence 1 table 1 host DRA1
secondary host DRA2
end
```

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

Limitations

This section identifies the limitations for this feature.

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

NetLoc Feature Enhancement

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

Feature Description

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

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

This feature introduces the following behavior changes:

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

Table 74: 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.

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 **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.
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.

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.	Delete Bearer Response is received with **only New MS TZ** parameter.	Old ULI and New MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New MS TZ is sent towards the PCRF in the CCR-U message.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Delete Bearer Response is received with **No MS TZ** parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only old MS TZ is sent towards the PCRF.
Nothing is received.	Delete Session Request is received with New ULI and New MS TZ parameters.	New ULI and New MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with New ULI and No MS TZ parameter.	New ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with No ULI and No MS TZ parameter.	Old ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.

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

- Inclusion of AVP support of NETLOC-ACCESS-NOT-SUPPORTED on Gx interface. This inclusion of AVP is based on the below conditions:
  - RAT type is other than E-UTRAN, UTRAN, WCDMA, GPRS, GERAN, and W-LAN
  - IP CAN type is other than 3GPP EPS, GPRS, and non 3GPP EPS
  - Re-Auth-Request is received with Required-Access-Info AVP.
  - NetLoc feature is enabled on the chassis.
  - Event-Trigger ACCESS_NETWORK_INFO_REPORT (45) is installed.

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

- *Table 75: 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 76: 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 77: 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, on page 725
- Configuring System to Delete Diamproxy-Session ID Mismatched Sessions, on page 726
- Monitoring and Troubleshooting the Mismatched Session Deletion Feature, on page 727

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 728
- Configuring DPCA for Negotiating Mission Critical QCIs, on page 728
- Monitoring and Troubleshooting the Mission Critical QCI, on page 729

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: 209.165.200.233
 Primary PCRF Server: 209.165.200.233
 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, on page 730
- Configuring the HSS/PCRF-based P-CSCF Restoration, on page 731
- Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration, on page 732

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.

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 78: 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 79: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

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

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF. **Note** • If RAN/NAS cause is received in the Delete Bearer Response, which is triggered as a part of the Delete Bearer command and cause as “Request Accepted”, P-GW forwards the RAN/NAS cause (received in Delete Bearer Response) to the PCRF. • If RAN/NAS cause is received in the Delete Bearer command and Delete Bearer Response with HO in progress, the RAN/NAS Cause received in the Delete Bearer command is forwarded to the PCRF. • If RAN/NAS Cause is received in the Delete Bearer command and Delete Bearer Response with Accepted/Other Cause and new RAN/NAS Cause, the new RAN/NAS cause is forwarded to the PCRF.
	Accepted / Other GTP CCR-UCauses	CCR-U **Note** If RAN/NAS cause is received in the delete bearer response that is initiated through RAR/CCA-U, then P-GW doesl not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".
Delete Session Request	Accepted	CCR-T

ANI Behavior Towards PCRF

Section 4.5.6, 4.5.7, 4.5.12 of 3GPP 29.212 v13.4.0 mentions that if the RAN-NAS-Cause feature is supported, the PCEF should provide the available access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Trusted-WLAN feature is supported), User-Location-Info-Time AVP (if available), and 3GPP-MS-TimeZone AVP (if available).

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 80: 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

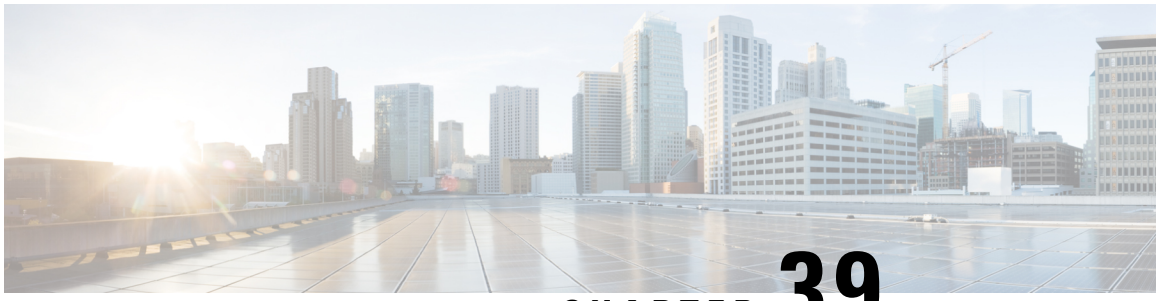
diameter encode-supported-features netloc-ran-nas-cause

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
```



CHAPTER 39

Gx Support for eMPS

- Feature Summary and Revision History, on page 747
- Feature Description, on page 748
- How It Works, on page 749
- Configuring Gx Support for eMPS, on page 750
- Monitoring and Troubleshooting the Gx Support for eMPS, on page 752

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	ASR 5500
Feature Default	• For GTP and Gx Prioritization for eMPS sessions: Disabled - Configuration Required • For Parsing of DRMP AVP: Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers, and that provide priority treatment in support of National Security and Emergency Preparedness (NS/EP) communications. A Service Provider is a public telecommunications service provider authorized by the NCS to provide GETS (including Legacy GETS), Wireless Priority Service (WPS), and/or NS/EP NGN Priority Services (NS/EP NGN-PS). The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is required when the Service Providers' networks are impaired due to congestion and/or damaged from natural disasters (such as floods, earthquakes, and hurricanes) and man-made disasters (such as physical, cyber, or other forms of terrorist attacks).

With this feature, support is added for NS/EP NGN priority service over the network which eventually requires the P-GW node to first identify an eMPS bearer/session (based on configured Enhanced Multimedia Priority Service (eMPS) evolved Allocation and Retention Priority (eARP)), and then prioritize their GTP and Gx signaling over the network.



Important For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPs bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

Prioritization of GTP and Gx Signaling

1. Prioritizing the GTP signaling for eMPS sessions implies:
   - Excluding the eMPS session's GTP control traffic from throttling due to Load Overload Control (For supplemental information about Load Overload Control, refer to the *3GPP R12 GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*).
2. Prioritizing the Gx signaling for eMPS sessions implies:
   - Excluding the eMPS session's Gx traffic from outgoing RLF throttling (RLF throttling is only applicable for Gx outgoing messages).
   - Excluding the eMPS session's Gx traffic from max-outstanding queue decisions.

Parsing the DRMP AVP from RAR Messages

Support is also extended for parsing the DRMP AVP from RAR messages on the Gx interface. And, if the DRMP value is received as 0, the corresponding response (RAA) message is prioritized, that is to say, excluded from Gx RLF throttling and max-outstanding queue decisions.

Relationships to Other Features

This feature is related to eMPS profile, Load Overload Control, Gx RLF throttling, and Max-outstanding configuration features, and one or more among these features may require additional license key to be installed.

How It Works

The following is a high-level overview of how this feature works:

- The newly introduced CLI command, **diameter session-prioritization**, is used to enable or disable Gx signaling prioritization for eMPS sessions. This CLI command is at policy-control configuration in IMS-authorization service, and it is required to:
  - Exclude the eMPS session's Gx traffic from RLF throttling.
  - Exclude the eMPS session's Gx traffic from max-outstanding queue decisions.

  The following Gx signaling is excluded from RLF throttling and max-outstanding queue decisions:
  - All Gx signaling for an eMPS session.
  - Gx signaling related to eMPS upgrade/downgrade toggling which also includes inter-access technology handovers.
  - Gx signaling which is initiated as part of eMPS upgrade failure (UBRsp/CBRsp failures from access side).
- Support is added for parsing DRMP AVP from RAR and prioritizing corresponding RAA if the DRMP value is received as 0. This behavior is enabled by default and applicable to both eMPS and non-eMPS sessions, and independent of the diameter session-prioritization CLI command.
- **GTP Load Overload Throttling behavior**: The Cisco P-GW supports GTP Load Overload Throttling for both self-overload and peer-overload scenarios. However, GTP signaling for eMPS sessions should be excluded from throttling even under these conditions. For this prioritization to work, all the eARP values configured under eMPS profile must be configured under Load Overload profile configuration (for both self-overload and peer-overload). For additional eARP values configured under Load Overload profile configuration (self-overload and peer-overload), the legacy behavior of self-overload and peer-overload continues.

  If there is any change in the eARP values configured under eMPS profile configuration:

  1. For existing sessions:
     a. The new configuration is considered for eMPS upgrade/downgrade toggling, when there is any change in eARP value of existing bearer(s) of that session or at the time of bearer creation for that session.
     b. Till the session is marked eMPS, the legacy behavior of self-overload and peer-overload continues for the newly configured eARP values.
  2. For new sessions:
     a. New configuration takes effect seamlessly.

- Session recovery and ICSR recover the eMPS state of the session.
- As per Government Industry Requirements (GIR) document, eMPS marking is done only for P-GW EUTRAN and S4-SGSN PDNs.

Limitations

Following are the known limitations of the feature:

- When a session is marked eMPS, it will continue to be excluded from GTP throttling under GTP self-overload situation even after it has been downgraded to a non-eMPS session.
- If for a session, any Update Bearer Request or Create Bearer Request which can upgrade the session from non-eMPS to eMPS fails due to internal failure, the corresponding CCR-U may not be prioritized sometimes.

Configuring Gx Support for eMPS

This section provides information about the CLI commands available in support of the feature.

Configuring eMPS Profile

Use the following commands to configure eMPS profile, which is used to identify/mark a bearer/session as an eMPS bearer/session.

```
configure
  emps-profile emps_profile
    earp earp_value earp_value
    end
```

Important For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPS bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

Enabling Gx Prioritization for eMPS Sessions

Use the following commands under the Policy Control Configuration Mode to enable prioritization of Gx messages based on eMPS state of the session.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        [ no ] diameter session-prioritization
        end
```

Notes:

- By default, the **diameter session-prioritization** CLI command is disabled and Gx messages will not be prioritized based on eMPS value.
- If previously configured, use the **no diameter session-prioritization** CLI command to set the default behavior.
- The **diameter session-prioritization** CLI takes affect when Gx, along with eMPS profile, is enabled in the configuration.

Enabling GTP Prioritization for eMPS Sessions under GTP Load Overload Throttling

Use the following configurations for prioritizing the eMPS sessions related to GTP signaling, in case the GTP Peer Overload Control and/or Self-Protection configuration is enabled in the system. These configurations provide option to exclude eMPS session's GTP traffic from throttling under Peer Overload/Self Protection conditions.

```
configure
  emps-profile emps_profile_name
    earp earp_value earp_value
    end
```

```
configure
  gtpc-overload-control-profile overload_profile
    throttling-behavior earp earp_value earp_value exclude
    self-protection-behavior earp earp_value earp_value exclude
    end
```

Notes:

- **emps-profile** *emps_profile_name*: Configures eMPS profile for defining attributes of an eMPS session. The *emps_profile_name* is a string of size from 1 to 63.
- **earp**: Configures a maximum of 3 eARP priority level (PL) values so that sessions with configured eARP priority values can be marked as eMPS sessions. Maximum of 3 eARP values can be configured under an eMPS profile.
- As per above configuration, sessions with any one bearer with either eARP value will be excluded from Load Overload GTP Throttling.



Important For supplemental information related to GTP-C overload control throttling/self-protection behavior and configurations details, refer to the *3GPP R12 GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPs bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

For information related to configuration of Gx RLF Throttling and Gx max-outstanding queue, refer the *CLI Configuration Guide*.

Verifying the Gx Support for eMPS Configuration

This section provides information to verify the Gx Support for eMPS configuration.

show configuration

The output of this CLI command has been enhanced to display the following new field:

- diameter session-prioritization

show configuration verbose

The output of this CLI command has been enhanced to display the following new field:

- diameter session-prioritization

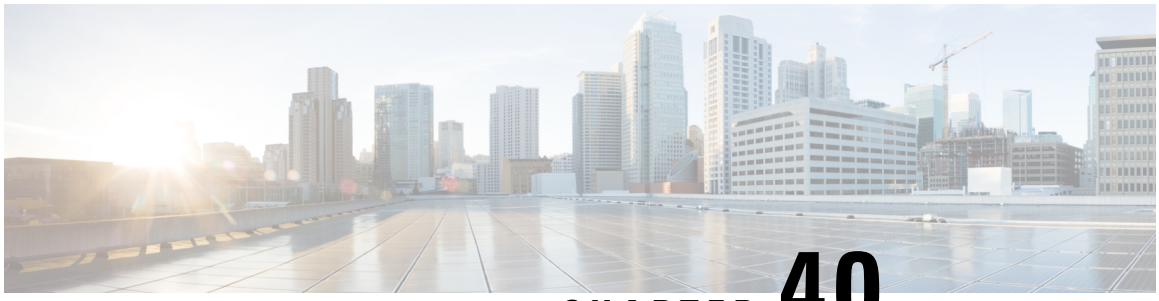
Monitoring and Troubleshooting the Gx Support for eMPS

This section provides information about CLI commands available to monitor and troubleshoot the feature.

show ims-authorization policy-control statistics

Use this CLI command to view statistics related to the number of prioritized DRMP messages. Following is a partial sample output:

```
show ims-authorization policy-control statistics

Rule Installation Failure:
  Resource Limitation:           0            Unknown Bearer ID:             0
  Invalid QCI:                   0            Invalid ARP:                   0
  Bearer-Id in QoS:              0            Parse Error:                   0
  Invalid Redirect Address:      0            ADC Absent:                    0
  Incorrect Metering Method:     0            Incorrect Rating Group:        0
  Incorrect Online AVP:          0            Incorrect Offline AVP:         0
  Incorrect Flow Status:         0            Incorrect Usage Monitoring AVP:0
  Incorrect Required Access Info:0            Incorrect Flow Description:     0
  Incorrect Reporting Level:     0

DRMP Statistics:
  RAR with P0 priority:          0            RAR with other priority:      2
```



CHAPTER 40

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 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.

- Feature Summary and Revision History, on page 753
- Introduction, on page 754
- Features and Terminology, on page 756
- Configuring Gy Interface Support, on page 796

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	PGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Related Changes in This Release	Not Applicable

Related Documentation	• *Command Line Interface Reference* • *PGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
Support is added for addition of server unreachable field in CDR.	21.27
First introduced.	21.22

Introduction

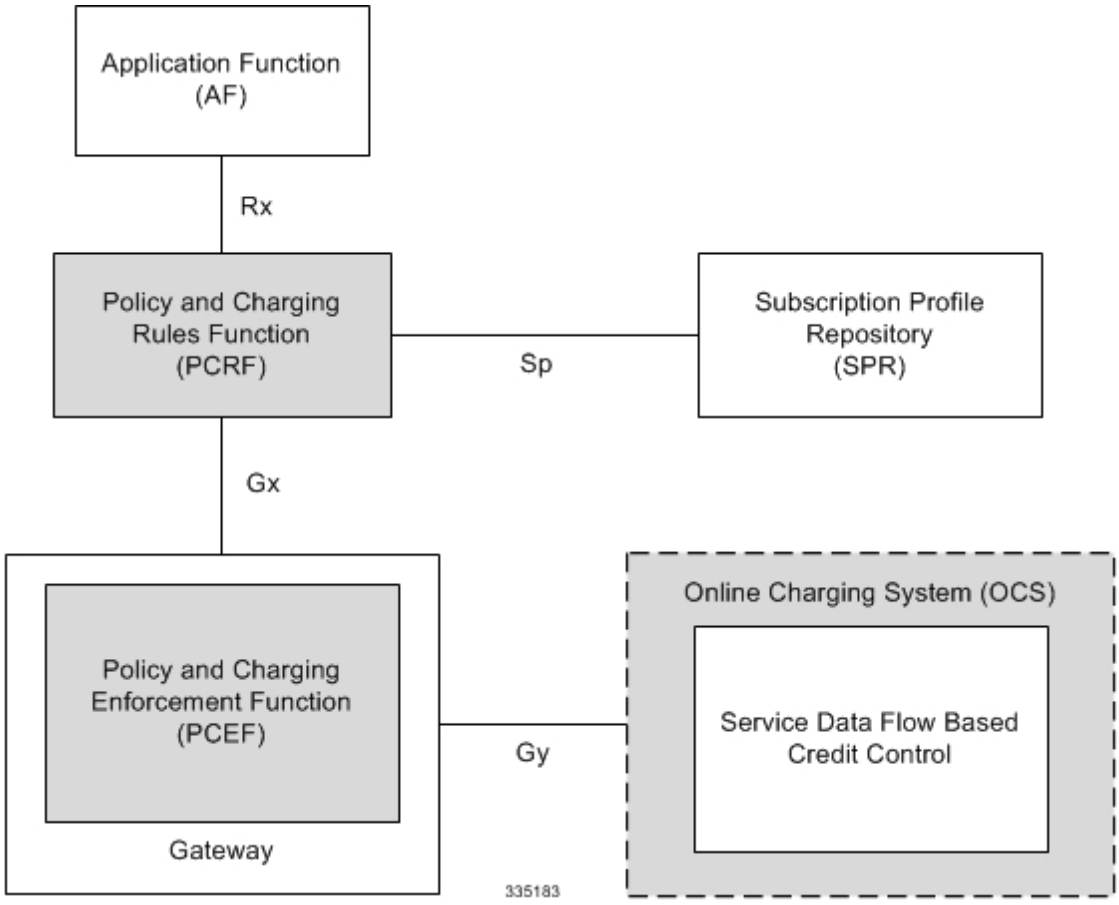
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

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.

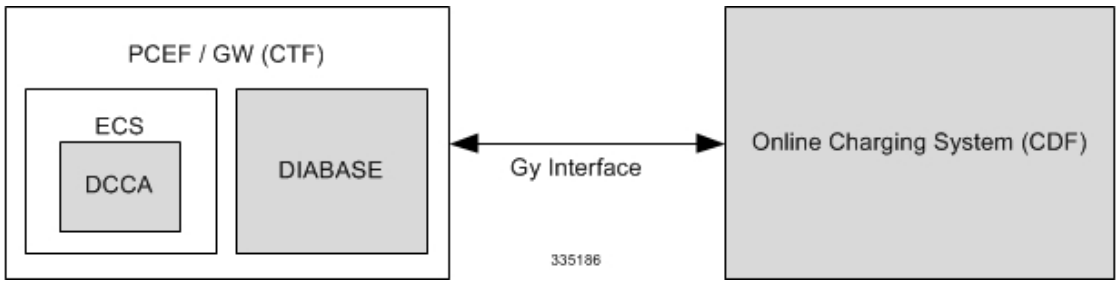
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 66: 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 67: 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.

  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.

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)

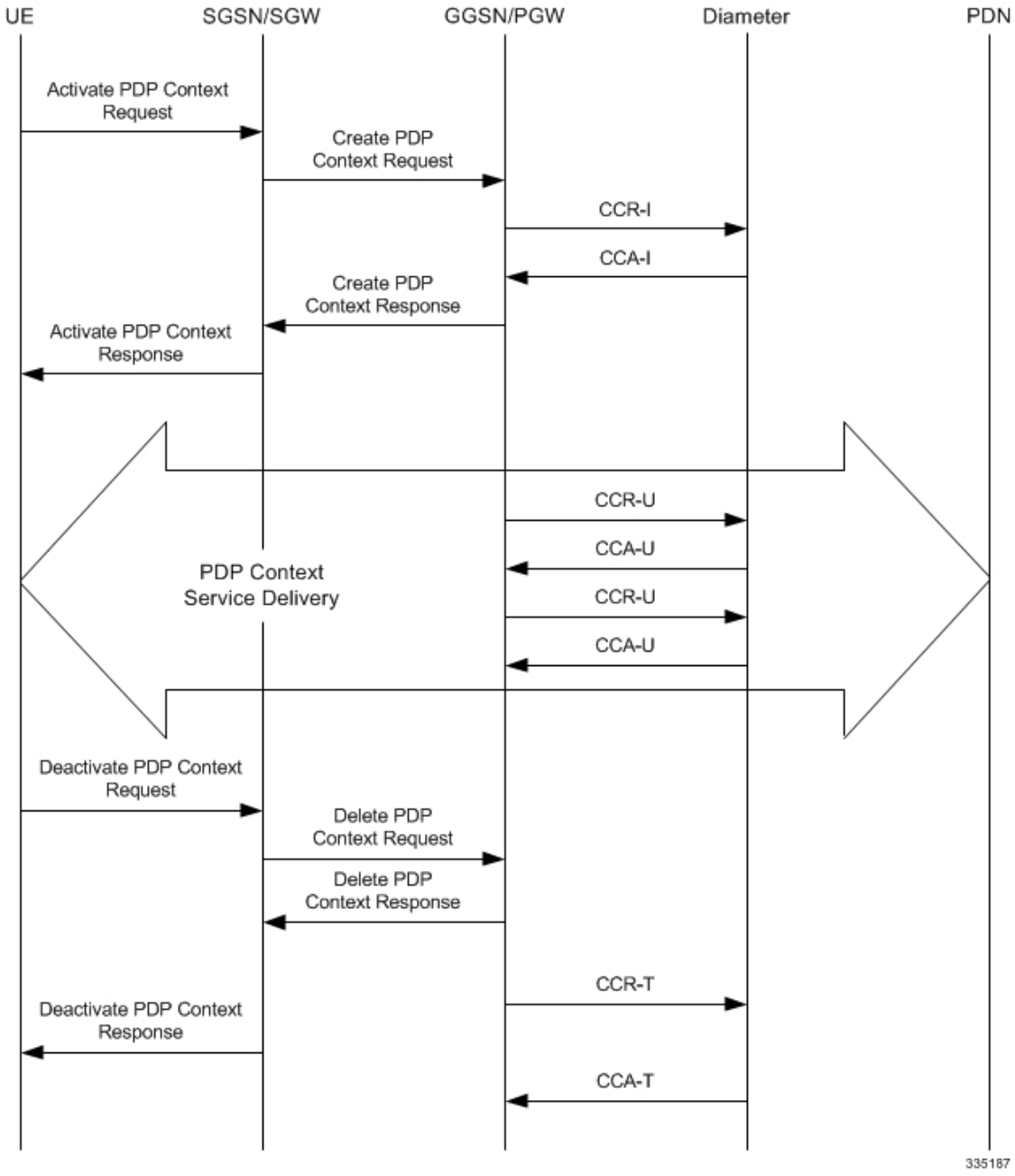
  If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.
- Credit Control Answer - Terminate (CCA-T)

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).

When the calls were terminated due to audit failure during ICSR switchover, DCCA allows generation of CCR-Ts over Gy interface.

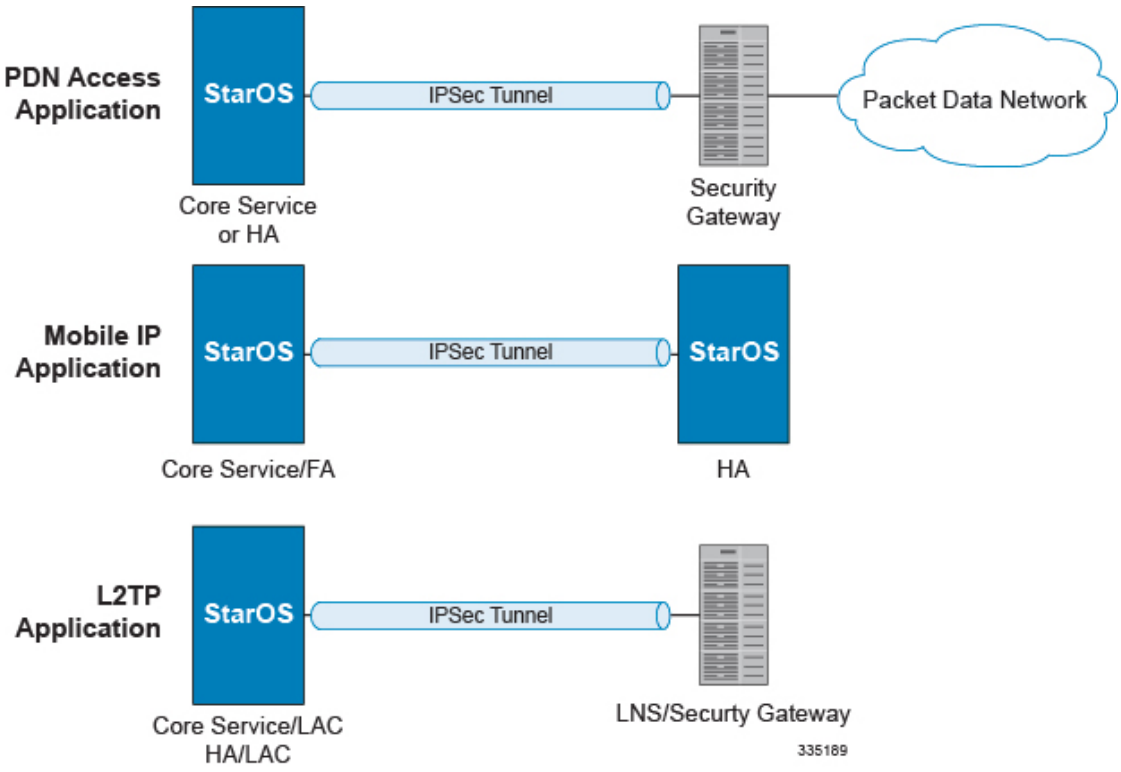
The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.

Figure 68: 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 69: 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.

Once CCR-U is sent out over Gy interface, the containers are cached only after CCA-U is received successfully. The Rf trigger is 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.

In the StarOS 21.20.22 release, support for Tariff-Time-Change AVP is enhanced to maintain continuous traffic flow in the fast path and the user's traffic rate when the Tariff-Time-Change AVP is received from Gy for a Rating Group.

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 767.

Credit Control Failure Handling

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

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

CCFH with Failover Supported

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

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

- Retry and Terminate: On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

CCFH with Failover Not Supported

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

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

Failover Support

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

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

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

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

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

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

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

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

Recovery Mechanisms

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



Important The DCCA supports maximum of three bearers (including default) for the ICSR Checkpointing and Recovery. When more than three bearers are configured in the DCCA, checkpointing occurs from Active to Standby for all the bearers. However, during recovery, only the first three bearers are recovered and the rest remain in the memory consuming resources.

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

Error Mechanisms

Following are supported Error Mechanisms.

Unsupported AVPs

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

Invalid Answer from Server

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

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

Result Code Behavior

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

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

Supported AVPs

The Gy functionality supports the following AVPs:

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

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

    Gy supports this AVP only in USU.
  - CC-Request-Number (AVP Code: 415)
  - CC-Request-Type (AVP Code: 416):

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

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

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

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

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

    Gy currently supports only URL (2) value.
  - Redirect-Server (AVP Code: 434)
  - Redirect-Server-Address (AVP Code: 435)
  - Requested-Service-Unit (AVP Code: 437)
  - Result-Code (AVP Code: 268)
  - Service-Context-Id (AVP Code: 461)

- Service-Identifier (AVP Code: 439)
- Subscription-Id (AVP Code: 443)
- Subscription-Id-Data (AVP Code: 444)
- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):

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

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

  Gy currently supports only IMEISV value.

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

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

- Envelope-Reporting (AVP Code: 1268)
- Envelope-Start-Time (AVP Code: 1269)
- GGSN-Address (AVP Code: 847)
- Offline-Charging (AVP Code: 1278)
- PDP-Address (AVP Code: 1227)
- PDP-Context-Type (AVP Code: 1247)

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

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

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

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

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

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

- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Auth-Application-Id (AVP Code: 258)
  - Destination-Host (AVP Code: 293)
  - Destination-Realm (AVP Code: 283)
  - Disconnect-Cause (AVP Code: 273)

- Error-Message (AVP Code: 281)
- Event-Timestamp (AVP Code: 55)
- Failed-AVP (AVP Code: 279)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Origin-Host (AVP Code: 264)
- Origin-Realm (AVP Code: 296)
- Origin-State-Id (AVP Code: 278)
- Redirect-Host (AVP Code: 292)
- Redirect-Host-Usage (AVP Code: 261)
- Redirect-Max-Cache-Time (AVP Code: 262)
- Rating-Group (AVP Code: 432)
- Result-Code (AVP Code: 268)
- Route-Record (AVP Code: 282)
- Session-Id (AVP Code: 263)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control

- Currency-Code (AVP Code: 425)
- Direct-Debiting-Failure-Handling (AVP Code: 428)
- Exponent (AVP Code: 429)
- G-S-U-Pool-Identifier (AVP Code: 453)
- G-S-U-Pool-Reference (AVP Code: 457)
- Requested-Action (AVP Code: 436)
- Service-Parameter-Info (AVP Code: 440)
- Service-Parameter-Type (AVP Code: 441)
- Service-Parameter-Value (AVP Code: 442)
- Unit-Value (AVP Code: 424)
- Value-Digits (AVP Code: 447)

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

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

- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applic-Info
- 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.

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.

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.

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.

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.

Addition of Server Unreachable Field in CDR

Feature Description

When the Online Charging System (OCS) sends negative messages, transport connection fails between the Policy and Charging Enforcement Function (PCEF) and the OCS. The connection error causes session establishment failure and prevents subscribers from the use of services. The following procedures are used to overcome the connection errors:

- **Failure Handling (FH)**: The exisiting FH mechanism operates if the diameter session failover is present, allows the system to choose whether to continue the session and convert to offline, or to terminate the session when a connection or message-level error occurs.
- **Server Unreachability (SU)**: This failure handing mechanism provides more granular control over failure procedures. In addition to the session after the message- and connection-level (transport) failures,

this mechanism is used when the responses are slow from the OCS. It also provides the options to either continue the session for a specific time duration or quota exhaustion before termination.

To use the configured server and interim quota (volume and time), SU retries before a session is converted to offline or gets terminated.

When **gtpp attribute servers-unreachable** is configured under gtpp group and the SU feature is enabled then, serversUnreachableContinue or serversUnreachableTerminate in interim or final CDR allows the following process flow:

1. SU failure is triggered.
2. CDR is generated.
3. Based on the SU configuration in Call Control Profile, the generated CDR contains the serversUnreachableContinue or serversUnreachableTerminate fields.

The following table describes the serversUnreachable fields in the CDR.

Table 81: ServersUnreachable Fields in CDR

Field Name	Description	Tag	Format	Size	ASN1 Code
serversUnreachableContinue	When servers unreachable procedure is executed, element is present.	256	Boolean	1	0x9f8200
serversUnreachableTerminate	When servers unreachable procedure is executed, element is present.	257	Boolean	1	0x9f8201

Table 82: ServersUnreachable CDR Fields in ACS Configuration

SU Configuration	SU Detected Fields during Interim State	SU Detected Fields After End of Interim State	SU not Detected Fields (normal call with Gy)
server-unreachable initial-request terminate	When a CDR field is triggered differently, do not include the SU terminate field since it is an interim CDR • **SU continue** is **FALSE** • **SU Terminate** is **FALSE** in final CDR	• **SU continue** is **FALSE** • **SU Terminate** is **TRUE** in final CDR	• **SU continue** is **FALSE** • **SU Terminate** is **FALSE** in final CDR

server-unreachable update-request terminate	When a CDR field is triggered differently, do not include the SU terminate field since it is an interim CDR • **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR
server-unreachable initial-request continue	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR
server-unreachable update-request continue	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR

For more information, refer to the Gy chapter in the *PGW Administration Guide*.

Adding Server Unreachable Field in CDR

Use the following configuration commands to add the server unreachable field in CDR:

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute servers-unreachable
      end
```

NOTES:

- **gtpp attribute servers-unreachable**: Specifying this option includes the optional field **ServersUnreachablesContinue** or **ServersUnreachablesTerminate** in the CDR.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature using show commands.

Show Commands and Outputs

This section provides information regarding show command and their outputs in support of this feature.

show gtpp group name <group name>

Field	Description
Servers Unreachable present	Displays "Yes" or "No" to indicate the presence of servers unreachable element.

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.

CPU utilization is very high if the max-outstanding count is low and network is congested.

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. 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.

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, on page 788
- Configuring CC based Selective Gy Session Control, on page 789
- Monitoring and Troubleshooting the Selective Gy Session Control Feature, on page 790

Feature Description

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. Now, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The **cc profile** *cc-profile-index* **prepaid prohibited** CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging characteristic is selected and used. If there is no matching charging characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

Diamter Error Code and Counters

SaMOG supports Diameter error code counters for all transactions and diameter interfaces on SaMOG (Web-auth) services through P-GW LBO module on various StarOS platforms ASR5500/ASR5700.

The following set of result code specific counters are available for the responses received from the OCS (Online Charging System), on Gy interface. DCCA (Diameter Credit Control Application) is the protocol used on the Gy interface.

Table 83: Result Code Specific Counters

Error Category	Result Code	Result Code Value
Transient Failures [4XXX]	DIAMETER_END_USER_SERVICE_DENIED	4010
	DIAMETER_CREDIT_LIMIT_REACHED	4012
Permanent Failures [5XXX]	DIAMETER_RATING_FAILED	5031

Relationships to Other Features

This feature can also be used when the CC profile configuration is enabled through the GGSN service. When the CC profile is configured under APN service and GGSN service, the prepaid prohibited configuration for the matching CC profile is applied irrespective of the services.

Limitations

The following are the limitations of this feature:

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session-setup. Once the credit-control-group is selected (after session setup), this feature is not applicable.

Configuring CC based Selective Gy Session Control

The following sections provide the configuration commands to configure the Gy Session Control feature based on the CC profile of the subscriber.

Configuring CC Value

The following commands are used to configure Charging Characteristic values as postpaid/prepaid to disable/enable Gy session towards the OCS.

```
configure
   context context_name
      apn apn_name
         cc-profile { cc_profile_index | any } { prepaid-prohibited |
credit-control-group cc_group_name }
         end
```

Notes:

- *cc_profile_index*: Specifies the CC profile index. *cc_profile_index* must be an integer from 0 through 15.
- **any**: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring **any** keyword will not override other specific configurations under APN.
- **prepaid-prohibited**: Disables prepaid Gy session for the configured profile index.
- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

- **no cc-profile** *cc_profile_index*: This command falls back to "any" cc-profile behavior irrespective of the CC profile index value configured.

Verifying the Selective Gy Session Control Configuration

Use the following command in Exec mode to display/verify the configuration of Selective Gy Session Control feature.

```
show configuration
```

Monitoring and Troubleshooting the Selective Gy Session Control Feature

This section provides information regarding show commands and/or their outputs in support of the Selective Gy Session Control feature.

show active-charging sessions

The "Credit-Control" field that appears as part of the **show active-charging sessions [callid | imsi | msisdn]** command output enables the user to determine the credit control state as "On" for online charging enabled session or "Off" for prepaid prohibited session and monitor the subscriber session.

Credit-Control Group in Rulebase Configuration

This section describes the overview and implementation of the Credit-Control (CC) Group Selection based on the rulebase of the subscriber.

This section discusses the following topics for this feature:

- Feature Description, on page 790
- Configuring Credit-Control Group in Rulebase, on page 791
- Monitoring and Troubleshooting the CC-Group Selection in Rulebase, on page 792

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. Now, the CC group selection functionality is extended to rulebase configuration.

This feature is explicitly required in scenarios where IMSA was not used, AAA server could not send CC group during authentication, and only a single APN/subscriber-profile was used for all the subscribers. In such situations, this feature targets to provide a premium CC group within rulebase to enable premium treatment to subscribers based on their types.

This feature introduces a new configurable option inside the rulebase configuration, so that the users can specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This configured CC group overrides or has a higher priority than the CC group configured within the subscriber profile/APN. If the AAA or PCRF server sends the CC-Group AVP, the CC group value defined through the AVP overrides the rulebase configured CC group.

When this feature is enabled, the configuration allows specifying an association between the rulebase name and the CC group so that when a premium subscriber connects, a premium rulebase and a premium CC group are selected.

Important Mid-session configuration change will not impact the existing subscribers in the system. This configuration change will be effected only to the new sessions.

Implementing this new configuration option enables different types of Assume-Positive behavior for subscribers based on the available quota. This results in achieving preferential treatment for premium customers.

The precedence order for selection of the CC group is defined as:

- PCRF provided CC group
- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

Important This feature should not be used when there is an option for AAA server to send the CC group during authentication process. If during the authentication, AAA server sends a CC group, and the rulebase selected has a CC group defined within, then the rulebase defined CC group is selected for the session.

Limitations

There are no limitations or restrictions with this feature. However, it is important to keep in mind the precedence order for CC group selection.

Configuring Credit-Control Group in Rulebase

The following sections provide the configuration commands to configure the Credit-Control Group based on the rulebase of the subscriber.

Defining Credit-Control Group

The following commands are used to configure a desired Credit-Control group name when using the rulebase selected by PCRF.

```
configure
require active-charging
active-charging service service_name
   rulebase rulebase_name
      credit-control-group cc_group_name
      end
```

- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

- **no credit-control-group**: Removes the previously configured CC group from the rulebase configuration. This is the default setting.
- This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.
- This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers.
- If this CLI command is configured, the selection of the CC group will be based on the precedence order. That is, the rulebase defined CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.
- If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

Verifying the Credit-Control Group Configuration

Use the following command in Exec mode to display/verify the configuration of CC group in rulebase.

```
show configuration verbose
```

Monitoring and Troubleshooting the CC-Group Selection in Rulebase

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

show active-charging sessions full

The output of this show CLI command displays the selected credit-control-group for the session. The output details are useful in verifying and troubleshooting the issues with this feature.

show configuration errors

This show CLI will list an error if the credit-control group that is configured inside the rulebase is not defined.

show configuration verbose

This command will show the "credit-control-group" option specified for the rulebase. For troubleshooting purpose, capture the output of **show configuration verbose** and **show subscribers full** along with the **monitor-protocol** output containing "Radius Access-Accept".

Combined CCR-U Triggering for QoS Change Scenarios

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. Upon receiving the Online AVP from PCRF, the gateway will establish the Gy session.

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:

Procedure

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 796 and Configuring HA / PDSN Gy Interface Support, on page 797.

Step 3 Configure Event-based Gy support as described in Configuring PLMN and Time Zone Reporting, on page 799.

Step 4 *Optional.* Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in Configuring Server Unreachable Feature, on page 800.

Step 5 *Optional.* Configure Static Rulebase for CCR as described in Configuring Static Rulebase for CCR, on page 801.

Step 6 *Optional.* Configure Gy for GTP based S2a/S2b as described in Configuring Gy for GTP based S2a/S2b, on page 801.

Step 7 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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

Configuring GGSN / P-GW / IPSG Gy Interface Support

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

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
               origin host <diameter_host> address <ip_address>
               peer <peer> realm <realm> address <ip_address>
               exit
          exit
     active-charging service <ecs_service_name>
          credit-control [ group <cc_group_name> ]
               diameter origin endpoint <endpoint_name>
               diameter peer-select peer <peer> realm <realm>
               diameter pending-timeout <timeout_period>
               diameter session failover
               diameter dictionary <dictionary>
               failure-handling initial-request continue
               failure-handling update-request continue
               failure-handling terminate-request continue
               exit
          exit
     context <context_name>
           apn <apn_name>
               selection-mode sent-by-ms
               ims-auth-service <service>
               ip access-group <access_list_name> in
               ip access-group <access_list_name> out
               ip context-name <context_name>
               active-charging rulebase <rulebase_name>
               credit-control-group <cc_group_name>
               end
```

Notes:

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

Configuring HA / PDSN Gy Interface Support

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

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
```

```
                origin host <diameter_host> address <ip_address>
                peer <peer> realm <realm> address <ip_address>
                exit
          exit
     active-charging service <ecs_service_name>
          ruledef <ruledef_name>
                ip any-match = TRUE
                exit
          charging-action <charging_action_name>
                content-id <content_id>
                cca charging credit rating-group <rating_group>
                exit
          rulebase <rulebase_name>
                action priority <action_priority> ruledef <ruledef_name>
charging-action <charging_action_name>
                exit
          credit-control [ group <cc_group_name> ]
                diameter origin endpoint <endpoint_name>
                diameter peer-select peer <peer> realm <realm>
                diameter pending-timeout <timeout>
                diameter session failover
                diameter dictionary <dictionary>
                failure-handling initial-request continue
                failure-handling update-request continue
                failure-handling terminate-request continue
                pending-traffic-treatment noquota buffer
                pending-traffic-treatment quota-exhausted buffer
                exit
          exit
     context <context_name>
          subscriber default
                ip access-group <acl_name> in
                ip access-group <acl_name> out
                ip context-name <context_name>
                active-charging rulebase <rulebase_name>
                credit-control-group <cc_group_name>
                end
```

Notes:

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

Configuring PLMN and Time Zone Reporting

PLMN and Time Zone Reporting feature requires a credit-control group to be defined in the APN or subscriber configuration or there must be a default credit-control group configured. The following CLI commands are available to enable/disable PLMN and Time Zone Reporting feature.

To enable PLMN and Time Zone Reporting through subscriber-template, use the following configuration:

```
configure
     context <context_name>
          subscriber name <subscriber_name>
               dns primary <primary_ipaddress>
               dns secondary <secondary_ipaddress>
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Notes:

- The **credit-control-client event-based-charging** command should be used to enable PLMN and Time Zone Reporting.

  For more information on configuring PLMN and Time Zone Reporting feature, refer to the *Command Line Interface Reference*.

To enable PLMN and Time Zone Reporting through APN template, use the following configuration:

```
configure
     context <context_name>
          apn <apn_name>
               selection-mode sent-by-ms
               accounting-mode none
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               ip address pool name<pool_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Rest of the parameters needed for Event-based Gy such as dictionary, endpoint will be picked from the credit-control group.

In a scenario where the triggers are configured through the CLI command and another set of triggers are also received from Gx, then the triggers from Gx will have a higher priority.

Configuring Server Unreachable Feature

The Server Unreachable feature requires a failure handling behavior to be defined in the Diameter Credit Control configuration. The following CLI commands are available to enable/disable OCS Unreachable Failure Handling feature.

To enable OCS Unreachable Failure Handling feature, use the following configuration:

```
configure
require active-charging
         active-charging service <service_name>
              credit-control
                   servers-unreachable { initial-request | update-request
 } { continue | terminate }  [ { after-interim-volume <bytes> |
after-interim-time <seconds> } +   server-retries <retry_count> ]
                  servers-unreachable behavior-triggers { initial-request
 | update-request } transport-failure [ response-timeout | tx-expiry ]
                   servers-unreachable behavior-triggers initial-request
 { result-code { any-error | result-code [ to end-result-code ] } }
                   servers-unreachable behavior-triggers update-request
{ result-code { any-error | result-code [ to end-result-code ] } }
                  end
```

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

Notes:

- This CLI command "**servers-unreachable { initial-request | update-request } { continue | terminate } [{ after-interim-volume ...**" allows configuring interim-volume and interim-time in the following ways:
  - after-interim-volume <bytes> alone followed by server-retries.
  - after-interim-time <secs> alone followed by server-retries.
  - after-interim-volume <bytes> after-interim-time <secs> followed by server-retries.
- This CLI command "**servers-unreachable behavior-triggers**" is used to trigger the servers-unreachable failure handling at either Tx expiry or Response timeout (This CLI is similar to retry-after-tx-expiry in "**failure-handling update-request continue retry-after-tx-expiry**" command.).
- This CLI command "**servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }**" is used to trigger the servers-unreachable failure handling based on the configured Diameter error result codes.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Static Rulebase for CCR

To allow static configuration of rulebase name to be passed to OCS via CCR message, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              charging-rulebase-name rulebase_name
              no charging-rulebase-name
              end
```



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

Notes:

- By default, the rulebase obtained from APN/subscriber template will be sent to OCS through the CCR message.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Gy for GTP based S2a/S2b

To provide Gy Support for WiFi integration in P-GW for GTP based S2a/S2b, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              diameter update-dictionary-avps 3gpp-rel11
              [  default | no ] diameter update-dictionary-avps
              end
```

Notes:

- **3gpp-rel11**: Provides support for 3GPP Rel.11 specific AVPs in the standard Gy dictionary.

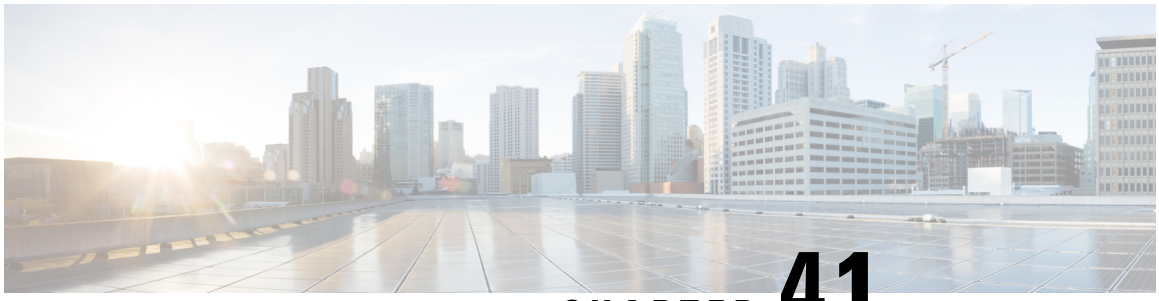
Gathering Statistics

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

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

Statistics/Information	Action to perform
Complete statistics for ECS sessions.	**show active-charging sessions full**

Statistics/Information	Action to perform
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*> **]**



CHAPTER 41

Gy Failure Handling Enhancement

- Feature Summary and Revision History, on page 803
- Feature Description, on page 804
- How It Works, on page 804
- Configuring Gy Failure Handling, on page 805
- Monitoring and Troubleshooting the Gy Failure Handling, on page 805

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

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

Revision Details	Release
A new option to continue the session, but drop the traffic, is introduced in the FH-template that is associated with a Credit Control Group. An existing CLI command is enhanced to enable the feature.	21.3
First introduced.	Pre 21.2

Feature Description

In releases prior to 21.3, the Gy failure-handling-template (FH-template) had no option to block the chargeable traffic while retaining the PDN session.

In 21.3 and later releases, "continue discard-traffic" option has been added to Gy failure-handling-template to block the chargeable traffic while retaining the PDN session.

How It Works

This section provides a brief overview of how this feature works:

- A new option to continue the session, but drop the traffic, is introduced in the FH-template that is associated with a Credit Control Group. An existing CLI command is enhanced to enable the feature.
- When the "continue discard-traffic" FH action is enforced, all traffic is blocked for the given DCCA session. The DCCA session refers to the PDN (and all bearers therein) or to a specific bearer. The matching bearers a DCCA session corresponds to, continues as it is for FH action "continue". Only the traffic that requires online charging is dropped.
- The "continue discard-traffic" status remains enforced unless a Rule modification or installation is received from the PCRF for a pure dynamic rule. The online AVP (online = 1) is sent eventually from the PCRF which resumes the Gy session for the given bearer (sub session). This behavior is based on the "offline-session re-enable" CLI that is available in the credit-control-group configuration mode.
- All traffic that requires online-charging is dropped.
- The charging action is identified and only if the charging action requires "online" charging, the corresponding drop action is taken.
- The "continue discard-traffic" status on a subscriber remains as is post recovery. Traffic is blocked after recovery as long as Gx does not re-enable the Gy session.



Note

- The **Gy Failure Handling Enhancement** feature works along with the *OCS Failure Reporting to PCRF* (introduced in Release 21.0) and the *Enhancement to OCS Failure Reporting for Gy* (introduced in Release 21.2) features. Refer to the respective *Release Change Reference* for additional information.
- When the CCFH/FH-Template is configured with Continue action (or this new FH-Template “continue-discard”) and the corresponding action is being taken, then the reporting to the PCRF happens as per the *OCS Failure Reporting to PCRF* feature.

Configuring Gy Failure Handling

Use the following commands under the Diameter Failure Handling Template Configuration Mode to discard data traffic while retaining the subscriber session.

```
configure
  failure-handling-template template_name
    msg-type { credit-control-initial | credit-control-terminate |
credit-control-update } failure-type any action continue discard-traffic
    end
```

Notes:

- Use the **msg-type { credit-control-initial | credit-control-terminate | credit-control-update } failure-type any action continue discard-traffic** CLI command to specify the behavior if there is a communication failure with the prepaid server. If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.
- The enhancement of "discard-traffic" is added to action "continue". This blocks data traffic while retaining the subscriber session.
- If previously configured, use the **no msg-type { credit-control-initial | credit-control-terminate | credit-control-update } failure-type any** CLI command to remove the configuration associated with the failure handling template.
- The "discard-traffic" keyword can only be configured along with "continue" action, and it takes affect when the respective failure occurs.
- This CLI option is disabled by default. The "discard-traffic" keyword needs explicit configuration if the respective discard action is desired.

Monitoring and Troubleshooting the Gy Failure Handling

This section provides information regarding monitoring and troubleshooting the feature.

Gy Failure Handling Show Command(s) and/or Outputs

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

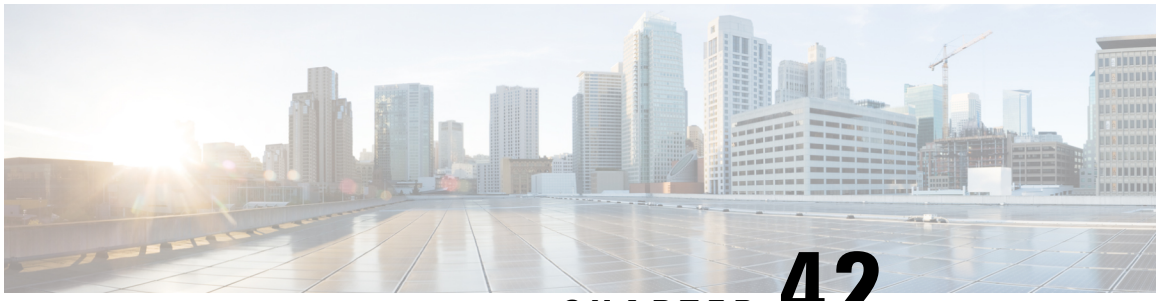
show active-charging credit-control statistics

The output of this show command has been enhanced to display the following new field in support of this feature:

- Action-Drop:

Following is a partial sample output:

```
Failure Handling Stats:
      Action-Terminated:       0            Action-Continue:         0
      Offline Active Sessions: 0            Action-Drop:             0
```



CHAPTER 42

Gy Interface Specification for Compliance 2019

- Feature Summary and Revision History, on page 807
- Feature Description, on page 808
- How It Works, on page 808
- Configuring Presence Reporting Area, on page 810
- Multiple Subscription ID, on page 810
- Configuring Extended Bandwidth QoS, on page 811
- Show Command and Output, on page 811

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.23

Feature Description

This feature adds support for the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards for Gy interface.

The Presence Reporting Area is an area defined within the 3GPP packet domain for reporting of UE presence within that area. This is required for policy control and in charging scenarios.

Currently, when the PRA information is received, P-GW forwards the Presence Reporting Area Information to the PCRF and this information is not being sent to OCS(Gy).

Following are the specific requirements to support specific Gy interface in P-GW:

1. Presence reporting status : Upon receiving Trigger-Type 73 in CCA-I, P-GW will send Presence-Reporting-Status in CCRU/T towards OCS whenever there is PRA status change reported through S-GW
2. Extended QoS parameters to be sent in CCR messages towards OCS as part of QoS-Information AVP
3. Enhanced-Diagnostics AVP in CCR-T: Report RAN-NAS-Release-Cause Only in CCR-T
4. Support for Multiple Subscription-ID-E.164 ,IMSI and NAI

How It Works

1. The following procedure describes the PRA supporting for Gy interface and its associated behavior:

   During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA is required for an IP-CAN session. Then the PCRF determines based on the subscriber's profile configuration and the supported AVP features. The parameter CNO-ULI is set for the same. For the IP-CAN session reporting, the PCRF provides Presence-Reporting-Area-Information AVP, which contains the PRA identifier within the Presence-Reporting-Area-Identifier AVP to the PCEF. For a UE-dedicated PRA, the PCRF provides the list of elements consisting of the PRA within the Presence-Reporting-Area-Elements-List AVP to the PCEF. Presence-Reporting-Area-Elements-List is not currently supported. The PCRF subscribes to the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) event trigger at the PCEF at any time during the entire IP-CAN session to activate the reporting changes of the UE presence in the PRA.

   For the same IP-CAN session, the OCS can also determine if the UE presence requires any updates to OCS in Presence-Area-Information AVP. To support this, you must enable the 'trigger pra' config. OCS must send the Trigger-type CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA (73) in Trigger AVP as part of CCA-I towards PGW. The OCS also sends the Presence-Reporting-Area-Identifier in CCA-I (the assumption is that it will same as the PRAID sent from PCRF). PRA reports are then sent towards OCS.

   Upon receiving Trigger-Type 73 in CCA-I, PGW will send Presence-Reporting-Status in CCRU/T towards OCS whenever there is PRA status change reported through S-GW. Presence reporting support is already available for updating Presence Action Start/Stop towards S-GW in CSReq for the Gx interface. For the Gy interface, the same control plane infrastructure is used. A new trigger type is introduced under credit control for the Gy interface so that Trigger Type

-CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA(73) is processed in CCA messages sent from OCS.

When the trigger type CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA (73) is enabled over Gy interface, PRA-IDs are sent to PGW in CCA-I/CCA-U. Whenever there is a PRA status change(MBReq with PRA change), the CCR-U with PRA information AVP is sent to OCS as well.

When the session ends, CCR-T has the PRA information AVP along with the details of the latest PRA-ID and status. At this time the assumption is that Gx and Gy sides would subscribe to the same PRA-ID since it is for the same session. It is also assumed that Gy side subscribe/unsubscribe for a PRA-ID session would not send PRA Start/Stop in CSReq towards SGW since it is already handled from the Gx side. Gy side would only keep a record of PRA-ID for which the presence reporting needs to be sent to the OCS server or not.

2. Extended QoS parameters to be sent in CCR messages towards OCS as part of QoS-Information AVP

   Following extended parameters must be included in the QoS-Information AVP sent to OCS:

   a. Extended-Max-Requested-BW-UL
   b. Extended-Max-Requested-BW-DL
   c. Extended-GBR-UL
   d. Extended-GBR-DL
   e. Extended-APN-AMBR-UL
   f. Extended-APN-AMBR-DL

   When the PCRF has programmed Extended QOS parameters for a particular subscriber, the Extended QOS parameters needs to be sent to OCS in CCR message. The new AVPs sent as part of CCR-Initial/update/Terminate is applicable as per policy updated from PCRF for the specific subscriber.

   ACSMGR has infomation on QoS parameters for the bearer and this is used to send information to DCCA and ultimately OCS server.

3. Enhanced-Diagnostics AVP in CCR-T: Report RAN-NAS-Release-Cause Only in CCR-T

   The Enhanced-Diagnostics AVP (AVP code 3901) is sent in CCR-T message towards OCS and complements the Change-Condition AVP for Offline Charging from PCN Nodes. The RAN-NAS-Release-Cause AVP is under a grouped AVP to allow extensions to other types of release causes in the future.

4. Support for Multiple Subscription-ID - E.164 ,IMSI and NAI

   Multiple subscription ID enables required for various service types under Credit Control Configuration.

   Currently, Multiple subscription ID AVP is encoded in the Gy CCRs based on dictionary and service-type checks. With the subscription ID AVP, customers will have the provision of enabling required Subscription-Id types for various services.

   Each service can have a maximum of three Subscription-Id types (for example: E164, IMSI and NAI) and the advantage of this Multiple subscription ID is that any further dictionary additions in DCCA can be minimized.

Configuring Presence Reporting Area

This section provides information on configuration commands available in support of this feature:

- Configuring PRA (cno-uli) for Gx
- Configuring PRA for Gy

Configuring PRA (cno-uli) for Gx

Use the following configuration commands to enable the PRA:

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        { default | no }diameter encode-supported-features cno-uli
  end
```

Configuring PRA for Gy

Use the following configuration commands to enable trigger-type PRA:

```
configure
  active-charging service service_name
    credit-control group group_name
      trigger-type pra
  end
```

NOTES:

- **pra**: Configures change in ue presence in presence reporting area.

Multiple Subscription ID

Use the following configuration commands to enable the Subscription-Ids for various service types:

```
configure
  active-charging service service_name
    credit-control-group group_name
      subscription-id service-type closedrp ( e164 | imsi | nai }
  end
```

For an instance, if a customer wants E.164, IMSI and NAI value to be encoded in Gy CCR for P-GW service, then the below CLI should be configured in the Credit Control Configuration mode.

```
subscription-id service-type pgw e164 imsi nai
```

NOTES:

- **subscription-id**: Configures Credit Control subscription-ids for service-types.
- **service-type**: Configures Credit Control subscription-ids based on service-types.
- **closedrp**: Configures subscription-id for closedrp service.

Configuring Extended Bandwidth QoS

Use the following configuration commands in Policy Control Configuration to enable the Extended Bandwidth QoS:

```
configure
          context context_name
             ims-auth-service ims_auth_service_name
               policy-control
                  [ no ]diameter encode-supported-features
extended-bw-newradio
     end
```

Show Command and Output

show active-charging sessions full all

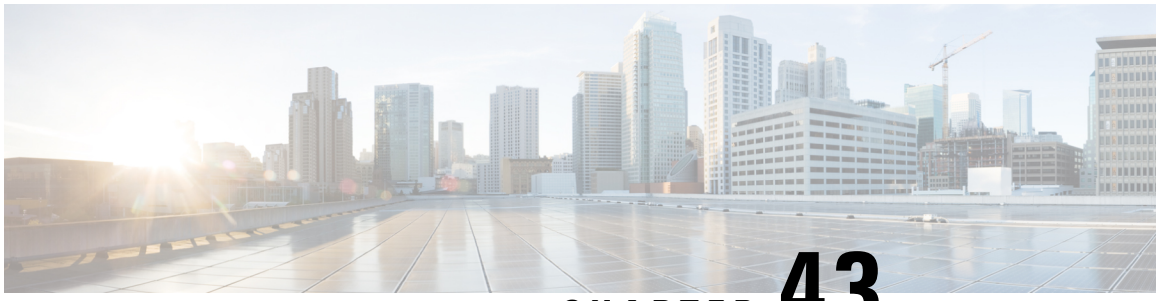
The following new field is displayed to the output of this command:

- Pending Triggers: pra

show active-charging service all | grep pra

The following new fields are displayed to the output of this command:

- Service name
- Credit Control
  - Trigger type:pra



CHAPTER 43

HSS and PCRF Based P-CSCF Restoration Support

This feature enables support for HSS-based and PCRF-based P-CSCF restoration that helps to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure.

- Feature Description, on page 813
- How It Works, on page 814
- Configuring the HSS/PCRF-based P-CSCF Restoration, on page 823
- Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration, on page 825

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 includes 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.

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. 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 P-GW 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.

Emergency PDN HSS based P-CSCF Restoration for S5/S8 will be performed if CLI is configured at P-GW service to support the restoration for emergency PDNs.

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 P-CSCF Restoration extension mechanism during P-CSCF ReDiscovery with P-CSCF FQDN, local DNS cache will be queried first. If FQDN is already present in local DNS cache, then DNS query will not be sent out to the DNS server and P-GW will immediately get the DNS response.

  Since local DNS cache flush will not be done, operator should configure the cache accordingly.

Licensing

Use of P-CSCF Restoration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

How It Works

- Restoration is supported for IPv4/IPv6/IPv4v6 calls.
- With extension, Restoration Support UBR will always go on default bearer.

- P-GW does not compare any of the stored values with the new updated P-CSCF IP addresses; it relies on the DNS provided/discovered values and forwards the P-CSCF IP addresses as is.
- P-CSCF Restoration will be performed for all PDN connections, regardless of APN configuration of IMS/non-IMS.
- Upon receiving P-CSCF Restoration trigger for extended mechanism, P-CSCF address discovery priority is first for P-CSCF FQDN. If FQDN is already present in DNS cache, then as per current implementation of HSS based (S5/S8) P-CSCF Restoration, DNS query will not be sent to the DNS server and P-GW will immediately get the DNS response.

  Since local DNS cache flush will not be done, operator should configure the cache accordingly.
- In case of S6b RAR, P-GW supports configuration for whether to perform ReAuthentication Request and Response (AAR/AAA) with extended restoration support.

  Authentication after RAR for restoration is not mandatory as it increases the authentication signaling flow at AAA Server. In order to maintain backward compatibility with the existing Diameter Relay Agents (DRA)/AAA servers, which expect authentication after RAR, authentication can be configured for RAR with P-CSCF Restoration.
- If the DNS resolution for FQDN fails or P-GW does not have P-CSCF address configured in any other way, P-GW will still send UBR with no P-CSCF address PCO/APCO during restoration.
- If the P-CSCF Restoration is already in progress, then restoration will not be performed again for any second restoration indication received.
- For basic P-CSCF Restoration, call will be cleared with disconnect reason "ue-pcscf-reselect-not-supported (613)".
- P-GW does not expect change in S6b P-CSCF FQDN during ReAuth. In the rare scenario that P-CSCF FQDN is changed in S6b ReAuth, then the new FQDN will be used in next P-CSCF Discovery. If P-CSCF FQDN if changed during ReAuth, then it is not recovered.
- For S6b, every AAR supported-feature will be negotiated. ReAuth AAR will also do the feature renegotiation. It’s expected that S6b AAA server should do the renegotiation in every AAA. This is specifically applicable to LTE-WiFi and vice versa handoff. During LTE attachment, supported-feature will not be sent. During WiFi handoff, however, support for P-CSCF Restoration should be indicated in AAR.
- Supported-feature on Gx for P-CSCF Restoration will apply to GGSN/eHRPD calls as well to support handoff scenarios.
- For S6b RAT type WLAN, AAA group supports configuration to control when AAR is sent with the supported-feature to S6b server. If AAA group disables this functionality, then once the AAA response comes with supported-feature it is considered not negotiated. Thus, negotiation depends on the CLI configuration of supported-feature at the time of handling AAA.
- Supported-feature for P-CSCF Restoration in S6b will only go for RAT type WLAN.
- During IPv6 reporting S6b information update, if information update AAA is pending and RAR for restoration is received, then only the restoration will be handled. In this case, ReAuth will not be performed again for extended restoration, even if configured.
- APCO for Update Bearer Request (UBRequest) for extended P-CSCF Restoration in ePDG will be sent at bearer context level itself. APCO is not at message level for UBRequest.

- If S6b RAR ReAuth is pending and AAA of ReAuth is not yet received when RAR for restoration is received, then only the restoration will be handled. In this case, ReAuth will not be performed again for extended restoration, even if configured.
- For PCRF based P-CSCF Restoration/HSS based (S2a/S2b) P-CSCF Restoration, if UE PDN type and the PCO requested P-CSCF address do not match (for example, PDN type is IPv4 and PCO P-CSCF requested in IPv6, and vice versa), then basic restoration will be performed.
- UE Capability PCO and P-CSCF Restoration for S5/S8:

P-CSCF Reselect Support	P-CSCF Address Requested	MME-triggered Restoration	PCRF-triggered Restoration
✓	✓	Extended Restoration	Extended Restoration
✓	✗	Restoration Ignored	Basic Restoration
✗	✓	Basic Restoration	Basic Restoration
✗	✗	Basic Restoration	Basic Restoration

For S2a only, if MCM mode/WPMSI flag and UE P-CSCF re-selection support and P-CSCF address request is received, then only extended P-CSCF Restoration will be performed. For all other scenarios, if P-CSCF Restoration Indication is received, then basic P-CSCF Restoration is performed.

If both MCM/SCM flag are set, then it's considered SCM.

For S2b only, if UE P-CSCF re-selection support and P-CSCF address request is received during establishment or handoff is received, then only extended P-CSCF Restoration will be performed. For all other scenarios, if P-CSCF Restoration Indication is received, then basic P-CSCF Restoration is performed.

Call Flows

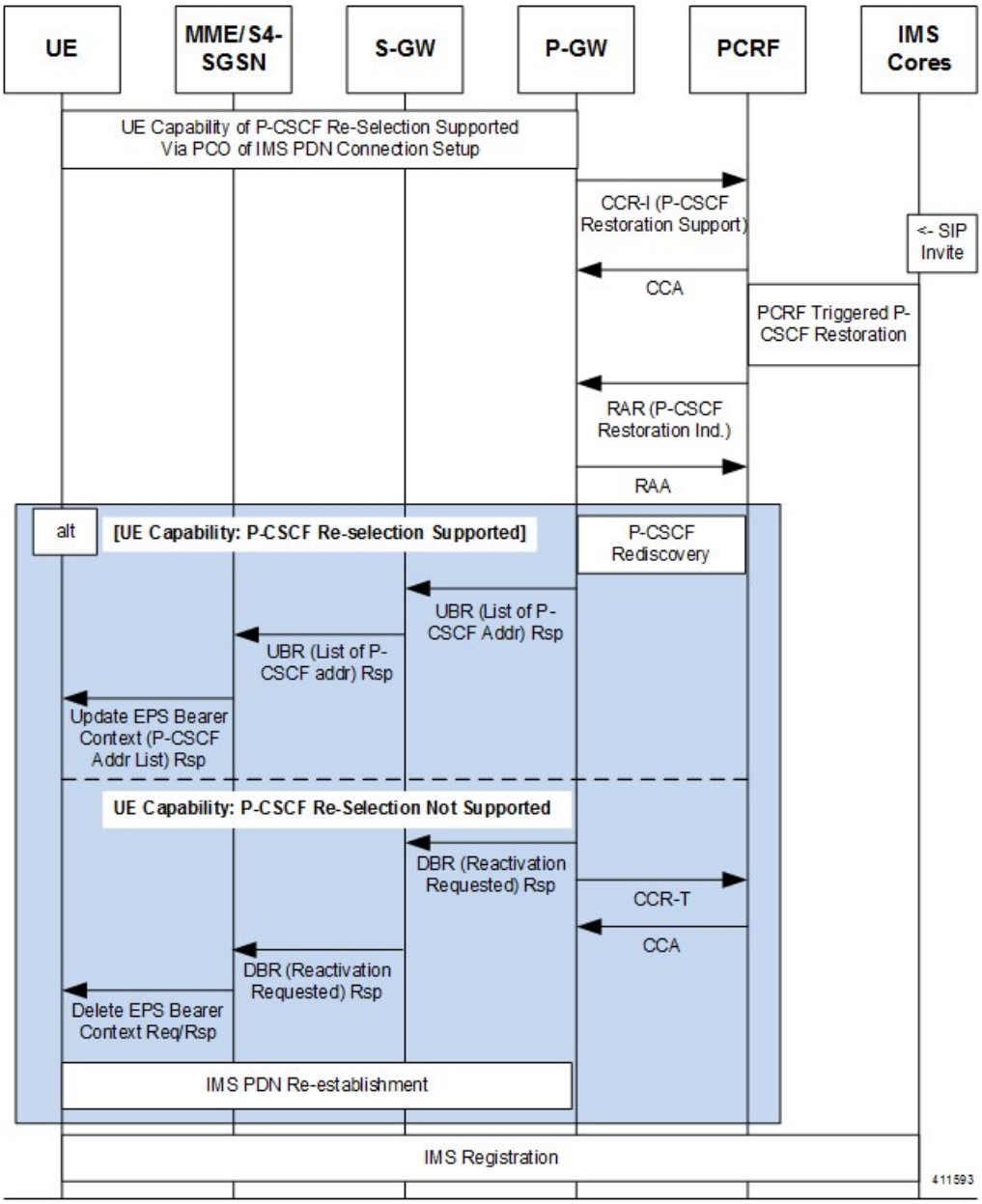
PCRF Based P-CSCF Restoration for LTE (S5/S8)

The PCRF-based P-CSCF Restoration makes use of the path through an alternative P-CSCF and PCRF to inform the P-GW regarding P-CSCF Restoration.

There are two mechanisms to handle the P-CSCF Restoration support:

1. **Basic Restoration Support**: UE does not support the P-CSCF Re-selection. P-GW informs UE to release the PDN connection. P-GW initiates bearer deactivation procedure for the default bearer with cause "reactivation requested".
2. **Extended Restoration Support**: P-GW sends the UBR with PCO having list of alternate P-CSCF addresses after the P-CSCF rediscovery. The optional extension avoids the PDN deactivation and re-activation and is based on the P-GW identifying whether or not the UE supports "Update PDP context/bearer at P-CSCF failure". The UE indicates this capability to the P-GW at the activation of the PDN connection in a PCO parameter.

Figure 70: PCRF Based P-CSCF Restoration - EPC



P-CSCF Restoration for WLAN (S2a/S2b)

This section describes solutions to support P-CSCF Restoration for UEs with WLAN access.

There are two mechanisms to handle the P-CSCF Restoration support:

1. **Basic Restoration Support**: The basic mechanism for the HSS-based solution and for the PCRF-based solution relies on the release of the PDN connection, followed by its re-establishment to trigger a new IMS registration by the UE.

2. **Extended Restoration Support**: The extension mechanism for trusted WLAN and untrusted WLAN access avoids the release of the PDN connection and triggers a new IMS registration by the UE over the existing PDN connection.

   The extension mechanism for trusted WLAN is supported only for multi-connection mode (MCM).

In the basic P-CSCF Restoration for TWAN access or untrusted WLAN access, the P-GW sets the cause "Reactivation requested" when tearing down the PDN connection.

If the re-authorization request is used for the purpose of the P-CSCF Restoration for WLAN, only the P-CSCF Restoration Request bit shall be set in the RAR Flags.

If the P-CSCF Restoration Request bit in the RAR Flags is set in ReAuthorization request (S6b):

- When P-GW triggers the extended P-CSCF restoration mechanism, the P-GW may send the authorization request.
- When P-GW triggers the basic P-CSCF restoration mechanism, the P-GW shall send a Session Termination Request to the 3GPP AAA Server.

For Trusted WLAN Access

- The TWAN shall advertise the support of the WLCP PDN connection modification request procedure over S2a at establishment (or handover) of the PDN connection. This allows the P-GW to use the P-CSCF Restoration extension on this TWAN.
- UE capability (UE support of the P-CSCF Restoration extension for the TWAN access) to the P-GW at the establishment (or handover) of the PDN connection over the WLAN is transferred via PCO IE.
- Upon receipt of a P-CSCF Restoration Indication, the P-GW may invoke this P-CSCF Restoration extension procedure if:
  - The UE is accessing the EPC via a TWAN in the multi-connection mode
  - The UE indicated support of this extension for the TWAN access via PCO, and
  - If the TWAN indicated support of the WLCP PDN connection modification procedure.
  - If UE requested P-CSCF address at establishment or handover.

  Otherwise, the basic restoration procedure is executed.
- For a trusted WLAN with the single connection mode or the transparent single connection mode, only the basic P-CSCF Restoration mechanism may apply.
- In the P-CSCF Restoration extension procedure for TWAN access, the P-GW shall send the updated list of the addresses of available P-CSCFs toward the UE via the TWAN using the PCO IE.

Figure 71: PCRF Based P-CSCF Restoration for Trusted WLAN Access

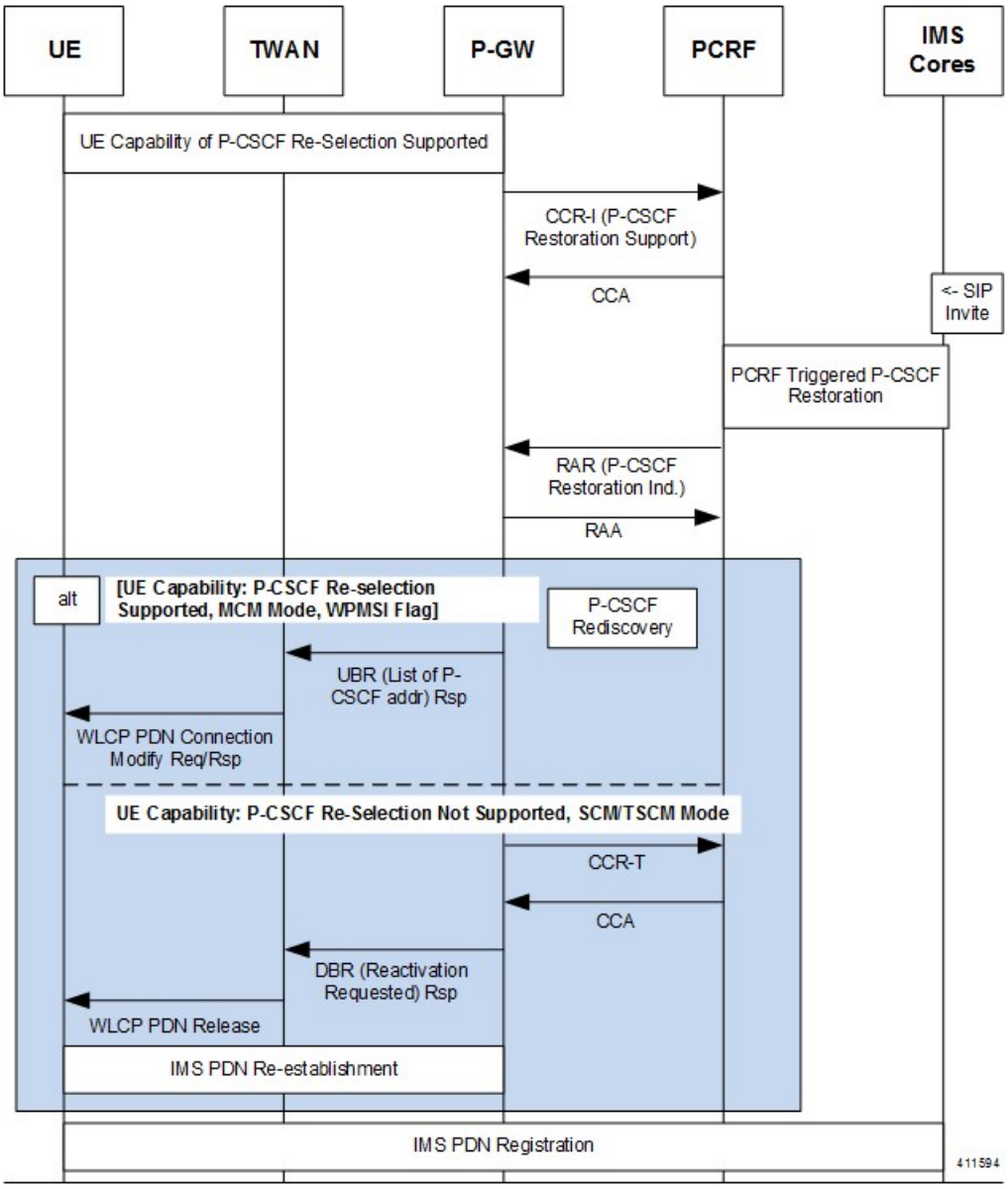
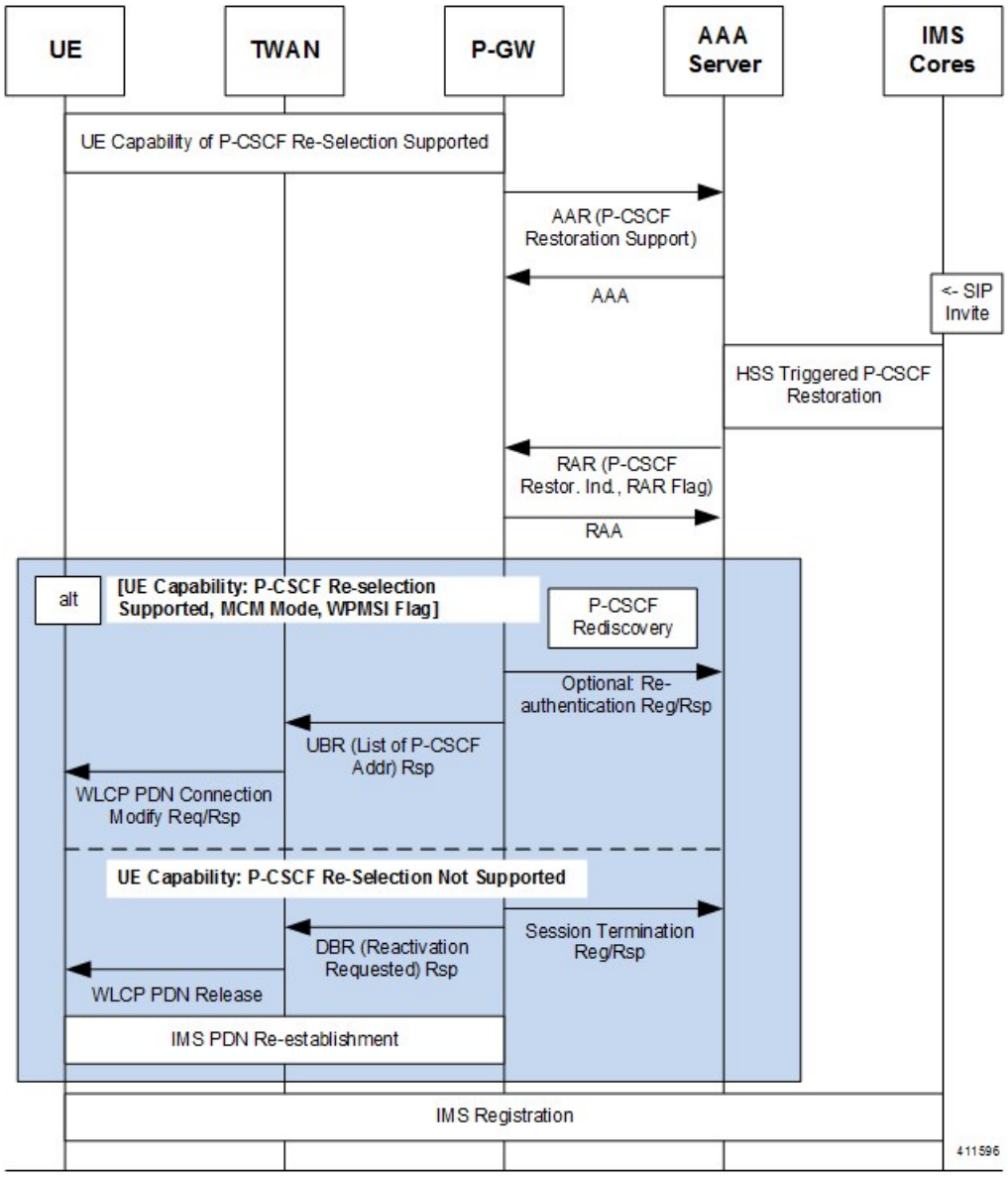


Figure 72: HSS Based P-CSCF Restoration for Trusted WLAN Access



Important Supported feature on S6b is sent in every ReAuth for RAT type WLAN.

For Un-Trusted WLAN Access

An ePDG which supports the P-CSCF Restoration extension for untrusted WLAN shall forward the UE capability (UE support of the P-CSCF restoration extension) in the APCO information element to the P-GW over the S2b interface at the PDN connection establishment (or handover) over S2b.

In the P-CSCF Restoration extension procedure for untrusted WLAN access, the P-GW shall send the updated list of the addresses of available P-CSCFs toward the UE via the ePDG using the APCO IE.

Figure 73: PCRF Based P-CSCF Restoration for Un-Trusted WLAN Access

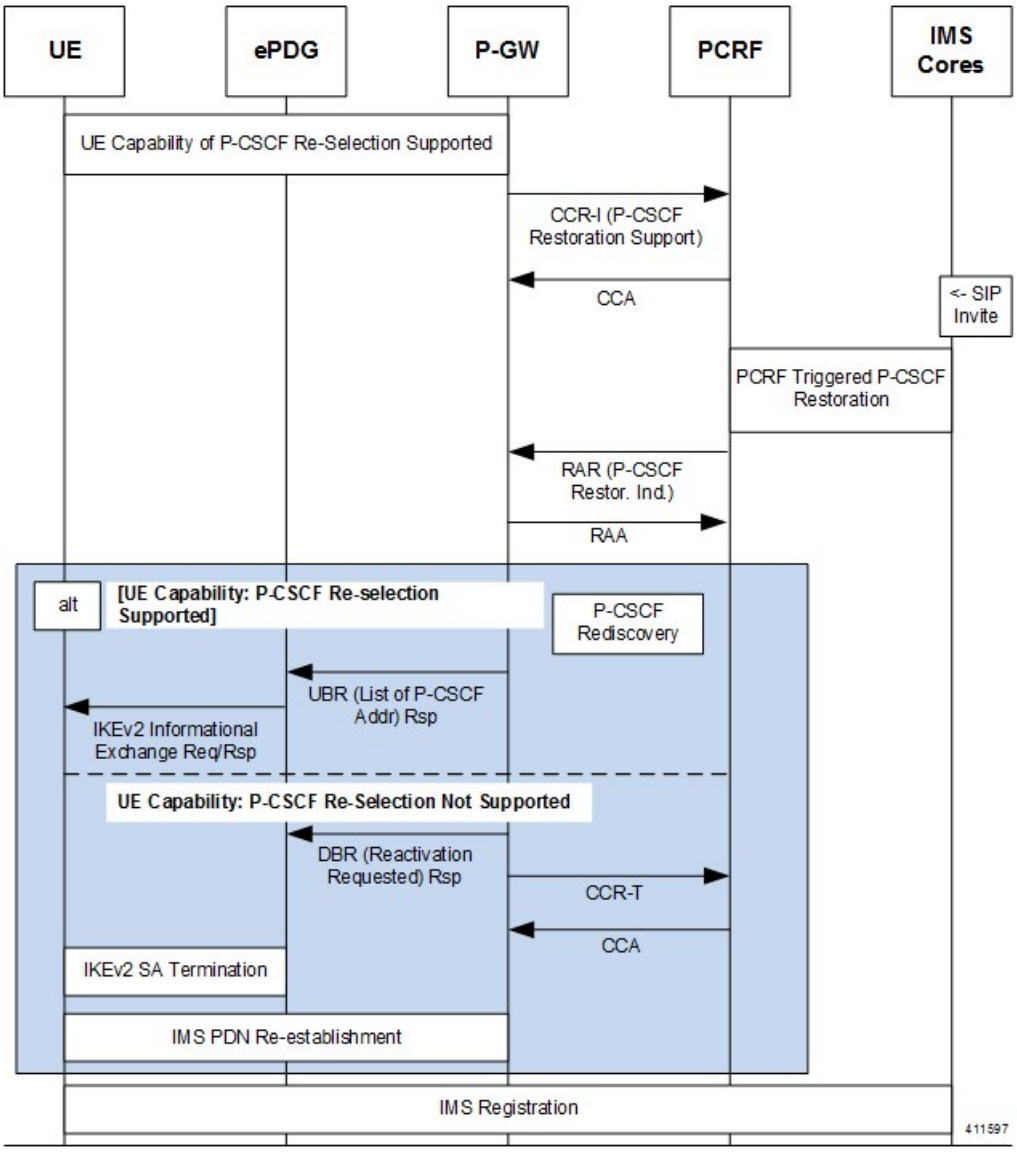
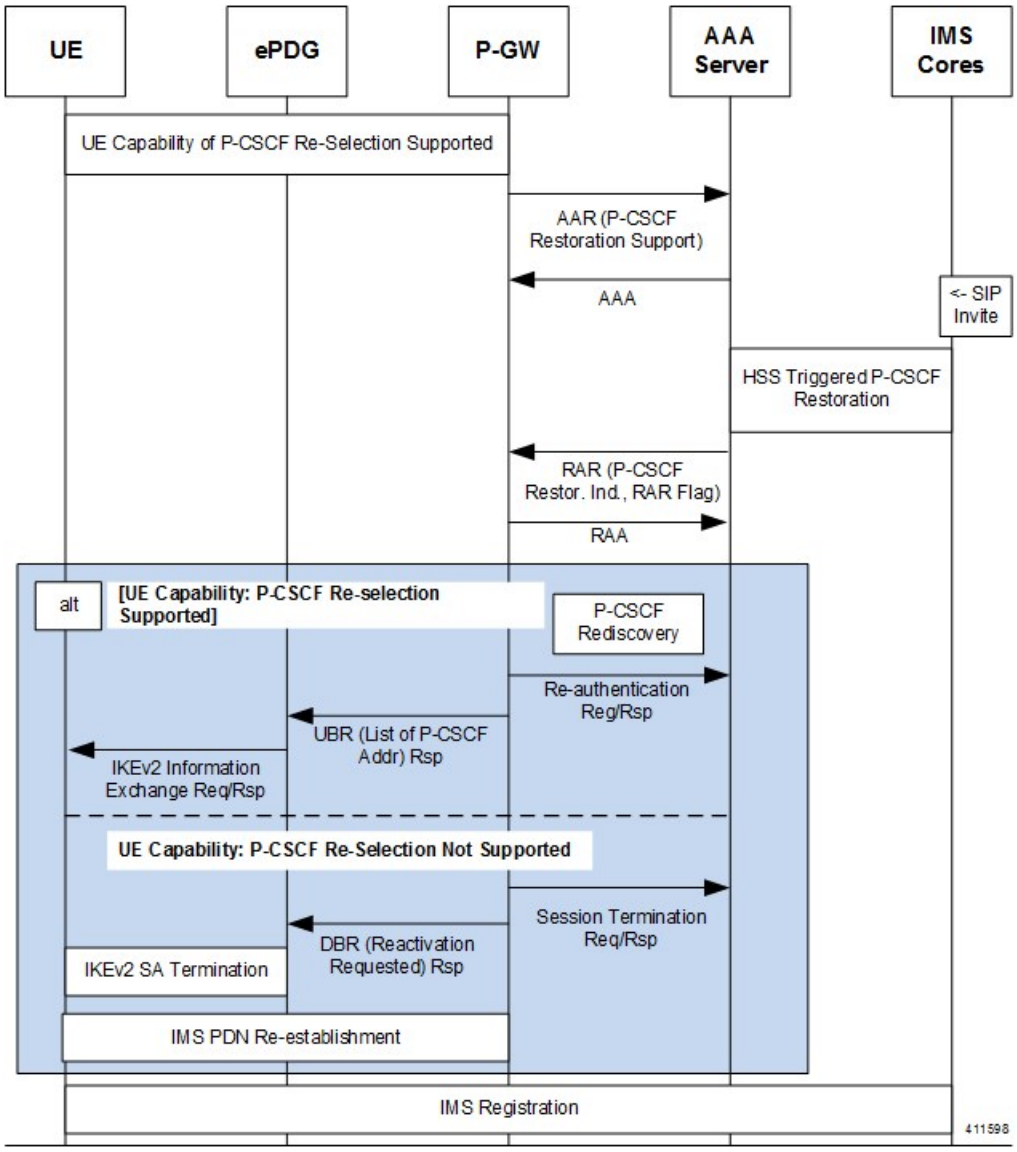


Figure 74: HSS Based P-CSCF Restoration for Un-Trusted WLAN Access



Standards Compliance

- Release 13 3GPP TS 23.380: IMS Restoration Procedures
- Release 13 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- Release 13 3GPP TS 29.212: Policy and Charging Control (PCC); Reference points
- Release 13 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- Release 13 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3

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 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 AVPs.
- **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.
- **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 for P-CSCF Restoration supported feature.

```
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, which is removing/resetting the supported features.
- **no encode-supported-features**: Removes the previously configured supported features.

Enabling P-CSCF Restoration for Emergency PDNs

Use the following configuration to enable P-CSCF Restoration for Emergency PDNs.

```
configure
   context context_name
      pgw-service service_name
         pcscf-restoration { hss-solution | custom-hss-solution }
         pcscf-restoration emergency-pdn
         end
```

Notes:

- **{ hss-solution | custom-hss-solution }** : Enables standards-based or private extension-based HSS solution for P-CSCF Restoration. This keyword must be configured on a separate command line from **emergency-pdn**.
- **emergency-pdn**: Enables P-CSCF Restoration for Emergency PDNs.

  This keyword is license dependent. For more information, contact your Cisco account representative. By default, this feature is disabled.
- **default pcscf-restoration**: P-CSCF Restoration is disabled for Emergency PDNs and Private Extn mechanism will be used for P-CSCF Restoration.
- **no pcscf-restoration emergency-pdn**: Disables P-CSCF restoration for Emergency PDNs.

Enabling Re-Auth After S6b Triggered P-CSCF Restoration of WLAN

Use the following configuration to enable Re-Auth after S6b triggered P-CSCF Restoration of WLAN.

```
configure
   context context_name
      pgw-service service_name
         pcscf-restoration s6b-reauth
         end
```

Notes:

- **s6b-reauth**: Enables Re-Auth after S6b triggered P-CSCF Restoration of WLAN. Only applicable for S2a and S2b. By default, Re-Auth will be performed for P-CSCF restoration extension on S6b.

  This keyword is license dependent. For more information, contact your Cisco account representative. By default, this feature is disabled.
- **default pcscf-restoration**: Re-Auth will be performed for P-CSCF restoration extension on S6b.
- **no pcscf-restoration s6b-reauth**: Disables Re-Auth after P-CSCF restoration extension on S6b.

Verifying the HSS/PCRF-based P-CSCF Restoration

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
....
```

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 pgw-service name <pgw_service>

This command generates a display that indicates the configuration status of this feature.

The following sample display is only a portion of the output.

P-GW service output is enhanced to clearly specify HSS-based solution of **MME-Triggered**; this avoids confusion with the HSS-based S6b Triggered solution. In addition, it displays whether **P-CSCF Restoration supported for Emergency PDNs** and/or **Re-Auth After s6b Triggered P-CSCF Restoration** is enabled.

```
show pgw-service name <pgw_service>

    Service name : pgw_service
    Restoration solution : HSS-based MME-Triggered (Rel12)
    P-CSCF Restoration supported for Emergency PDNs : Yes/No
    Re-Auth After s6b Triggered P-CSCF Restoration : Enabled / Disabled
 ....
```

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

Output of Show Commands

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 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 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.

show pgw-service name <pgw_service>

P-GW service output is enhanced to clearly specify HSS-based solution of **MME-Triggered**; this avoids confusion with the HSS-based S6b Triggered solution. In addition, it displays whether **P-CSCF Restoration supported for Emergency PDNs** and/or **Re-Auth After s6b Triggered P-CSCF Restoration** is enabled.

```
show pgw-service name <pgw_service>

    Service name : pgw_service
    Restoration solution : HSS-based MME-Triggered (Rel12)
    P-CSCF Restoration supported for Emergency PDNs : Yes/No
    Re-Auth After s6b Triggered P-CSCF Restoration : Enabled / Disabled
 ....
```

show pgw-service statistics all

This command provides statistics on the number of P-CSCF Restorations.

The MME received P-CSCF Restoration count has moved from " **P-CSCF Restoration Indications received:**" to "**MME triggered Restoration**". Now, " **P-CSCF Restoration Indications received:**" shows total number of P-CSCF Restoration indications received (HSS Triggered and PCRF Triggered). Bulkstat counter "**sessstat-pcscf-recovery-count**" will continue to display the MME received P-CSCF Restoration only.

The total number of triggers received on any interface (MME/PCRF/S6b) = Basic + Extended + Ignored (ignored for reasons such as restoration already in progress, license not present, validation check fails, or call not connected).

```
PDNs Released By Reason:
  Network initiated release:           0    MME initiated release:             0
    Admin disconnect:                  0    S4 SGSN initiated release:         0
    GTP-U error ind:                   0
    SGW path failure:                  0
    Local fallback timeout:            0
    UE P-CSCF Reselect not supported:  0
…

 S2bGTP-to-eHRPD handover:               eHRPD-to-S2bGTP handover:
        Attempted:                       0      Attempted:                      0
        Succeeded:                       0      Succeeded:                      0
        Failed:                          0      Failed                          0
 …
```

```
     P-CSCF Restoration Indications received:              <total_count
at service level>
       HSS Triggered Restoration:
         MME Triggered Restoration:                      <>
             Basic Restoration Performed:                <>
             Extension Restoration Performed:            <>
         S6b Triggered Restoration:                      <>
             Basic Restoration Performed:                <>
             Extension Restoration Performed:            <>
       PCRF Triggered Restoration:                       <>
           Basic Restoration Performed:                  <>
           Extension Restoration Performed:              <>

      Data Statistics Per Interface:
…
```

show srp checkpoint statistics active verbose

This command provides the following P-CSCF Restoration micro checkpoint information:

```
.
.
     Total pgw ubr_mbr micro-chkpnt sent:                0
     Total pcscf update micro-chkpnt sent:                  0
```

show srp checkpoint statistics standby verbose

This command provides the following P-CSCF Restoration micro checkpoint information:

```
.
.
```

```
 PGW ubr_mbr session microchkpt rcvd:          0

PCSCF info update microchkpt rcvd:              0
```

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.

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
....
```

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
....
```

Bulk Statistics

P-GW Schema

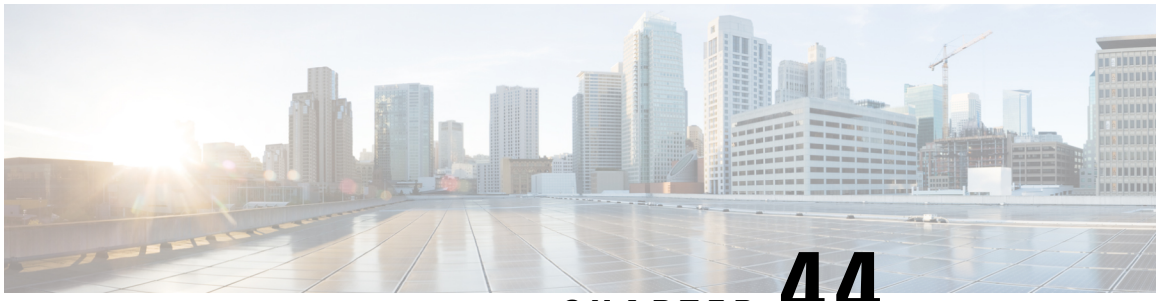
The following counters are specific to **pcscf-recovery**:

- sessstat-pcscf-recovery-count
- sessstat-pcscf-recovery-basic-count
- sessstat-pcscf-recovery-extension-count
- sessstat-s6b-pcscf-recovery-count
- sessstat-s6b-pcscf-recovery-basic-count
- sessstat-s6b-pcscf-recovery-extension-count
- sessstat-pcrf-pcscf-recovery-count
- sessstat-pcrf-pcscf-recovery-basic-count
- sessstat-pcrf-pcscf-recovery-extension-count

SAEGW Schema

The following counters are specific to **pcscf-recovery**:

- pgw-sessstat-pcscf-recovery-count
- pgw-sessstat-pcscf-recovery-basic-count
- pgw-sessstat-pcscf-recovery-extension-count
- pgw-sessstat-s6b-pcscf-recovery-count
- pgw-sessstat-s6b-pcscf-recovery-basic-count
- pgw-sessstat-s6b-pcscf-recovery-extension-count
- pgw-sessstat-pcrf-pcscf-recovery-count
- pgw-sessstat-pcrf-pcscf-recovery-basic-count
- pgw-sessstat-pcrf-pcscf-recovery-extension-count



CHAPTER 44

ICAP Interface Support

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

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

The following products currently support ICAP interface functionality:

- GGSN
- P-GW

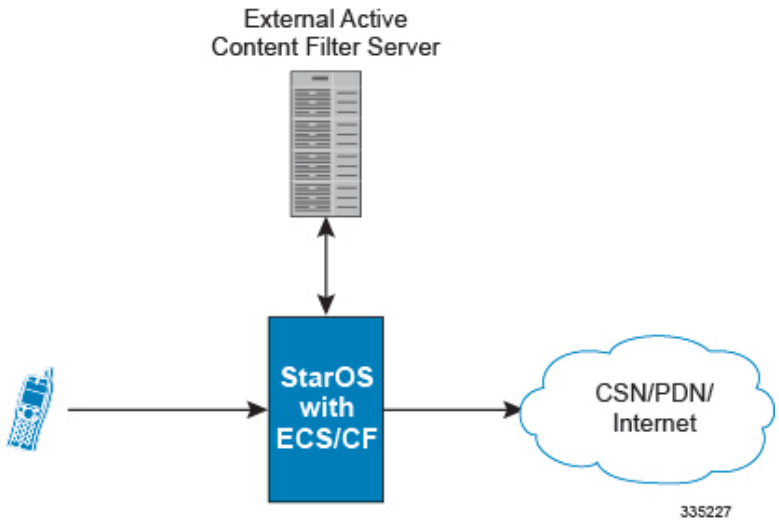
- ICAP Interface Support Overview, on page 831
- Configuring ICAP Interface Support, on page 836

ICAP Interface Support Overview

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

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

Figure 75: High-Level View of Streamlined ICAP Interface with external ACF



The system with ECS is configured to support DPI and the system uses this capability for content charging as well. WAP and HTTP traffic is content filtered over the ICAP interface. RTSP traffic that contains adult content can also be content filtered on the ICAP interface. Only the RTSP Request packets will be considered for content filtering over the ICAP interface.

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

- A 200 OK message if the request is accepted.
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber must be redirected.
- Deny-response code 200 for RTSP requests is not supported. Only 403 "Forbidden" deny-response code will be supported.

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

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

Functions of the ACF include:

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

Supported Networks and Platforms

This feature supports the Cisco ASR 5500 platform for the core network services configured on the system.

For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

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

Failure Action on Retransmitted Packets

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

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

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

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

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

GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.

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

  The following scenarios describe the failure actions where an RTSP request is received from the client. If ICAP is enabled, then the request goes to the ICAP server for content filtering.
  - Allow: If the failure action configured is "allow", the RTSP request packet is sent out after applying the appropriate disposition action. Here, the flow remains the same as in the case if the ICAP response received is 200 OK.
  - Content Insert: If the failure action configured is "content-insertion <string of size 1 to 128>", then this failure action for RTSP request will not be supported. Instead the failure action "Discard" for such an RTSP request will be supported.
  - Redirect-URL: If the failure action configured is "redirect-url <string of size 1 to 128>", then a TCP FIN_ACK packet with an RTSP "302 Moved Temporarily" response header is inserted towards the client containing the said URL for redirection. A TCP RST packet is inserted towards the server. The underlying TCP connection is thus closed. If the RTSP client wants to retry to the redirected URL, the opening of a new TCP connection must be initiated.
  - Discard: If the failure action configured is "discard", then the RTSP request packet received from the client is quietly discarded and no notification is sent to the client.
  - Terminate flow: If the failure action configured is "terminate-flow", then the TCP connection is torn down by injecting a TCP FIN-ACK towards the client and a RST packet towards the server. However, no notification will be sent to the RTSP client and the server regarding this flow termination.

ICAP Client Communication with RFC 3507 compliance

The ICAP Content Filtering solution is extended to support ICAP client communication with ICAP server on Cisco ASR 5500 P-GW and HA in compliance with RFC 3507 - Internet Content Adaptation Protocol (ICAP). Only HTTP Request modification and partial enhancement of error codes per RFC 3507 is addressed in this release. The ICAP client running on P-GW/HA communicates with external ICAP server over ICAP protocol. If content filtering is enabled for a subscriber, all HTTP GET requests from that subscriber are validated by

the content filtering server (ICAP server), and is allowed, denied or redirected depending on the content categorization request.

Content-Filtering can be enabled for subscribers either through Override Control (OC) feature for predefined and static rules, or L7 Dynamic Rule Activation feature. A configurable option is added in the Content Filtering Server Group Configuration Mode to configure ICAP header that includes two parameters - Subscriber number information and CIPA (Children's Internet Protection Act) category.



Important Override Control and L7 Dynamic Rule Activation are license-controlled features. A valid feature license must be installed prior to configuring these features. Contact your Cisco account representative for more information.

- Subscriber Number: The "Subscription ID" AVP is sent from gateway to PCRF in CCR message. The AVP values are received to the gateway from HSS. The gateway does not receive this AVP in CCI-A message.
- CIPA category: The category string will be provided by PCRF and is included as an extension header in ICAP request modification message. The AVP will be received from PCRF in CCA-I or RAR.

Dictionary and AVP Support

A new Content Filtering (CF) dictionary "custom4" is introduced and the following new AVPs are added to r8-gx-standard and custom4 dictionaries.

- Override-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of rules or charging-action. This AVP is used for overriding the content-filtering status of static and predefined rules. This attribute is included in the Override-Control grouped AVP.
- CIPA: This attribute contains the Children's Internet Protection Act (CIPA) category string value that is treated as an ICAP plan identifier. This identifier helps ICAP server in locating the correct Content Filtering plan i.e. CIPA category based on which the packet is processed.

  This attribute value is received from PCRF over Gx interface and is included in ICAP header while sending ICAP request.
- L7-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of L7 rules. This attribute indicates whether or not the ICAP functionality is enabled or disabled for L7 charging rule definition received for installation from PCRF. Based on this attribute value, the traffic matching to the dynamic rule is sent to ICAP server.

  This attribute is included in the L7-Application-Description grouped AVP for L7 rule processing. This is applicable only for HTTP protocol.



Important CIPA and flags for controlling content filtering via OC and L7 Dynamic Rules features is applicable only for r8-gx-standard dictionary.

In addition to the new AVP support, L7-Field AVP in the L7-Application-Description grouped AVP is encoded to additionally accept ANY-MATCH as the input. The current framework does not support the existing field "vlan-id" in Override-Control, which is present in charging action. Hence, the Override-Content-Filtering-State AVP replaces Override-VLAN-ID to support OC.

When subscriber initiates create session request, P-GW/HA sends CCR-I message to PCRF to obtain subscriber profile. PCRF responds with CCA-I message that contains CIPA and OC information if ICAP functionality is enabled for this subscriber.

In the case of L7 dynamic rules, the Content-Filtering capability is enabled by sending L7-Content-Filtering-State AVP in L7-Application-Description grouped AVP. At least one L7 filter should be present when L7-Content-Filtering-State is received for the dynamic rule. If L7-Content-Filtering-state AVP is sent along with L7 filter information AVP, then the Content-Filtering state will not be considered. Hence, the filter received with L7-Content-Filtering-State will not be processed and the L7 rule will be discarded.

In the case of Override Control, when content filtering is enabled for subscriber, PCRF sends ICAP flag through Override-Control AVP. This AVP overwrites charging action to enable ICAP feature for that subscriber.

Refer to the *AAA Interface Administration and Reference* for more information on the supported AVPs.

Limitations

The limitations for this feature are listed below:

- Only IPv4 addressing scheme is supported.
- ICAP content filtering is applicable only for HTTP traffic. HTTPS traffic is not supported by ICAP client.
- Accelerated path will not be supported for this feature.

Configuring ICAP Interface Support

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



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

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

Procedure

Step 1 Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in Creating ICAP Server Group and Address Binding, on page 837.

Step 2 Specify the active content filtering server (ICAP server) IP addresses and configure other parameters for ICAP server group by applying the example configuration in Configuring ICAP Server and Other Parameters, on page 837.

Step 3 Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in Configuring ECS Rulebase for ICAP Server Group, on page 838.

Step 4 Configure the charging action to forward HTTP/RTSP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in Configuring Charging Action for ICAP Server Group, on page 838.

Step 5 Verify your ICAP interface and external content filtering server group configuration by following the steps in Verifying the ICAP Server Group Configuration, on page 839.

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

Creating ICAP Server Group and Address Binding

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

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

Notes:

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

Configuring ICAP Server and Other Parameters

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

```
configure
   context <icap_context_name>
      content-filtering server-group <icap_server_grp_name>
         icap server <ip_address> [ port <port_number> ] [ max <max_msgs>] [
priority <priority> ] [ standby ]
         connection retry-timeout <retry_timeout>
         deny-message <msg_string>
         dictionary { custom1 | custom2 | custom3 | custom4 | standard }
        failure-action { allow | content-insertion <content_string> | discard
 | redirect-url <url> | terminate-flow }
         header extension options { cipa-category cipa_category_name |
subscriber-number subscriber_num_name } +
         response-timeout <timeout>
         end
```

Notes:

- Only one ICAP Server can be configured per Content Filtering Server Group.
- The **standby** keyword can be used to configure the ICAP server as standby. A maximum of ten active and standby ICAP servers per Content Filtering Server Group can be configured. The active and standby servers under the same server group can be configured to work in active-standby mode.

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

  url-extraction { after-parsing | raw }

  By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.
- The **custom4** dictionary is a custom-defined dictionary that specifies user-defined information in the ICAP request message. The ICAP request message includes subscriber number and CIPA category values.

  When **custom4** dictionary is configured, ICAP requests are formed as part of ICAP RFC 3507 request mode request. If any other dictionary is configured, the earlier implementation of ICAP client will not be partial RFC compliant.
- The **header extension options** command configures ICAP header parameters - subscriber number and CIPA category.

Configuring ECS Rulebase for ICAP Server Group

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

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

Notes:

- The **optimized-mode** keyword is not available.



Important After you configure **configure**, **require active-charging**, **active-charging service** <*acs_svc_name*> **[-noconfirm]**, and **rulebase** CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring Charging Action for ICAP Server Group

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

```
configure
   active-charging service <acs_svc_name>
      charging-action <charging_action_name> [ -noconfirm ]
```

```
[ no ] content-filtering processing server-group
end
```

Notes:

- If the content-filtering flag supplied by charging action is required to configure the Override Control feature, then the **no content-filtering processing** command must be configured. This will ensure overriding content-filtering processing to be enabled or disabled through the Override Control feature.

Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file and also to retrieve errors and warnings within an active configuration for a service.

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

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

Procedure

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

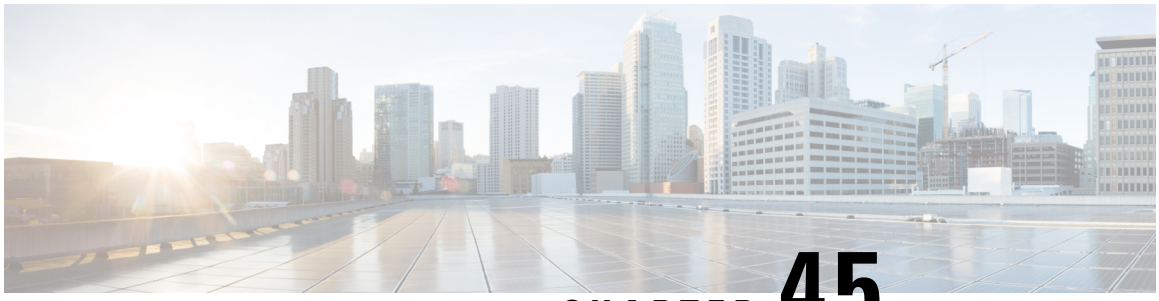
show content-filtering server-group

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

```
Content Filtering Group:         icap_cfsg1
    Context:                             icap1
    Origin Address:                      1.2.3.4
    ICAP Address(Port):                  1.2.3.4(1344)
    Max Outstanding:                     256
    Priority:                            1
    Response Timeout: 30(secs)  Connection Retry Timeout: 30(secs)
    Dictionary:                          standard
    Timeout Action:                      terminate-flow
    Deny Message:                        "Service Not Subscribed"
    URL-extraction:                      after-parsing
    Header Extension Options:            subscriber-number i-sub
    Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria:  1
```

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

show configuration errors



CHAPTER 45

IMS PCO Configurations when Gx is Down

- Feature Summary and Revision History, on page 841
- Feature Description, on page 842
- How It Works, on page 842
- Configuring the IMS PCO Configuration when Gx is Down, on page 844

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

When Gx is down, the IMS Packet Data Network (PDN) session uses the local policy. However, the existing Proxy-Call Session Control Function (P-CSCF) PCO list configuration under the "ims-auth" profile does not apply to the PDN session within the local policy. The alternative configuration is to configure the P-CSCF IPs under the APN configuration. This APN configuration has a limit of three IP addresses that does not meet the production configuration needs.

The IMS PDN session uses the P-CSCF list configuration under IMSA after falling back to local policy to achieve VoLTE Resiliency. With this feature, the P-CSCF PCO list applies to PDN session in local policy.

How It Works

The UE performs P-CSCF discovery before sending any Session Initiation Protocol (SIP) requests. P-GW provides the UE with the P-CSCF addresses when UE requests the parameters from the network within the Protocol Configuration Options element to include the P-CSCF address. If UE has more than one P-CSCF address, the selection then uses the configuration policy to select the P-CSCF.

Priority of P-CSCF addresses selection in P-GW is as follows:

- Addresses from DNS (S6b provides FQDN or FQDN received from Access Point Name (APN) configuration).
- Addresses from the IMSA-configured table.
- Configuration addresses that are part of APN configuration.

When local policy fallback occurs and Gx is down, P-CSCF list from IMSA profile is used. The following are the scenarios when local policy is used:

- P-CSCF list when Gx is down
- CCR-I Response Failure

Call Flows

The following call flows and procedures explain P-CSCF address selection and Response Failure scenarios.

P-CSCF Address Selection Call Flow

When Create Session Request (CSR) is received with PCO request, the P-GW checks for peers. If all peers are in the down state or no peers are available, then the Gx interface is considered as down. The PDN session fallbacks to the local policy and uses the P-CSCF list from IMSA.

When Virtual APN (VAPN) configuration is available and Gx is down, the P-CSCF uses addresses from IMSA of the selected VAPN. If VAPN configuration is not available, then the P-CSCF address list is received from IMSA of an APN.

Figure 76: P-CSCF Address Selection-Gx Down

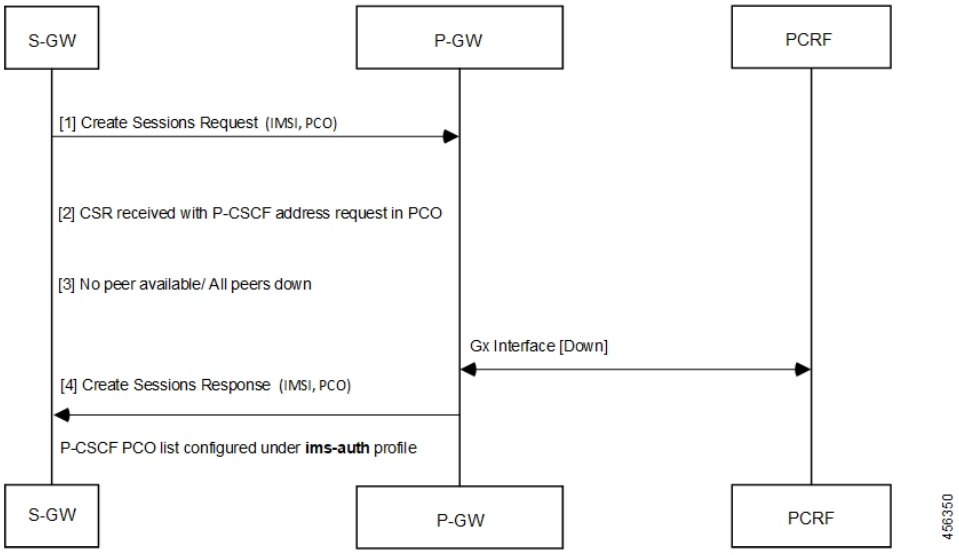


Table 84: Procedure

Step	Description
1	S-GW sends Create Session Request (IMSI, PCO) to P-GW.
2	P-GW receives Create Session Request with the P-CSCF address request in PCO from S-GW and checks for peers available for the Gx interface.
3	If no peers are available or all peers are down, then Gx interface is considered as down between PCRF and P-GW. The PDN session fallbacks to the local policy and uses the P-CSCF list from IMSA.
4	P-GW then sends a Create Session Response with P-CSCF PCO list configurations under the "ims-auth" profile to S-GW.

Response Failures Call Flow

When CSR is received with P-CSCF address request under PCO, the P-GW checks for peers.

If the peer is in the Up state and reachable, Gx is considered in Up state and CCR-I is sent for the primary host. If P-GW receives error response, then the secondary host is used. If the secondary host fails as well, then the PDN session falls back to the local policy and uses the P-CSCF list from IMSA.

Figure 77: Response Failure (CCR–Initial Request)

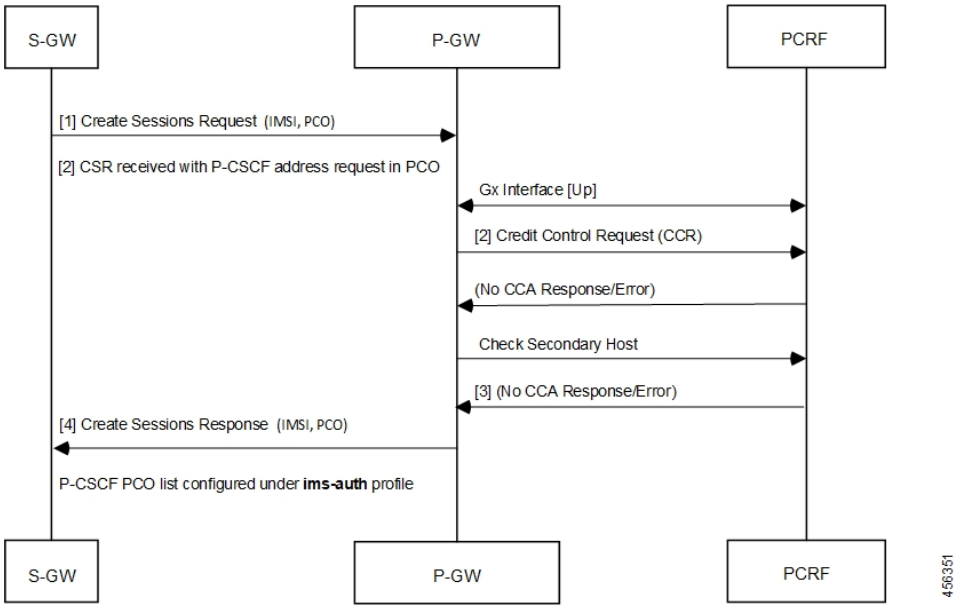


Table 85: CCR-I Response Failure

Step	Description
1	S-GW sends Create Session Request (IMSI, PCO) to P-GW.
2	P-GW receives Create Session Request with the P-CSCF address request in PCO from S-GW and checks for peers available for Gx interface. If the peer is in the Up state and reachable, Gx is in Up state. P-GW sends a Credit Control Request (CCR) to PCRF for the primary host.
3	PCRF does not send credit Control Answer (CCA) Response or sends an error code to P-GW. If case P-GW receives error response, then use the secondary host. If the secondary host fails, then the PDN session falls back to the local policy and uses the P-CSCF list from IMSA.
4	P-GW then sends a Create Session Response with the P-CSCF PCO list configurations under the "ims-auth" profile to S-GW.

Configuring the IMS PCO Configuration when Gx is Down

This section describes how to configure the IMS PCO configuration when Gx is down.

Enabling P-CSCF Address from IMSA in Local Policy Service

Use the following configuration to enable P-CSCF to use the address from IMSA, under Local Policy Service, when Gx is down.

```
configure
  local-policy-service service_name
    [ no ] use-pcscf-config-from-imsa
    end
```

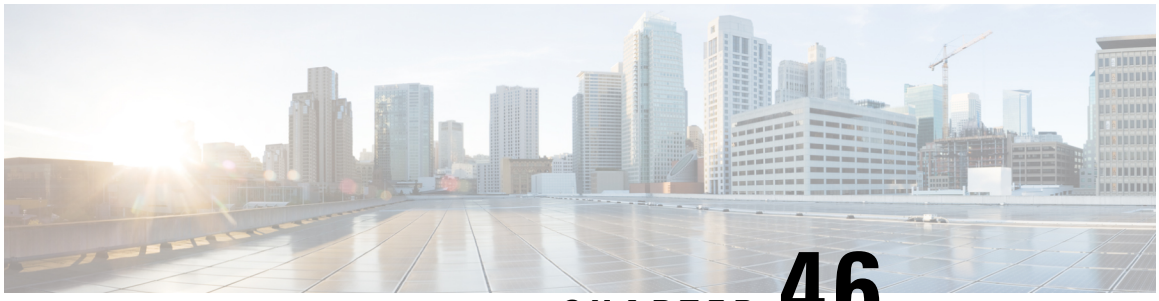
NOTES:

- **no** : Disables the feature.
- **use-pcscf-config-from-imsa**: Specifies to use the P-CSCF configuration from IMSA in Local Policy.
- To define the method of P-CSCF discovery to be used, use the existing **p-cscf discovery** CLI command under IMS Authorization Service Configuration mode.
- To add/append rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery, use the existing **p-cscf table** CLI command under IMS Authorization Service Configuration mode.

Verifying P-CSCF Configuration in Local Policy

Use the **show configuration** CLI command to verify if the P-CSCF Configuration in Local Policy is enabled or disabled. The output of this command does not display the mode if the **use-pcscf-config-from-imsa** is disabled.

The **show configuration verbose | grep “use-pcscf” use-pcscf-config-from-imsa** CLI command displays the mode for **use-pcscf-config-from-imsa** when it is enabled.



CHAPTER 46

Inclusion of APN AMBR in the Create Session Response

- Feature Information, on page 847
- Feature Changes, on page 848
- Command Changes, on page 848
- Performance Indicator Changes, on page 849

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	Enabled
Related CDETS ID(s)	CSCvd00467
Related Changes in This Release	Not Applicable
Related Documentation	Command Line Interface Reference P-GW System Administration Guide Statistics and Counters 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

Currently, APN AMBR is included in the Create Session Response even if it is not modified by the PCRF. This feature has been implemented to comply to the 3GPP specifications. With this feature, now APN AMBR will be included on the S5/S8, S4/S11, and S2a/S2b interfaces if the received APN-AMBR has been modified by the PCRF.

Previous Behavior: APN AMBR was included in Create Session Response even if it was not modified by the PCRF.

New Behavior: Now, APN AMBR will be included on the S5/S8, S4/S11, and S2a/S2b interfaces if the received APN-AMBR has been modified by the PCRF. A new CLI command has been added to enable/disable inclusion of the APN-AMBR value in the Create Session Response for the modified value received by the PCRF.



Important P-GW supports APN-AMBR value upto 4294967 kbps.

Command Changes

egtp

Two new keywords have been added to the **egtp** command to enable/disable inclusion of APN-AMBR value in Create Session Response for modified value received by PCRF.

```
configure
  context context_name
    pgw service service_name
      [ default | no ] egtp create-session-rsp apn-ambr-always-include
      end
```

Notes:

- **default:** APN AMBR is not included in the CS Response if APN AMBR is not received from the PCRF. P-GW supports APN-AMBR value upto 4294967 kbps.
- **no:** Does not include APN AMBR in the CS Response. This is the default behavior.

- **create-session-rsp:** Provides an option to include APN-AMBR in the Create Session Response
- **apn-ambr-always-include:** Always includes APN-AMBR IE in Create Session Response.

Performance Indicator Changes

show config

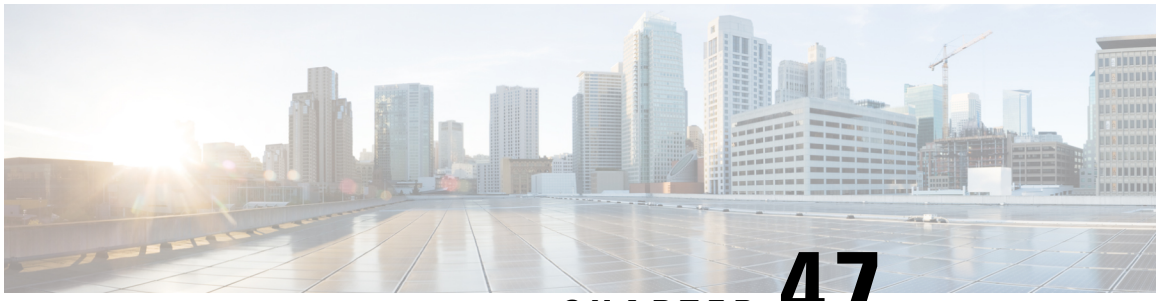
This command has been modified to display the following output:

```
plmn id mcc 404 mnc 00
plmn id mcc 404 mnc 005 primary
plmn id mcc 404 mnc 090
fqdn host abc.net realm 3gpp.org
dns-client context ISP1
associate ggsn-service GGSN
associate egtp-service PGW21EGTP
egtp create-session-rsp apn-ambr-always-include
```

show pgw-service name

This command has been modified to display the following output:

```
EGTP SGW Restoration Handling: Disabled
Session Hold Timer: n/a
Timeout: n/a
EGTP Modify bearer cmd negotiate qos: Disabled
EGTP GnGp Modify bearer res with APN-AMBR: Disabled
EGTP Modify bearer res with CHARGING-ID: Disabled
EGTP Modify bearer res with CHARGING-FQDN or CHARGING-GW-ADDRESS: Disabled
EGTP Modify bearer res with MSISDN: Disabled
EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch: Disabled
EGTP Bit Rate in Rounded Down Kbps: Disabled
EGTP Suppress Update Bearer Request (no bitrate change): Disabled
EGTP Create Session Response with APN-AMBR IE: Enabled
```



CHAPTER 47

Increase in Monitoring of Peers Supported Through Heartbeat Mechanism for PMIP Sessions

This chapter describes the following topics:

- Feature Summary and Revision History, on page 851
- Feature Description, on page 852
- Configuring the Increase in Number of PMIP Sessions Supported with the Heartbeat Mechanism Feature, on page 853
- Monitoring and Troubleshooting, on page 854

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC - SI • VPC - DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

In the existing setup, the HA Manager supports monitoring of Proxy Mobile IPv6 (PMIP) sessions for up to 256 peers through the heartbeat mechanism. Now there is a requirement to increase the monitoring of peers from 256 to 128000.

To increase the number of PMIP sessions to enable more peers to be monitored for path failure with the heartbeat mechanism, a new CLI **monitor-max-peers** is added under the LMA Service Configuration mode. This feature supports the following behavior:

- When configured, the maximum number of peers that can be supported for heartbeat monitoring can be increased from 256 to 128000 peers.
- The first 128000 peers are identified during the calls irrespective of whether the heartbeat mechanism is enabled or not.
- A separate list is maintained for retransmission heartbeats and periodic heartbeats for batch processing.
- The decision to monitor peers is done at the time of call setup, recovery, and ICSR. For example, consider that there are more than 256 peers (considering the CLI is configured for a maximum of 128000 peers) that are being monitored for heartbeat. Later, this configuration is changed to default, which is for a maximum of only 256 peers. Then, monitoring continues for all peers until HA Manager recovery or ICSR (with monitor-max-peers configuration of a maximum 256 peers) occurs.
- The parameters for batch processing for heartbeat messages are changed as follows:

	Batch Size (before)	Batch Size	Batch Interval (before)	Batch Interval
Periodic heartbeat batch	100	550	200 ms	200 ms
Retransmission heartbeat batch	100	550	200 ms	100 ms

- If more than 10% of peers (12800 peers) are not responding, then the detection of path failure of nodes is delayed. This delay is to avoid a huge impact on performance when such a condition occurs.

  If retransmissions start occurring for more than the batch size expected based on the calculations, then the heartbeat messages follow the periodic timer for sending heartbeat messages. For example, if the configuration of the heartbeat interval is 60 seconds, retransmission timeout is 3 seconds, and maximum retries is 3.

  Now if the number of heartbeat messages for retransmissions exceed the expected batch size, then instead of a retransmission occurring every 3 seconds, retransmissions of heartbeat messages start with interval of 60 seconds. Therefore, under normal condition if a peer path failure was detected at a maximum of 9 seconds (3*3), it is now detected at 180 seconds (60*3).

- Minimum heartbeat interval must be 60 seconds.

  If 128000 peers are configured for monitoring heartbeat, then heartbeat interval must not be configured for less than 60 seconds. If the heartbeat interval is configured for less than 60 seconds, then a configuration error is displayed.

- Minimum heartbeat retransmission timeout should be three seconds.

  If 128000 peers are configured for monitoring heartbeat, then heartbeat retransmission timeout must not be configured for less than three seconds. If the heartbeat interval is configured for less than 60 seconds, then a configuration error is displayed.

- The CLI is configured at the service level but the list is maintained at the instance level. Therefore, it is recommended that all services have the same configuration.

  If services have different configuration, then the limitation is based on that service level configuration. However, the maximum number of peers is determined based on how many peers are already there in that instance.

  For example, consider two services: lma1 and lma2. lma1 has the monitor-max-peers configured as 128000 peers. lma2 has monitor-max-peers configured as 256 peers. Now if the call comes from lma1, it checks the max peers limitation of 128000 peers. If the call comes from lma2, it checks max peers limitations of 256. However, for lma2 it may include all 256 peers that are being monitored in lma1.



Note This feature is customer-specific. For more information, contact your Cisco account representative.

Configuring the Increase in Number of PMIP Sessions Supported with the Heartbeat Mechanism Feature

The following section provides the configuration commands to enable or disable the feature.

heartbeat monitor-max-peers

This new CLI command supports monitoring of a maximum of 128000 PMIP sessions through the heartbeat mechanism. This CLI is added under the LMA Service Configuration mode.

To configure monitoring of a maximum number of PMIP sessions, enter the following commands:

```
context context_name
 configure lma-service service_name
  [ default ] heartbeat monitor-max-peers
  end
```

Notes

- **default:** Monitors 256 peers through the heartbeat mechanism. This CLI is disabled by default.
- **heartbeat monitor-max-peers:** Monitors a maximum of 128000 peers through the heartbeat mechanism.

Monitoring and Troubleshooting

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

Show Commands and/or Outputs

The output of the following CLI command has been enhanced in support of the feature.

show lma-service all

The following **show lma-service all** CLI command now includes the configured heartbeat monitor max peers value.

On configuring the new CLI – heartbeat monitor-max-peers:

```
show lma-service all
  Heartbeat Support:        Enabled
  Heartbeat Interval:       60
  Heartbeat Retransmission timeout: 1
  Heartbeat Max Retransmissions: 1
  Heartbeat Monitor Max Peers: 128000
```

On configuring the default CLI – default heartbeat monitor-max-peers

```
show lma-service all
  Heartbeat Support:        Enabled
  Heartbeat Interval:       60
  Heartbeat Retransmission timeout: 1
  Heartbeat Max Retransmissions: 1
  Heartbeat Monitor Max Peers: 256
```

Restrictions:

- A maximum of 128000 PMIP sessions can be monitored with the new CLI.
- The following CLI restrictions are added for configuring **heartbeat monitor-max-peers** CLI command.

  At service startup time (boxer configuration boot):

  If heartbeat interval is less than 60 seconds (for the lma-service) or retransmission timeout is less than 3 seconds (across lma-services) then the monitor-max-peers command displays a configuration error and the monitor-max-peers configuration is not applied and vice-versa.

  At the time of updating the Service configuration:

  - While configuring the heartbeat interval of less than 60 seconds if the monitor-max-peers is already configured in that lma-service or across lma-services then it displays a configuration error.
  - While configuring a heartbeat retransmission timeout of less than 3 seconds if the monitor-max-peers is already configured in that lma-service or across lma-services then it displays a configuration error.
  - While configuring monitor-max-peers if that lma-service or across lma-services has a heartbeat interval of less than 60 seconds or the heartbeat retransmission timeout is less than 3 seconds, then it displays a configuration error.

    CLI error displayed:

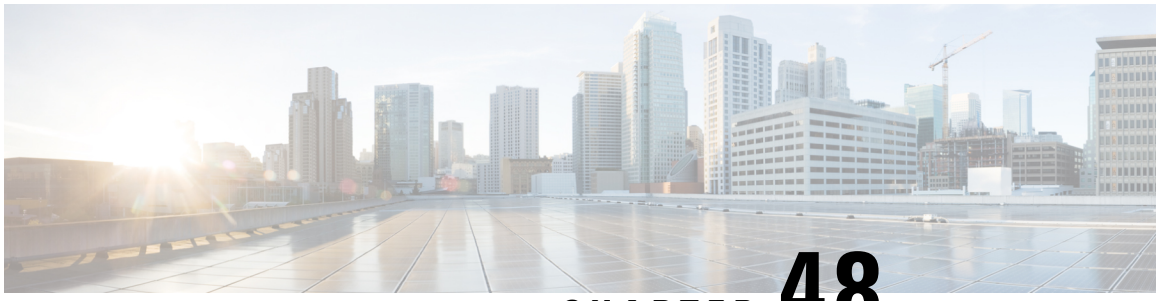
```
configure
contex pgw
lma-service lmav6
heartbeat interval 40
heartbeat monitor-max-peers
Failure: Recommended heartbeat interval: 60+, retransmission timeout: 3+, to
configure monitor-max-peers. Please retry.
heartbeat retransmission timeout 2
heartbeat monitor-max-peers
Failure: Recommended heartbeat interval: 60+, retransmission timeout: 3+, to
configure monitor-max-peers. Please retry.
end
```

```
configure
contex pgw
lma-service lmav6
heartbeat interval 60
heartbeat retransmission timeout 3
heartbeat monitor-max-peers
heartbeat interval 40
Failure: Recommended heartbeat interval: 60+, in presence of monitor-max-peers.
Please retry.
heartbeat retransmission timeout 2
Failure: Recommended heartbeat retransmission timeout: 3+, in presence of
monitor-max-peers. Please retry.
end
```

- Unusual logs are displayed as follows when there is more than 10% path failure and there is a delay in the detection of path failure.

  ```
  "Retransmissons list size exceeds than expected, hb message will be sent with
  periodicty of configured HB interval for callid 20016"
  ```

show lma-service all



CHAPTER 48

Inline TCP Optimization

This chapter includes the following topics:

- Feature Summary and Revision History, on page 857
- Feature Description, on page 858
- How It Works, on page 858
- Configuring Inline TCP Optimization, on page 859
- Monitoring and Troubleshooting, on page 863

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
In this release, the throughput gain has been increased. KPIs - separate counters for IP versions (IPv4/IPv6) and application protocols (HTTP/HTTPs), are added.	21.10

Revision Details	Release
In this release, two new commands - **accl-flags** and **cwnd-gain**, are added to the TCP Acceleration Profile Parameters configuration. Configuring these commands increases throughput gain and optimized mid-flow proxy engagement procedures for TCP accelerated flows. Also, the output for the **show tcp-acceleration-profile** command has been updated.	21.9.1
Inline TCP Optimization engine is enhanced to dynamically engage the TCP acceleration module at mid-flow.	21.9
First introduced.	21.8

Feature Description

Inline TCP Optimization is an integrated solution to service providers to increase the TCP flow throughput for TCP connections. This solution enables faster transmission of data for a better user experience.

The Inline TCP Optimization solution ensures accelerated TCP flows using a proprietary algorithm that provides efficient and optimal throughput at a given time. A TCP proxy has been integrated with this solution to monitor and control the TCP congestion window for optimal throughput.

The Inline TCP Optimization solution also supports split TCP sessions to accommodate wireless requirements and provides feature parity with other existing inline services.

Note Optimization only applies to the downlink data on the Gn interface.

The Inline TCP Optimization feature is license controlled. 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

The TCP Optimization feature includes the following functionalities:

- TCP Connection Splicing: The TCP connections are split into two connections; one connection towards Gn and the other connection towards Gi, inside P-GW. The connections are split in a transparent manner in the P-GW so that the UE and the Gi servers are transparent to the connection being split.
- TCP Proxy ensures seamless movement of data across these two TCP split connections.
- TCP Optimization is deployed on the Gn interface (towards the UE) of the TCP stack. A user-space TCP stack in P-GW is used.
- Cisco library for TCP optimization:
  - Provides algorithms that are designed to increase the TCP throughput.

- Interfaces with the User-space TCP stack (Gn interface) and notifies appropriate events that occur in the TCP connection and takes actions accordingly.
- Provides APIs to integrate the Cisco Library (for TCP optimization) and StarOS.



Note TCP Acceleration is enabled during the start of the TCP flow (when SYN packet is received). It cannot be disabled later during the flow.

Accelerating Selected TCP Flows

The Inline TCP Optimization solution is designed to optimize most-eligible TCP flows.

The following are a few criteria to select TCP flows for acceleration:

- Based on the amount of data seen on the flow: Flows that have data more than that of the threshold value are accelerated.
- TCP acceleration is avoided in certain scenarios for throttled TCP flows. For example:
  - ADC flows that configured to be throttled.
  - TCP flows throttled due to breaching data limit triggered by OCS/PCRF.
  - Tethered flows that are throttled.
- Based on GBR/non-GBR: Only TCP flows on default bearers is applicable for TCP acceleration.



Note TCP acceleration is only supported for LTE RAT-Type.

Configuring Inline TCP Optimization

Enabling TCP Acceleration under Active Charging Service

Use the following configuration to enable TCP acceleration:

```
configure
  require active-charging
  active-charging service service_name
    tcp-acceleration
    end
```

NOTES:

- **tcp-acceleration**: Enables TCP acceleration under the ACS Configuration mode.

Enabling TCP Acceleration under Trigger Action

Use the following configuration to enable TCP acceleration:

```
configure
   require active-charging
   active-charging service service_name
      trigger-action trigger_action_name
         tcp-acceleration profile profile_name
         end
```

NOTES:

- **tcp-acceleration**: Enables TCP acceleration under the ACS Trigger Action Configuration mode.
- **profile**: Identifies the TCP acceleration profile. The *profile_name* is a string ranging from 1 to 63 characters.

Configuring a TCP Acceleration Profile

Use the following configuration to configure a TCP Acceleration Profile:

```
configure
   require active-charging
   active-charging service service_name
      [ no ] tcp-acceleration-profile profile_name
      end
```

NOTES:

- **tcp-acceleration-profile**: Configures the TCP Acceleration feature profile for inline TCP optimization.
- **no**: Disables the TCP Acceleration profile.

Configuring TCP Acceleration Profile Parameters

Use the following commands to configure the TCP acceleration profile parameters:

```
configure
   require active-charging
   active-charging service service_name
      [ no ] tcp-acceleration-profile profile_name
         accl-flags flag_value
         default accl-flags
        buffer-size { [ downlink [ 128KB | 256KB | 512KB | 1024KB | 1536KB
 | 2048KB | 2560KB | 3072KB | 3584KB | 4096KB ] [ uplink [ 128KB | 256KB
 | 512KB | 1024KB | 1536KB | 2048KB | 2560KB | 3072KB | 3584KB | 4096KB
] ] ] | [ uplink [ 128KB | 256KB | 512KB | 1024KB | 1536KB | 2048KB |
2560KB | 3072KB | 3584KB | 4096KB ] [ downlink [ 128KB | 256KB | 512KB |
 1024KB | 1536KB | 2048KB | 2560KB | 3072KB | 3584KB | 4096KB ] ] ] }
         cwnd-gain { dynamic { off | on } [ factor factor_value ] | factor
factor_value [ dynamic { off | on } ] }
         default cwnd-gain
```

```
default buffer-size [ downlink | uplink ]
initial-cwnd-size window_size
default initial-cwnd-size
max-rtt max_rtt_value
default max-rtt
mss mss_value
default mss
end
```

NOTES:

- **default**: Assigns or restores default values to its following commands.
- **accl-flags**: Configures TCP acceleration related optimization flags. The flag_value is an integer ranging from 0 to 65535.
- **buffer-size**: Configures the TCP Proxy buffer size for downlink and uplink data in Kilobytes.

Note This command is supported from 21.9.1 and later releases

- **cwnd-gain**: Configures the TCP congestion window gain. This command is used by the TCP optimization engine to continuously calculate the actual congestion window size. Scaling the window size allows the TCP optimization engine to manage the in-flight of data in the engine.
  - The **dynamic** option in this command automatically scales-up the congestion window gain to ensure that it is sized correctly to allow for RTT variation during the flow.
  - The **factor** option configures the TCP congestion window gain factor. The *factor_value* is an integer ranging from 1 to 16378.

Note This command is supported from 21.9.1 and later releases

- **initial-cwnd-size**: Configures the initial congestion window size in segments. The *window_size* is an integer ranging from 1 to 65535.
- **max-rtt**: Configures the maximum RTT value in milliseconds. The *max_rtt_value* is an integer ranging from 1 to 10000.
- **mss**: Configures the maximum segment size for TCP in Bytes. The *mss_value* is an integer ranging from 496 to 65535.

Configuring Post-Processing Rule Name under Trigger Condition

Use the following commands to configure the post-processing rule names:

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      post-processing-rule-name { = | contains | ends-with | starts-with
```

```
} rule_name
      [ no ] post-processing-rule-name rule_name
      end
```

NOTES:

- **post-processing-rule-name**: Sets condition for a particular post-processing rule. The following operators specify how the rules are matched:
  - **=**: Equals
  - **!=**: Not Equals
  - **contains**: Contains
  - **ends-with**: Ends with.
  - **starts-with**: Starts with
- *name*: Specifies the name of the post-processing rule.

Configuring TCP Acceleration Related EDR Attributes

Use the following configuration to configure the EDR attributes:

```
configure
  require active-charging
  active-charging service service_name
    edr-format edr_format_name
      rule-variable tcp [ sn-tcp-accl | sn-tcp-accl-reject-reason |
sn-tcp-min-rtt | sn-tcp-rtt ] priority priority_value
      end
```

NOTES:

- **rule variable**: Assigns a rule variable attributes for EDR or UDR.
- **tcp**: Specifies Transmission Control Protocol (TCP) related fields.
  - **sn-tcp-accl**: Specifies the TCP Acceleration status for the TCP flow.
    - **0**: TCP Acceleration is not enabled on the flow.
    - **1**: TCP Acceleration is enabled on the flow.
    - **2**: Flow is eligible and attempted, but not TCP Accelerated.
    - **3**: Flow is eligible, but not attempted for TCP Acceleration
  - **sn-tcp-accl-reject-reason**: Specifies reason for not accelerating the TCP flow.
  - **sn-tcp-min-rtt**: Specifies min RTT observed for accelerated TCP flow.
  - **sn-tcp-rtt**: Specifies smoothed RTT for accelerated TCP flow.
- **priority**: Specifies the CSV position of the field (protocol rule) in the EDR. Priority must be an integer from 1 through 65535.

Configuring Flow Length Threshold for a TCP Flow under Trigger Action

The flow length threshold of a TCP flow is configured using Trigger Action under the service-scheme framework. The threshold value of the flow length is used to engage the TCP Acceleration module dynamically.

Use the following configuration to engage TCP acceleration module during mid-flow:

```
configure
  require active-charging
  active-charging service service_name
    trigger-action trigger_action_name
      tcp-acceleration flow-length threshold threshold_value
      no tcp-acceleration flow-length threshold
      end
```

NOTES:

- **no**: Disables flow recovery for a trigger-action.
- **flow-length**: Specifies the flow length action for a TCP flow.
- **threshold**: Specifies the threshold value of the flow length in bytes, for a TCP flow. The threshold value is an integer ranging from 1 to 10000 bytes.

Configuring a Flow Length Threshold Exceeded for a TCP Flow under Trigger Condition

The flow length condition **exceed** for a TCP flow is configured using Trigger Condition under the service-scheme framework.

Use the following configuration to configure a condition for a TCP flow length:

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      flow-length threshold exceed
      end
```

NOTES:

- **flow-length**: Specifies the flow length condition for a TCP flow.
- **threshold**: Specifies the threshold value configured in the trigger-action configuration.
- **exceed**: Invokes the exceed condition when the flow length is exceeded.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

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

show configuration

The output of this command displays the following fields for this feature::

- tcp-acceleration
- tcp-accelration profile tap
- buffer-size downlink *size* uplink *size*
- initial-cwnd-size
- max-rtt
- mss

show tcp-acceleration-profile { [all] | [name *profile-name*] }

The output of this command displays the following fields for this feature:

- TCP Acceleration Profile Name
  - Initial Congestion Window
  - Max RTT
  - MSS
  - Buffer Size (Downlink)
  - Buffer Size (Uplink)
  - Cwnd Gain Factor
  - Cwnd Gain Dynamic
  - Accl Flags
- Total tcp-acceleration-profile found

show active-charging tcp-acceleration info

The output of this command displays the following fields for this feature:

- TCP Acceleration Library Information
  - Version

show active-charging tcp-acceleration statistics sessmgr all

The output of this command displays the following fields for this feature:

- TCP acceleration Statistics

- Total Accelerated Flows
- Current Accelerated Flows
- Released Accelerated Flows
- Rejected Accelerated Flows
  - Feature Not Supported
  - RAT Type Not Supported
  - Bearer Not Supported
  - Resource Not Available (Memory)
  - Others
- Subscriber Level Statistics
  - Total Accelerated Subscribers
  - Current Accelerated Subscribers
- Protocol Level Statistics
  - Total Flows (IPv4 and IPv6)
    - TCP
    - HTTP
    - HTTPS
  - Active Flows (IPv4 and IPv6)
    - TCP
    - HTTP
    - HTTPS
  - Current Idle Flows (IPv4 and IPv6)
    - TCP
    - HTTP
    - HTTPS
  - Clearer by Idle Timer (IPv4 and IPv6)
    - TCP
    - HTTP
    - HTTPS

- Control Statistics
  - IPv4 (User-Side and Inet-Side)
    - TCP Terminations Rx
    - TCP Terminations Tx
  - IPv6 (User-Side and Inet-Side)
    - TCP Terminations Rx
    - TCP Terminations Tx
- Data Statistics
  - IPv4 (User-Side and Inet-Side)
    - Total Pkts Rx
    - Total Bytes Rx
    - Total Pkts Tx
    - Total Bytes Tx
    - HTTP (User-Side and Inet-Side)
      - Total Pkts Rx
      - Total Bytes Rx
      - Total Pkts Tx
      - Total Bytes Tx
      - Retrans Pkts Rx
      - Retrans Bytes Rx
      - Retrans Pkts Tx
      - Retrans Bytes Tx
    - HTTPS (User-Side and Inet-Side)
      - Total Pkts Rx
      - Total Bytes Rx
      - Total Pkts Tx
      - Total Bytes Tx
      - Retrans Pkts Rx
      - Retrans Bytes Rx
      - Retrans Pkts Tx
      - Retrans Bytes Tx

- IPv6 (User-Side and Inet-Side)
  - Total Pkts Rx
  - Total Bytes Rx
  - Total Pkts Tx
  - Total Bytes Tx
  - HTTP (User-Side and Inet-Side)
    - Total Pkts Rx
    - Total Bytes Rx
    - Total Pkts Tx
    - Total Bytes Tx
    - Retrans Pkts Rx
    - Retrans Bytes Rx
    - Retrans Pkts Tx
    - Retrans Bytes Tx
  - HTTPS (User-Side and Inet-Side)
    - Total Pkts Rx
    - Total Bytes Rx
    - Total Pkts Tx
    - Total Bytes Tx
    - Retrans Pkts Rx
    - Retrans Bytes Rx
    - Retrans Pkts Tx
    - Retrans Bytes Tx

show active-charging flows full all

The output of this command displays the following fields for this feature::

- TCP Acceleration

show active-charging trigger-action name *trigger_action_name*

On executing the above command, the following new field(s) are displayed for this feature:

- TCP Acceleration

- TCP Acceleration Treshold

show active-charging trigger-condition name *name*

The output of this command displays the following fields for this feature:

- Post-Processing Rule-name/GOR
- Flow-Length Threshold exceed

Bulk Statistics

The following bulk statistics are added in the **CUSP** schema in support of the Inline TCP Optimization (Phase 2) feature.

Bulk Statistics	Description
tcpaccl-totflows	Indicates the total number of TCP accelerated flows.
tcpaccl-currflows	Indicates the number of current TCP accelerated flows.
tcpaccl-usr-ipv4totpkts-rx	Indicates the total number of IPv4 TCP accelerated packets received from the UE.
tcpaccl-usr-ipv4totbytes-rx	Indicates the total number of IPv4 TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv4totpkts-tx	Indicates the total number of IPv4 TCP accelerated packets sent towards the UE.
tcpaccl-usr-ipv4totbytes-tx	Indicates the total number of IPv4 TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv4totpkts-rx	Indicates the total number of IPv4 TCP accelerated packets received from the internet.
tcpaccl-inet-ipv4totbytes-rx	Indicates the total number of IPv4 TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv4totpkts-tx	Indicates the total number of IPv4 TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv4totbytes-tx	Indicates the total number of IPv4 TCP accelerated bytes sent towards the internet.
tcpaccl-usr-ipv6totpkts-rx	Indicates the total number of IPv6 TCP accelerated packets received from the UE.
tcpaccl-usr-ipv6totbytes-rx	Indicates the total number of IPv6 TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv6totpkts-tx	Indicates the total number of IPv6 TCP accelerated packets sent towards the UE.

Bulk Statistics	Description
tcpaccl-usr-ipv6totbytes-tx	Indicates the total number of IPv6 TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv6totpkts-rx	Indicates the total number of IPv6 TCP accelerated packets received from the internet.
tcpaccl-inet-ipv6totbytes-rx	Indicates the total number of IPv6 TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv6totpkts-tx	Indicates the total number of IPv6 TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv6totbytes-tx	Indicates the total number of IPv6 TCP accelerated bytes sent towards the internet.

The following bulk statistics are added in the **CUSP** schema in support of the Inline TCP Optimization (Phase 3) feature.

Bulk Statistics	Descriptions
tcpaccl-tot-subs	Indicates the total number of subscribers with atleast one TCP accelerated flow.
tcpaccl-curr-subs	Indicates the current number of active subscribers with atleast one TCP accelerated flow.
tcpaccl-ipv4-tot-tcp-flows	Indicates the total number of TCP accelerated IPv4 flows.
tcpaccl-ipv6-tot-tcp-flows	Indicates the total number of TCP accelerated IPv6 flows.
tcpaccl-ipv4-tot-http-flows	Indicates the total number of TCP accelerated IPv4 HTTP flows.
tcpaccl-ipv6-tot-http-flows	Indicates the total number of TCP accelerated IPv6 HTTP flows.
tcpaccl-ipv4-tot-https-flows	Indicates the total number of TCP accelerated IPv4 HTTPS flows.
tcpaccl-ipv6-tot-https-flows	Indicates the total number of TCP accelerated IPv6 HTTPS flows.
tcpaccl-ipv4-curr-tcp-flows	Indicates the current number of active TCP accelerated IPv4 flows.
tcpaccl-ipv6-curr-tcp-flows	Indicates the current number of active TCP accelerated IPv6 flows.
tcpaccl-ipv4-curr-http-flows	Indicates the current number of active TCP accelerated IPv4 HTTP flows.

Bulk Statistics	Descriptions
tcpaccl-ipv6-curr-http-flows	Indicates the current number of active TCP accelerated IPv6 HTTP flows.
tcpaccl-ipv4-curr-https-flows	Indicates the current number of active TCP accelerated IPv4 HTTPS flows.
tcpaccl-ipv6-curr-https-flows	Indicates the current number of active TCP accelerated IPv6 HTTPS flows.
tcpaccl-ipv4-curr-tcp-idleflows	Indicates the current number of idle TCP accelerated IPv4 flows.
tcpaccl-ipv6-curr-tcp-idleflows	Indicates the current number of idle TCP accelerated IPv6 flows.
tcpaccl-ipv4-curr-http-idleflows	Indicates the current number of idle TCP accelerated IPV4 HTTP flows.
tcpaccl-ipv6-curr-http-idleflows	Indicates the current number of idle TCP accelerated IPV6 HTTP flows.
tcpaccl-ipv4-curr-https-idleflows	Indicates the current number of idle TCP accelerated IPV4 HTTPS flows.
tcpaccl-ipv6-curr-https-idleflows	Indicates the current number of idle TCP accelerated IPV6 HTTPS flows.
tcpaccl-ipv4-tcp-flows-idle-timeout	Indicates the total number of TCP accelerated IPv4 flows that are cleared due to idle timeout.
tcpaccl-ipv6-tcp-flows-idle-timeout	Indicates the total number of TCP accelerated IPv6 flows that are cleared due to idle timeout.
tcpaccl-ipv4-http-flows-idle-timeout	Indicates the total number of TCP accelerated IPv4 HTTP flows that are cleared due to idle timeout.
tcpaccl-ipv6-http-flows-idle-timeout	Indicates the total number of TCP accelerated IPv6 HTTP flows that are cleared due to idle timeout.
tcpaccl-ipv4-https-flows-idle-timeout	Indicates the total number of TCP accelerated IPv4 HTTPS flows that are cleared due to idle timeout.
tcpaccl-ipv6-https-flows-idle-timeout	Indicates the total number of TCP accelerated IPv6 HTTPS flows that are cleared due to idle timeout.
tcpaccl-usr-ipv4-tcpterm-rx	Indicates the total number of TCP Reset termination request received from UE for TCP accelerated IPV4 flows.
tcpaccl-usr-ipv6-tcpterm-rx	Indicates the total number of TCP Reset termination request received from UE for TCP accelerated IPV6 flows.

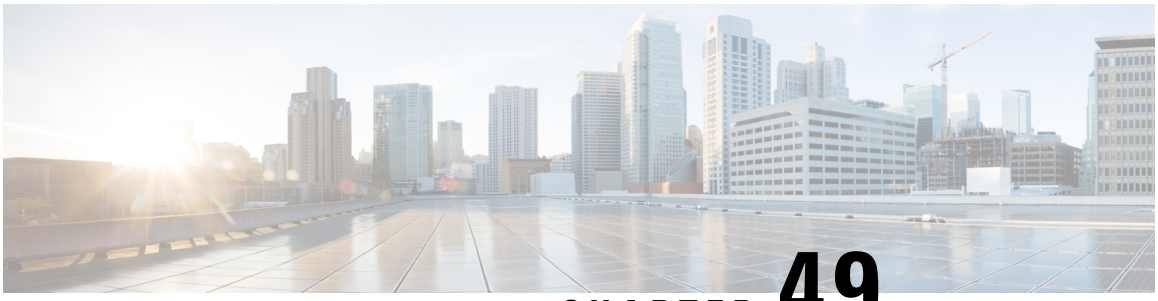
Bulk Statistics	Descriptions
tcpaccl-usr-ipv4-tcpterm-tx	Indicates the total number of TCP Reset termination request sends towards UE for TCP accelerated IPV4 flows.
tcpaccl-usr-ipv6-tcpterm-tx	Indicates the total number of TCP Reset termination request sends towards UE for TCP accelerated IPV6 flows.
tcpaccl-inet-ipv4-tcpterm-rx	Indicates the total number of TCP Reset termination request received from server for TCP accelerated IPV4 flows.
tcpaccl-inet-ipv6-tcpterm-rx	Indicates the total number of TCP Reset termination request received from server for TCP accelerated IPV6 flows.
tcpaccl-inet-ipv4-tcpterm-tx	Indicates the total number of TCP Reset termination request sends towards server for TCP accelerated IPV4 flows.
tcpaccl-inet-ipv6-tcpterm-tx	Indicates the total number of TCP Reset termination request sends towards server for TCP accelerated IPV6 flows.
tcpaccl-usr-ipv4-http-totpkts-rx	Indicates the total number of IPv4 HTTP TCP accelerated packets received from the UE.
tcpaccl-usr-ipv4-http-totbytes-rx	Indicates the total number of IPv4 HTTP TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv4-http-totpkts-tx	Indicates the total number of IPv4 HTTP TCP accelerated packets sent towards the UE.
tcpaccl-usr-ipv4-http-totbytes-tx	Indicates the total number of IPv4 HTTP TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv4-http-totpkts-rx	Indicates the total number of IPv4 HTTP TCP accelerated packets received from the internet.
tcpaccl-inet-ipv4-http-totbytes-rx	Indicates the total number of IPv4 HTTP TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv4-http-totpkts-tx	Indicates the total number of IPv4 HTTP TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv4-http-totbytes-tx	Indicates the total number of IPv4 HTTP TCP accelerated bytes sent towards the internet.
tcpaccl-usr-ipv6-http-totpkts-rx	Indicates the total number of IPv6 HTTP TCP accelerated packets received from the UE.

Bulk Statistics	Descriptions
tcpaccl-usr-ipv6-http-totbytes-rx	Indicates the total number of IPv6 HTTP TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv6-http-totpkts-tx	Indicates the total number of IPv6 HTTP TCP accelerated packets sent towards the UE.
tcpaccl-usr-ipv6-http-totbytes-tx	Indicates the total number of IPv6 HTTP TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv6-http-totpkts-rx	Indicates the total number of IPv6 HTTP TCP accelerated packets received from the internet.
tcpaccl-inet-ipv6-http-totbytes-rx	Indicates the total number of IPv6 HTTP TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv6-http-totpkts-tx	Indicates the total number of IPv6 HTTP TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv6-http-totbytes-tx	Indicates the total number of IPv6 HTTP TCP accelerated bytes sent towards the internet.
tcpaccl-usr-ipv4-https-totpkts-rx	Indicates the total number of IPv4 HTTPS TCP accelerated packets received from the UE.
tcpaccl-usr-ipv4-https-totbytes-rx	Indicates the total number of IPv4 HTTPS TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv4-https-totpkts-tx	Indicates the total number of IPv4 HTTPS TCP accelerated packets sent towards the UE.
tcpaccl-usr-ipv4-https-totbytes-tx	Indicates the total number of IPv4 HTTPS TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv4-https-totpkts-rx	Indicates the total number of IPv4 HTTPS TCP accelerated packets received from the internet.
tcpaccl-inet-ipv4-https-totbytes-rx	Indicates the total number of IPv4 HTTPS TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv4-https-totpkts-tx	Indicates the total number of IPv4 HTTPS TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv4-https-totbytes-tx	Indicates the total number of IPv4 HTTPS TCP accelerated bytes sent towards the internet.
tcpaccl-usr-ipv6-https-totpkts-rx	Indicates the total number of IPv6 HTTPS TCP accelerated packets received from the UE.
tcpaccl-usr-ipv6-https-totbytes-rx	Indicates the total number of IPv6 HTTPS TCP accelerated bytes received from the UE.
tcpaccl-usr-ipv6-https-totpkts-tx	Indicates the total number of IPv6 HTTPS TCP accelerated packets sent towards the UE.

Bulk Statistics	Descriptions
tcpaccl-usr-ipv6-https-totbytes-tx	Indicates the total number of IPv6 HTTPS TCP accelerated bytes sent towards the UE.
tcpaccl-inet-ipv6-https-totpkts-rx	Indicates the total number of IPv6 HTTPS TCP accelerated packets received from the internet.
tcpaccl-inet-ipv6-https-totbytes-rx	Indicates the total number of IPv6 HTTPS TCP accelerated bytes received from the internet.
tcpaccl-inet-ipv6-https-totpkts-tx	Indicates the total number of IPv6 HTTPS TCP accelerated packets sent towards the internet.
tcpaccl-inet-ipv6-https-totbytes-tx	Indicates the total number of IPv6 HTTPS TCP accelerated bytes sent towards the internet.
tcpaccl-usr-ipv4-http-pktsretrans-tx	Indicates the total number of packets retransmitted towards the UE for TCP accelerated IPV4 HTTP flows.
tcpaccl-usr-ipv4-http-pktsretrans-rx	Indicates the total number of retransmitted packets received from the UE for TCP accelerated IPV4 HTTP flows.
tcpaccl-usr-ipv4-http-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the UE for TCP accelerated IPV4 HTTP flows.
tcpaccl-usr-ipv4-http-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the UE for TCP accelerated IPV4 HTTP flows.
tcpaccl-inet-ipv4-http-pktsretrans-tx	Indicates the total number of packets retransmitted towards the server for TCP accelerated IPV4 HTTP flows.
tcpaccl-inet-ipv4-http-pktsretrans-rx	Indicates the total number of retransmitted packets received from the server for TCP accelerated IPV4 HTTP flows.
tcpaccl-inet-ipv4-http-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the server for TCP accelerated IPV4 HTTP flows.
tcpaccl-inet-ipv4-http-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the server for TCP accelerated IPV4 HTTP flows.
tcpaccl-usr-ipv6-http-pktsretrans-tx	Indicates the total number of packets retransmitted towards the UE for TCP accelerated IPV6 HTTP flows.

Bulk Statistics	Descriptions
tcpaccl-usr-ipv6-http-pktsretrans-rx	Indicates the total number of retransmitted packets received from the UE for TCP accelerated IPV6 HTTP flows.
tcpaccl-usr-ipv6-http-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the UE for TCP accelerated IPV6 HTTP flows.
tcpaccl-usr-ipv6-http-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the UE for TCP accelerated IPV6 HTTP flows.
tcpaccl-inet-ipv6-http-pktsretrans-tx	Indicates the total number of packets retransmitted towards the server for TCP accelerated IPV6 HTTP flows.
tcpaccl-inet-ipv6-http-pktsretrans-rx	Indicates the total number of retransmitted packets received from the server for TCP accelerated IPV6 HTTP flows.
tcpaccl-inet-ipv6-http-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the server for TCP accelerated IPV6 HTTP flows.
tcpaccl-usr-ipv4-https-pktsretrans-tx	Indicates the total number of packets retransmitted towards the UE for TCP accelerated IPV4 HTTPS flows.
tcpaccl-usr-ipv4-https-pktsretrans-rx	Indicates the total number of retransmitted packet received from the UE for TCP accelerated IPV4 HTTPS flows.
tcpaccl-usr-ipv4-https-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the UE for TCP accelerated IPV4 HTTPS flows.
tcpaccl-usr-ipv4-https-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the UE for TCP accelerated IPV4 HTTPS flows.
tcpaccl-inet-ipv4-https-pktsretrans-tx	Indicates the total number of packets retransmitted towards the server for TCP accelerated IPV4 HTTPS flows.
tcpaccl-inet-ipv4-https-pktsretrans-rx	Indicates the total number of retransmitted packet received from the server for TCP accelerated IPV4 HTTPS flows.
tcpaccl-inet-ipv4-https-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the server for TCP accelerated IPV4 HTTPS flows.

Bulk Statistics	Descriptions
tcpaccl-inet-ipv4-https-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the server for TCP accelerated IPV4 HTTPS flows.
tcpaccl-usr-ipv6-https-pktsretrans-tx	Indicates the total number of retransmitted bytes received from the server for TCP accelerated IPV4 HTTPS flows.
tcpaccl-usr-ipv6-https-pktsretrans-tx	Indicates the total number of packets retransmitted towards the UE for TCP accelerated IPV6 HTTPS flows.
tcpaccl-usr-ipv6-https-pktsretrans-rx	Indicates the total number of retransmitted packets received from the UE for TCP accelerated IPV6 HTTPS flows.
tcpaccl-usr-ipv6-https-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the UE for TCP accelerated IPV6 HTTPS flows.
tcpaccl-usr-ipv6-https-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the UE for TCP accelerated IPV6 HTTPS flows.
tcpaccl-inet-ipv6-https-pktsretrans-tx	Indicates the total number of packets retransmitted towards the server for TCP accelerated IPV6 HTTPS flows.
tcpaccl-inet-ipv6-https-pktsretrans-rx	Indicates the total number of retransmitted packets received from the server for TCP accelerated IPV6 HTTPS flows.
tcpaccl-inet-ipv6-https-bytesretrans-tx	Indicates the total number of bytes retransmitted towards the server for TCP accelerated IPV6 HTTPS flows.
tcpaccl-inet-ipv6-https-bytesretrans-rx	Indicates the total number of retransmitted bytes received from the server for TCP accelerated IPV6 HTTPS flows.



CHAPTER 49

Inter-MME Handover for Modify Bearer Requests without S11-U TEID

- Feature Summary an Revision History, on page 877
- Feature Description, on page 878
- How it Works, on page 878
- Configuring Inter-MME Handover for Modify Bearer Requests without S11-U TEID, on page 880
- Monitoring and Troubleshooting, on page 881

Feature Summary an Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

During NB-IoT/Control Plane CIoT EPS Optimization, user data gets transported or SMS messages are passed through MME. This is done by encapsulating them in Non-Access Stratum (NAS), reducing the total number of Control Plane messages when handling a short data transaction. If the Control Plane CIoT EPS Optimization applies, then the MME.

- Indicates S11 interface User Plane (S11-U) tunneling of the NAS user data and sends its own S11-U IP address and MME DL Tunnel End Point Identifier (TEID) for Downlink (DL) data forwarding to the S-GW.
- The S-GW returns a Create Session Response, for Control Plane CIoT EPS optimization, with the S-GW address for S11-U and S-GW TEID. They are used by the MME to forward the Uplink (UL) data toward the S-GW.

In such instances, there might be following constraints:

- S-GW validates Modify Bearer requests (MBR) without S11-U F-TEID.
- If there is no S11-U F-TEID in the MBR, then the S-GW rejects the Inter-MME Handover (HO), since F-TEID is considered mandatory when S11TF flag is set.

To overcome the above constraints and to address the requirements of the IoT devices, the S-GW supports Inter-MME Handover Modify Bearer Requests, without the S11-U TEID functionality, for the NB-IoT subscribers.

How it Works

When the feature is enabled under S-GW Service Configuration mode, the following validation takes place:

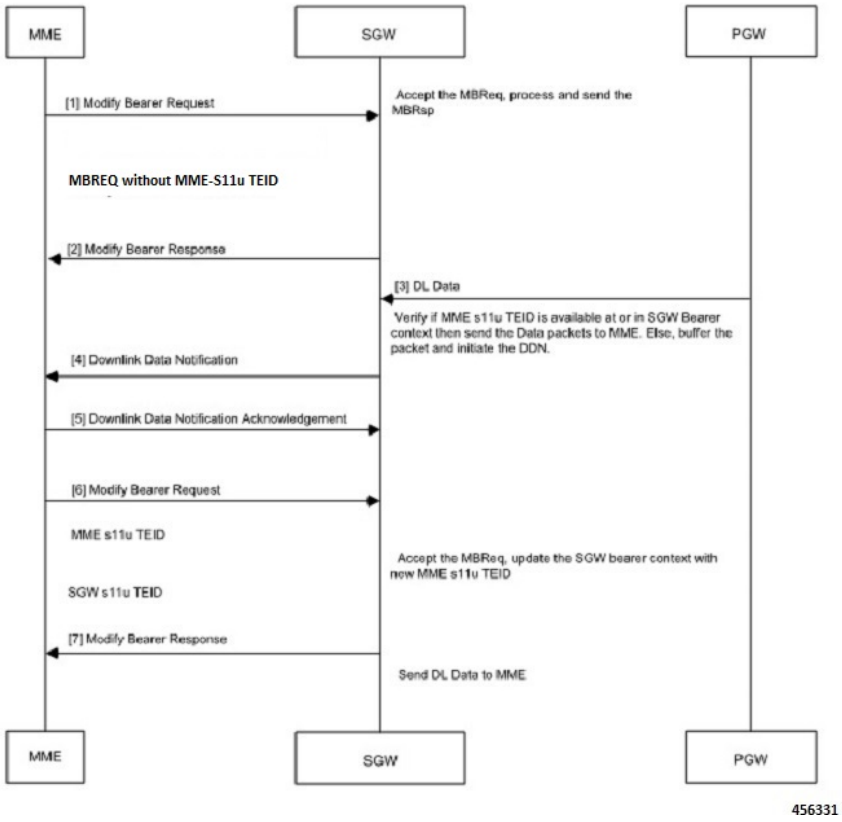
- Handling of IE validation at EGTP Protocol
- Downlink data handling
- Uplink data handling

Call Flow

Handling IE Validation at EGTP Protocol: When Handling IE validation at EGTP Protocol is enabled using the **mme-s11u-without-teid** CLI command under S-GW Service Configuration mode, and the flag is set to be TRUE (default is FALSE):

- The S11-U TEID validation is bypassed.
- The S-GW accepts the Modify Bearer Request and continues the process until handover is successful.

Figure 78: Call Flow for Handling IE Validation at EGTP Protocol



The following table explains the function between MME and S-GW during initial attach procedure.

Table 86: Procedure

Step	Description
1	User Equipment (UE) sends the initial Attach to MME and establishes Control Plane CIoT optimization S11-U EPS bearer with source MME, S-GW, and P-GW.
2	UE moves to the idle state after some time.
3	Source MME releases the S11-U tunnel with S-GW due to no activity.
4	UE moves to Active state in new eNB, and sends Tracking Area Update (TAU) request to the target MME.
5	Target MME uses TAU Request and sends Context Request to source MME.
6	Source MME provides all GTP-C GTP-U F-TEID to the new target MME in Context Response.

Step	Description
7	If the target MME did not send MME GTP-U S11-U TEID, S5/S8 related information inside the Bearer Context of the Modify Bearer Request, Modify Bearer Request from target MME reaches S-GW without any information about MME S11-U TEID and S5/S8.
8	S-GW verifies the Modify Bearer Request it finds S11-U TEID is missing in the request message. As S11-U TEID is considered as mandatory IE, if S11TF flag is set in Modify Bearer Request message. S-GW does not reject modify Bearer Request even if MME S11TF flag is set but MME S11-U-Teid is not present whenever the feature CLI is enabled.

Downlink Data Handling: S-GW receives the Downlink data from P-GW. If MME S11-U TEID is not available in the S-GW bearer context or if the S11-U interface is inactive, the S-GW buffers the DL packets and initiates Downlink Data Notification to MME with the following steps.

Table 87: Procedure

Step	Description
1	Modify Bearer Request Received without MME S11-U TEID.
2	Modifiy Bearer Response sent to MME includes the S-GW S11-U TEID.
3	S-GW receives downlink Data from P-GW on S5/S8 interface.
4	Downlink Data notification is sent to MME.

Uplink Data Handling: S-GW accepts the Uplink data received from the MME and forwards the data to P-GW on S5/S8 interface. For example, the following steps occur at the time of handling Uplink data when Modify Bearer Request is received without the MME S11-U TEID.

Table 88: Procedure

Step	Description
1	Modify Bearer Request is received without MME S11-U TEID.
2	Modify Bearer Response sent to MME includes the S-GW S11-U TEID.
3	Uplink Data is received from MME on S11 interface data tunnel.
4	Uplink Data is forwarded to P-GW on S5/S8 interface data tunnel.

Configuring Inter-MME Handover for Modify Bearer Requests without S11-U TEID

Use the following configuration to enable/disable the Inter-MME Handover for Modify Bearer Requests without S11-U TEID feature.

```
configure
   context context_name
     sgw-service service_name
      [ no | default ] egtp modify-bearer-req accept mme-s11u-without-teid

         end
```

NOTES:

- **default**: Disables the feature. The feature is disabled by default.
- **egtp modify-bearer-req accept mme-s11u-without-teid** : Enables the S-GW to accept MBR without S11u TEID IE present in the Request Message.
- **no**: Disables the feature.

Verifying Inter-MME Handover for Modify Bearer Requests without S11-U TEID Feature Configuration

Use the **show sgw-services name** *sgw_service* or the **show configuration** CLI command to verify if the feature is Enabled or Disabled.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Inter-MME Handover for Modify Bearer Requests without S11-U TEID on the P-GW/S-GW.

Show Commands and Outputs

The following CLI commands are available in support of the Inter-MME Handover for Modify Bearer Requests without S11-U TEID.

show sgw-service statistics all

The output of this CLI command, and also the **show saegw-service statistics all function sgw** CLI command, has been enhanced to display the following fields.

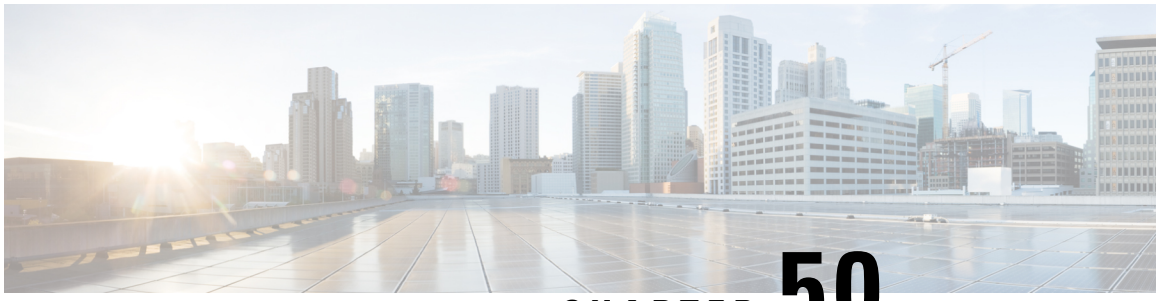
Field	Description
S11-U Buffered Data Statistics Without MME TEID:	
Uplink	Indicates the total number of Uplink data packets that are buffered. **Note** This field is not applicable for the Inter-MME Handover Modify Bearer Requests without S11-U TEID feature.
Total Pkts	Indicates the total number of packets received from MME. **Note** This field is not applicable for the Inter-MME Handover Modify Bearer Requests without S11-U TEID feature.

Field	Description
Downlink	Indicates the total number of Downlink data packets that are buffered at S-GW when there is no MME S11-U TEID.
Total Pkts	Indicates the total number of Downlink packets buffered when there is no MME S11-U TEID.

show egtpc statistics

The output of this CLI command has been enhanced to display the following fields.

Field	Description
Modify Bearer Request Without MME S11u TEID	
Total Rx	Indicates the total number of Modify Bearer Request messages received without MME S11-U TEID Information Element (IE).
Accepted	Indicates the total number of Modify Bearer Request messages accepted without MME S11-U TEID Information Element (IE).



CHAPTER 50

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, on page 883
- How it Works, on page 884
- Configuring the IPNE Feature, on page 890
- Monitoring the IPNE Service, on page 891

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.

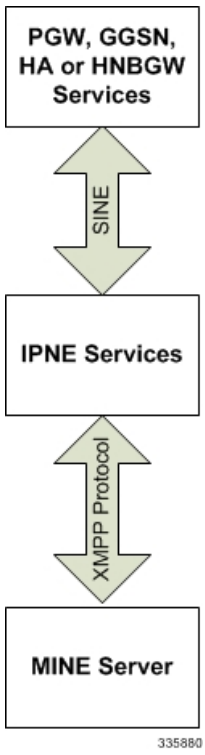
For the subscription that is installed by the IPNE client on a subscriber's call id, ECS should send a notification message to the IPNE client whenever a subscribed trigger is detected.

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 79: High-Level IPNE Architecture



The interaction takes place at the time of:

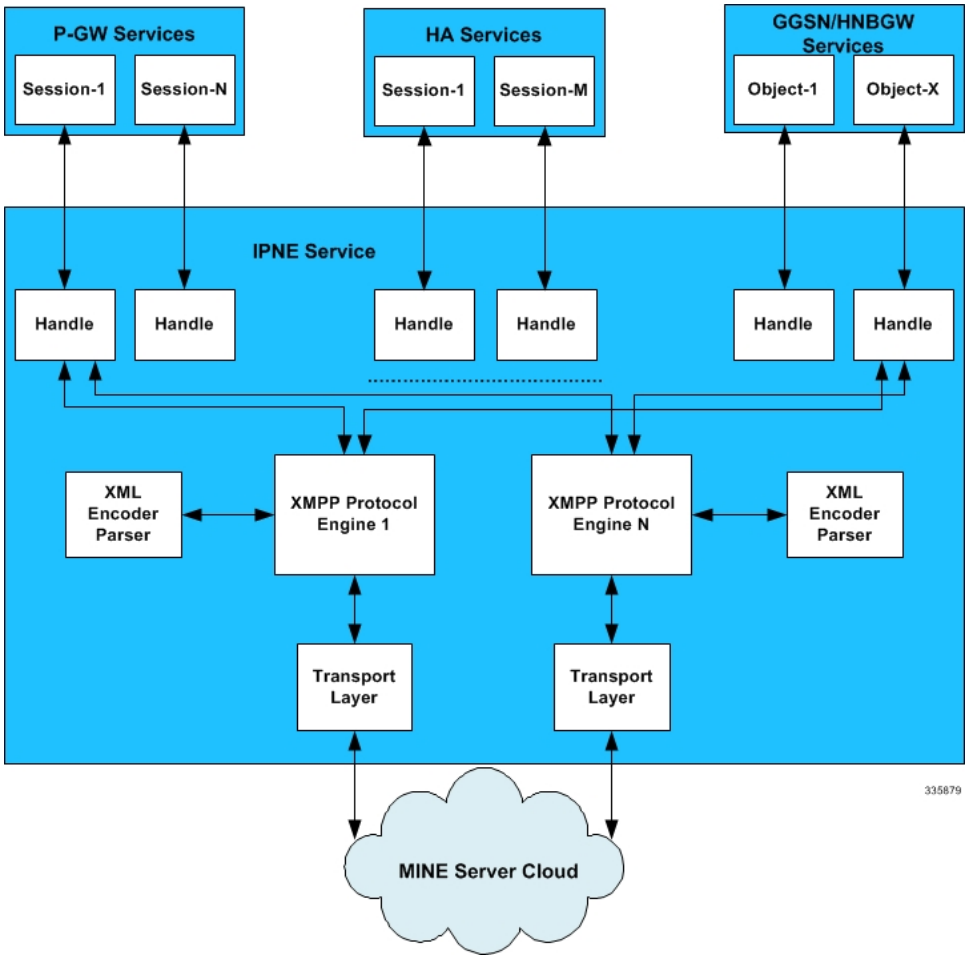
- Session setup so as to add the session information at the IPNE side
- To pass the feed messages to the MINE server
- While responding to the query request sent by the MINE server.
- Subscription notification from IPNE client to MINE server

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 80: 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 81: IPNE Handling of Query from MINE Server

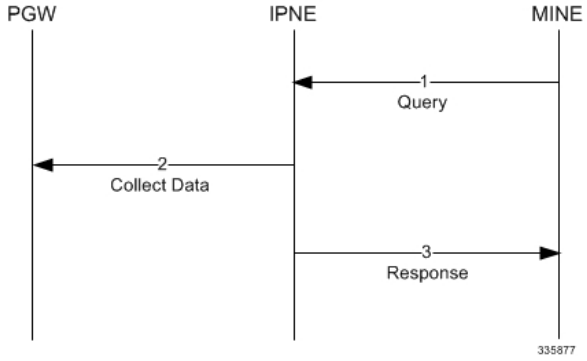


Table 89: IPNE Handling of Query from MINE Server

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 82: IPNE Service Handling a Subscription from the MINE Server

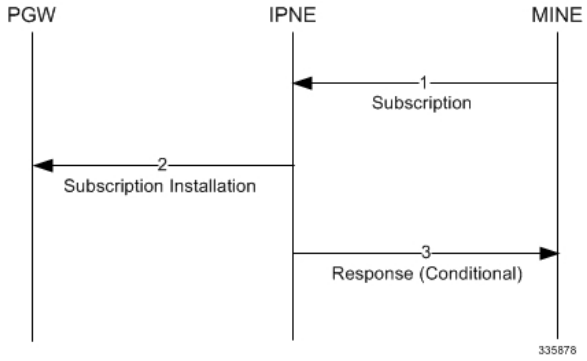


Table 90: IPNE Service Handling a Subscription from the MINE Server

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 83: IPNE Service Sends Unsolicited Feed Message to the MINE Server

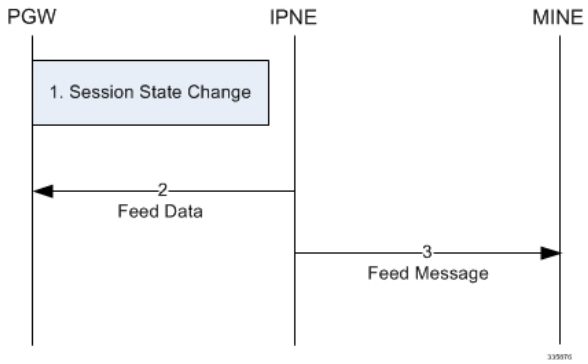


Table 91: IPNE Service Sends Unsolicited Feed Message to the MINE Server

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 84: IPNE Session Addition

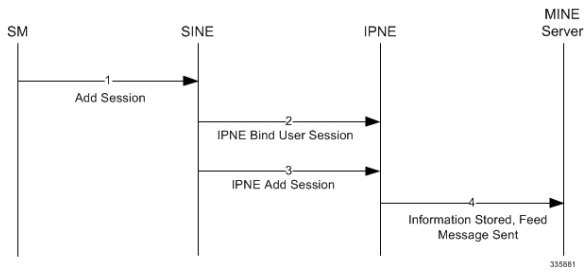


Table 92: IPNE Session Addition

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 85: IPNE Session Deletion

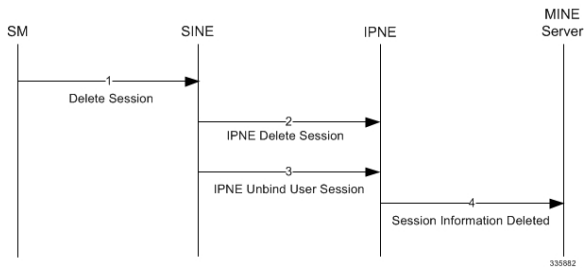


Table 93: IPNE Session Deletion

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.

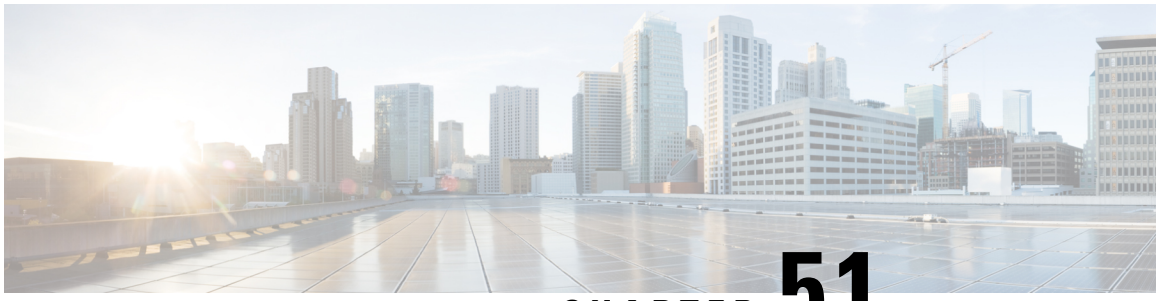
show ipne statistics all

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**.



CHAPTER 51

L2TP Access Concentrator

This chapter describes the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) functionality support on Cisco® ASR 5500 chassis 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.

Important The L2TP Access Concentrator 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*.

When enabled though the session license and feature use key, the system supports L2TP for encapsulation of data packets between it and one or more L2TP Network Server (LNS) nodes. In the system, this optional packet encapsulation, or tunneling, is performed by configuring L2TP Access Concentrator (LAC) services within contexts.

Important While establishing the L2TP session from LAC to LNS, the PPP connection for the user is established. The server uses CHAP authentication protocol to authenticate the connection. While calculating the CHAP response for the CHAP challenge received by the server, the server does not consider the CHAP password.

Important The LAC service uses UDP ports 13660 through 13668 as the source port for sending packets to the LNS.

This chapter contains the following topics:

- Applicable Products and Relevant Sections, on page 894
- Supported LAC Service Configurations for PDSN Simple IP, on page 895
- Supported LAC Service Configurations for the GGSN and P-GW, on page 899
- Supported LAC Service Configuration for Mobile IP, on page 905
- Configuring Subscriber Profiles for L2TP Support, on page 908
- Feature Description, on page 912

• Configuring LAC Services, on page 912
• Modifying PDSN Services for L2TP Support, on page 914
• Modifying APN Templates to Support L2TP, on page 916

Applicable Products and Relevant Sections

The LAC feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Applicable Product(s)	Refer to Sections

PDSN/FA/HA	• *Supported LAC Service Configurations for PDSN Simple IP*
	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	  • *Tunneling All Subscribers in a Specific Context Without Using RADIUS Attribu*
	• *Configuring LAC Services*
	• *Modifying PDSN Services for L2TP Support*

GGSN/SGSN/FA/P-GW	• *Supported LAC Service Configurations for the GGSN*
	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	• *Enabling Multicast Services over L2TP*
	• *Configuring LAC Services*
	• *Modifying APN Templates to Support L2TP*

ASN GW	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	  • *Tunneling All Subscribers in a Specific Context Without Using RADIUS Attribu*
	• *Configuring LAC Services*

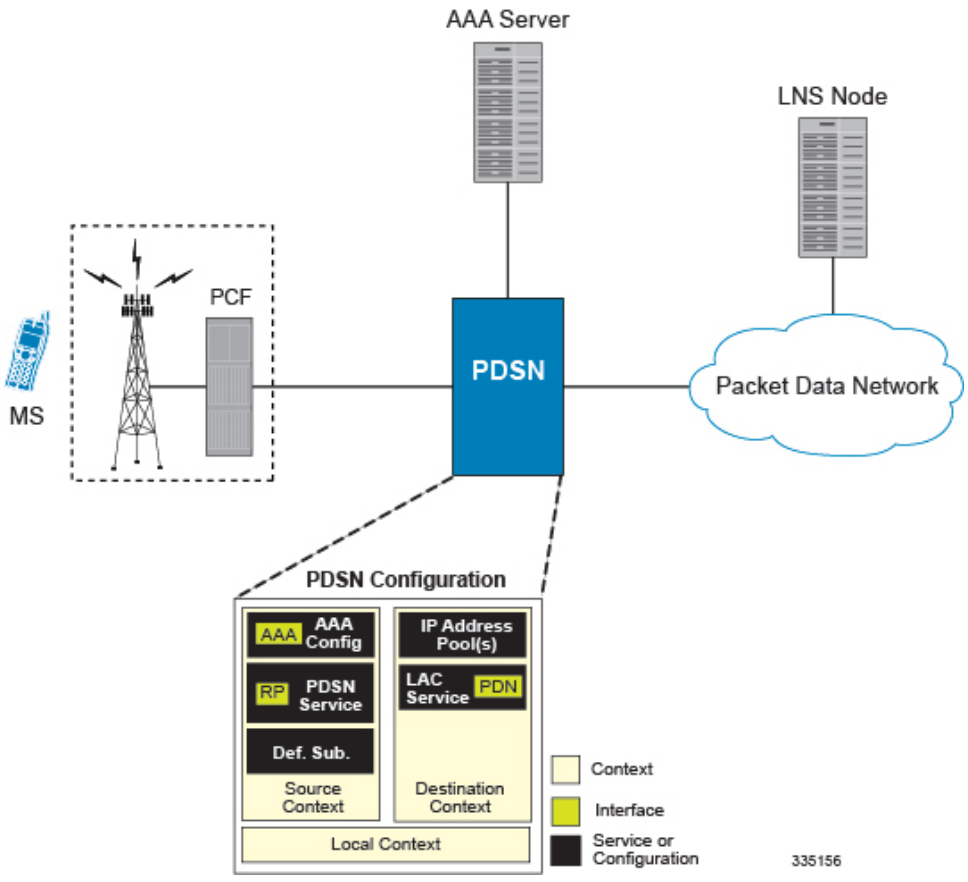
Supported LAC Service Configurations for PDSN Simple IP

LAC services can be applied to incoming PPP sessions using one of the following methods:

- **Attribute-based tunneling:** This method is used to encapsulate PPP packets for only specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.
- **PDSN Service-based compulsory tunneling:** This method of tunneling is used to encapsulate all incoming PPP traffic from the R-P interface coming into a PDSN service, and tunnel it to an LNS peer for authentication. It should be noted that this method does not consider subscriber configurations, since all authentication is performed by the peer LNS.

Each LAC service is bound to a single system interface configured within the same system context. It is recommended that this context be a destination context as displayed in the following figure.

Figure 86: LAC Service Configuration for SIP



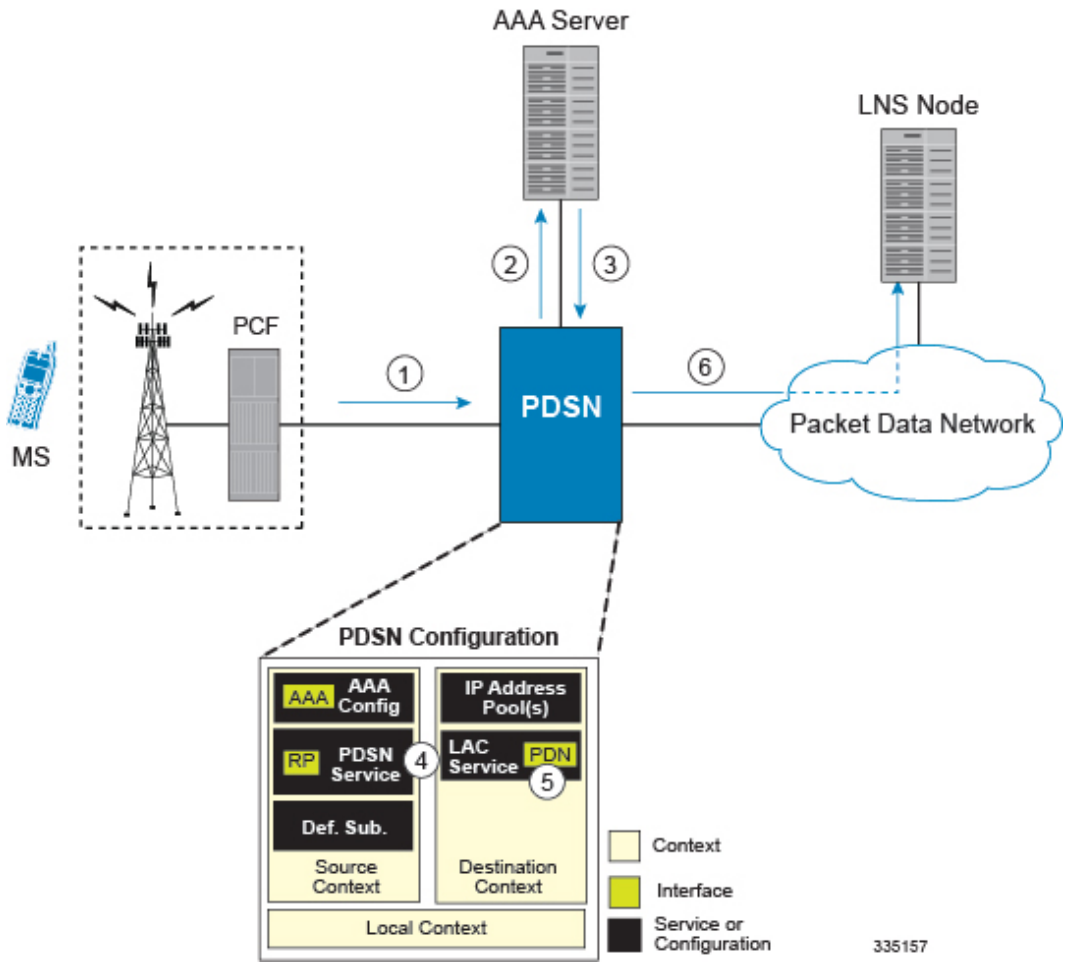
Attribute-based Tunneling

This section describes the working of attribute-based tunneling and its configuration.

How The Attribute-based L2TP Configuration Works

The following figure and the text that follows describe how Attribute-based tunneling is performed using the system.

Figure 87: Attribute-based L2TP Session Processing for SIP



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The PDSN service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for PDSN Simple IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

Procedure

Step 1 Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

Step 3 Configure the PDSN service(s) with the tunnel context location according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.

Step 4 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*.

PDSN Service-based Compulsory Tunneling

This section describes the working of service-based compulsory tunneling and its configuration.

How PDSN Service-based Compulsory Tunneling Works

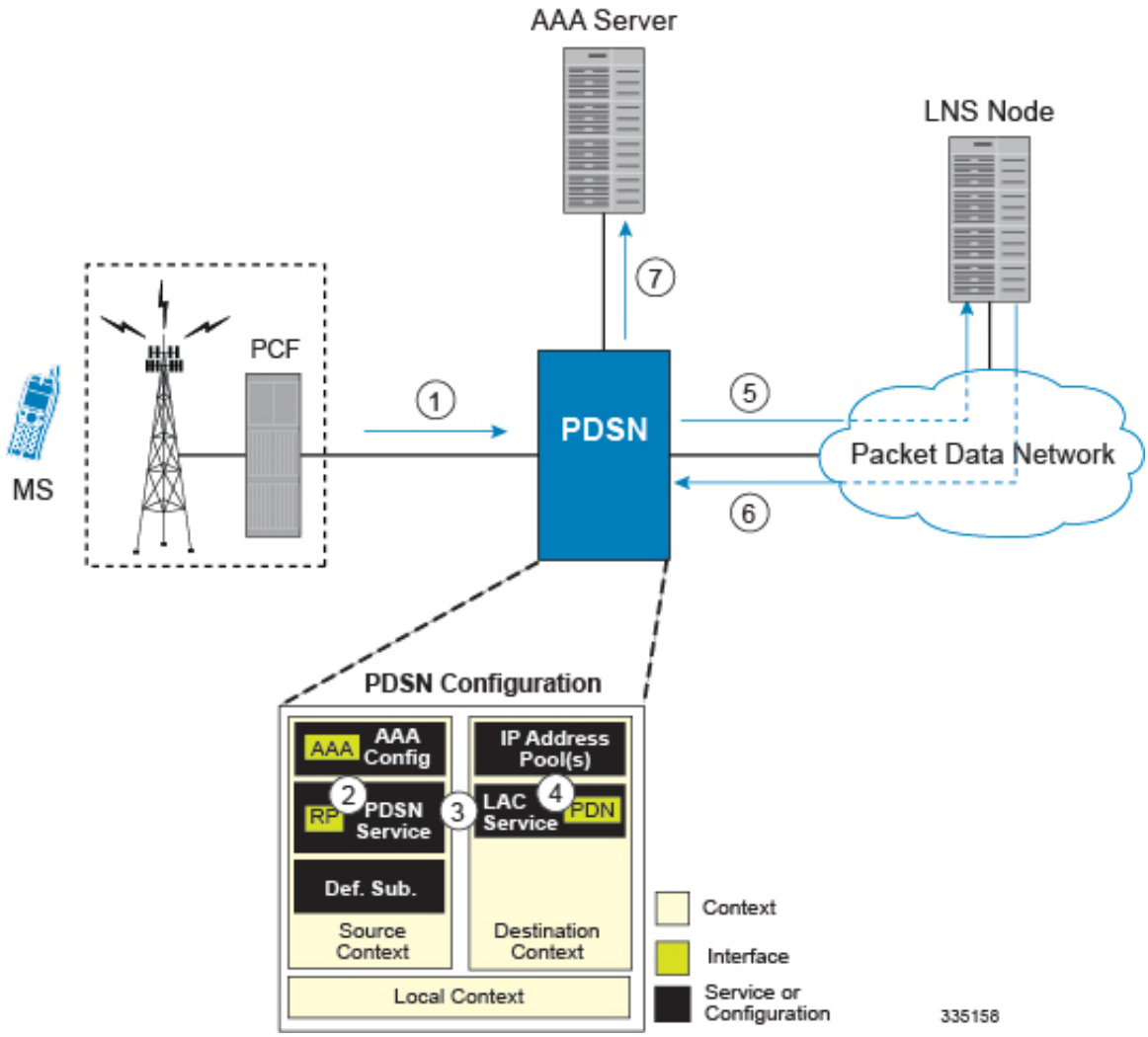
PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

Accounting start and interim accounting records are still sent to the local RADIUS server configured in the system's AAA Service configuration. When the L2TP session setup is complete, the system starts its call counters and signals the RADIUS server to begin accounting. The subscriber name for accounting records is based on the NAI-constructed name created for each session.

PDSN service-based compulsory tunneling requires the modification of one or more PDSN services and the configuration of one or more LAC services.

The following figure and the text that follows describe how PDSN service-based compulsory tunneling is performed using the system.

Figure 88: PDSN Service-based Compulsory Tunneling Session Processing



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service detects its **tunnel-type** parameter is configured to L2TP and its **tunnel-context** parameter is configured to the Destination context.
3. The PDSN forwards all packets for the session to a LAC service configured in the Destination context. If multiple LAC services are configured, session traffic will be routed to each using a round-robin algorithm.
4. The LAC service initiates an L2TP tunnel to one of the LNS peers listed as part of its configuration.
5. Session packets are passed to the LNS over a packet data network for authentication.
6. The LNS authenticates the session and returns an Access-Accept to the PDSN.
7. The PDSN service initiates accounting for the session using a constructed NAI.

   Session data traffic is passed over the L2TP tunnel established in step 4.

Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP

This section provides a list of the steps required to configure L2TP compulsory tunneling support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

Procedure

Step 1 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

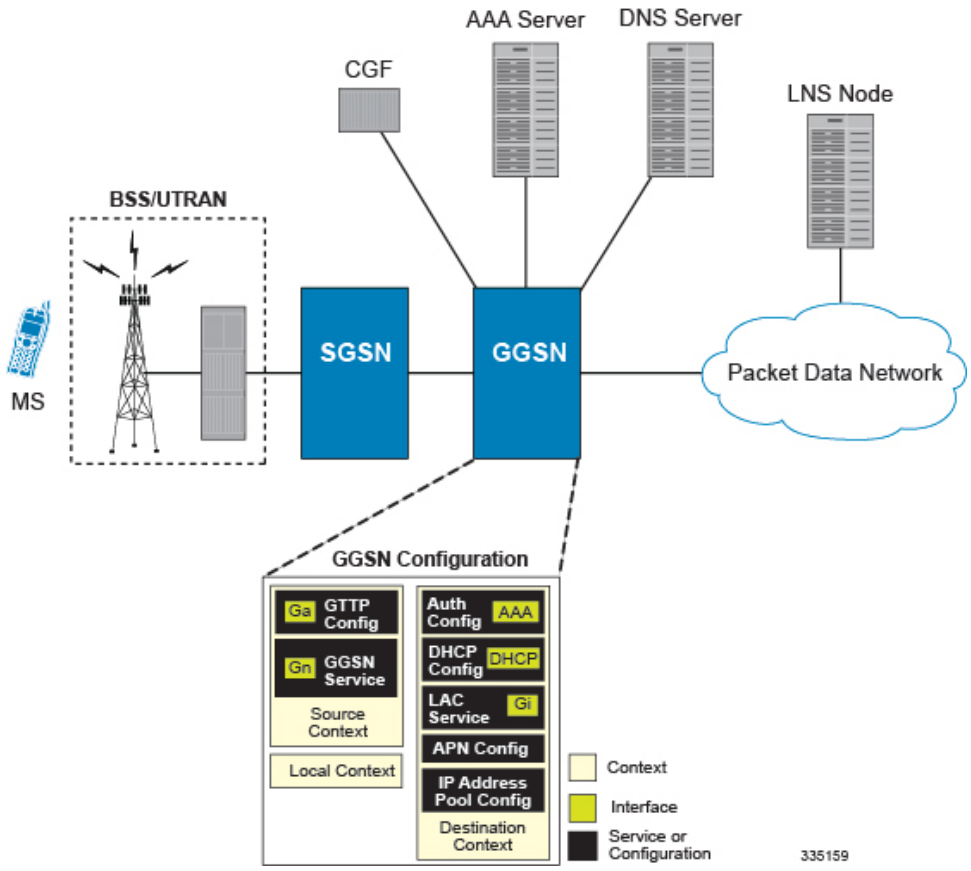
Step 2 Configure the PDSN service(s) according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.

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*.

Supported LAC Service Configurations for the GGSN and P-GW

As mentioned previously, L2TP is supported through the configuration of LAC services on the system. Each LAC service is bound to a single system interface configured within the same system destination context as displayed in following figure.

Figure 89: GGSN LAC Service Configuration



LAC services are applied to incoming subscriber PDP contexts based on the configuration of attributes either in the GGSN's Access Point Name (APN) templates or in the subscriber's profile. Subscriber profiles can be configured locally on the system or remotely on a RADIUS server.

LAC service also supports domain-based L2TP tunneling with LNS. This method is used to create multiple tunnels between LAC and LNS on the basis of values received in "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute received from AAA Server in Access-Accept as a key for tunnel selection and creation. When the LAC needs to establish a new L2TP session, it first checks if there is any existing L2TP tunnel with the peer LNS based on the value of key "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

If LAC service needs to establish a new tunnel for new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message. If all available peer-LNS are exhausted, LAC service will reject the call

L2TP tunnel parameters are configured within the APN template and are applied to all subscribers accessing the APN. However, L2TP operation will differ depending on the subscriber's PDP context type as described below:

- **Transparent IP:** The APN template's L2TP parameter settings will be applied to the session.
- **Non-transparent IP:** Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.

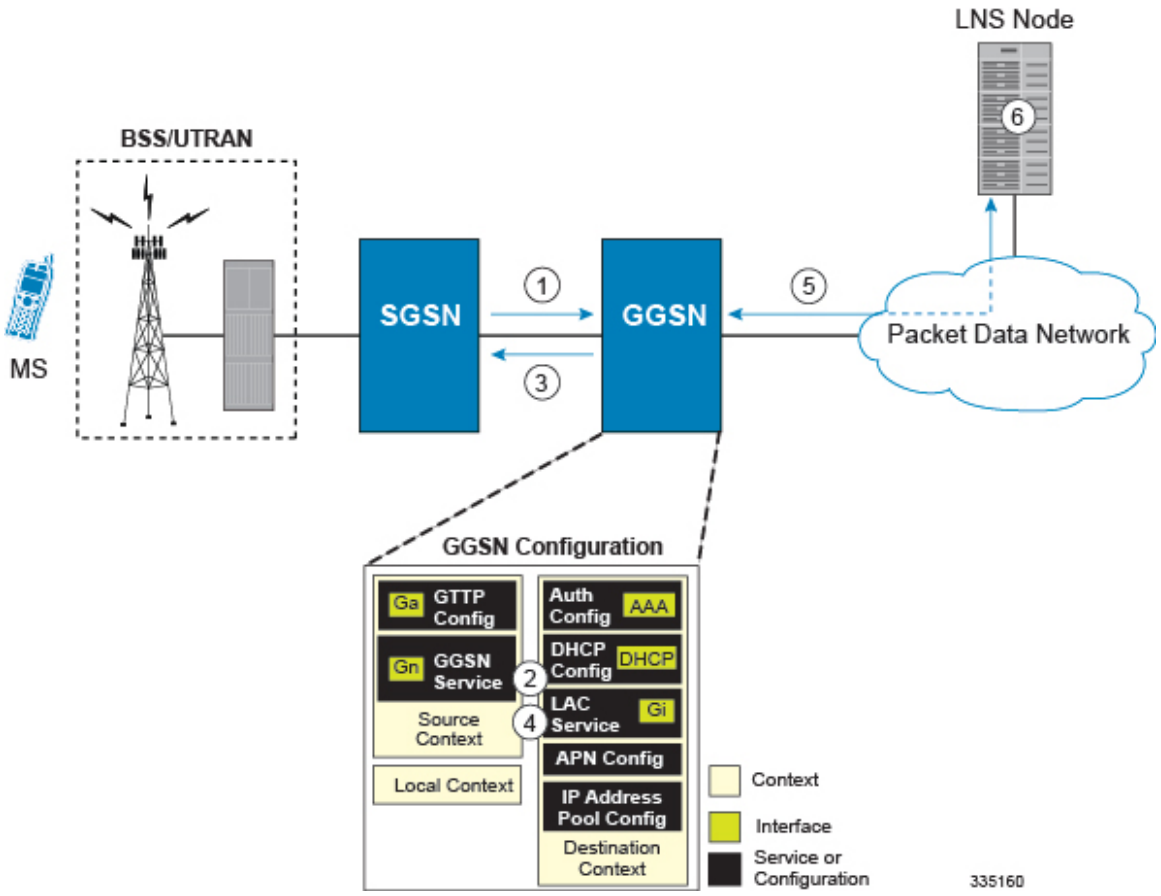
- **PPP:** The APN template's L2TP parameter settings will be applied and all of the subscriber's PPP packets will be forwarded to the specified LNS.

More detailed information is located in the sections that follow.

Transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 90: Transparent IP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

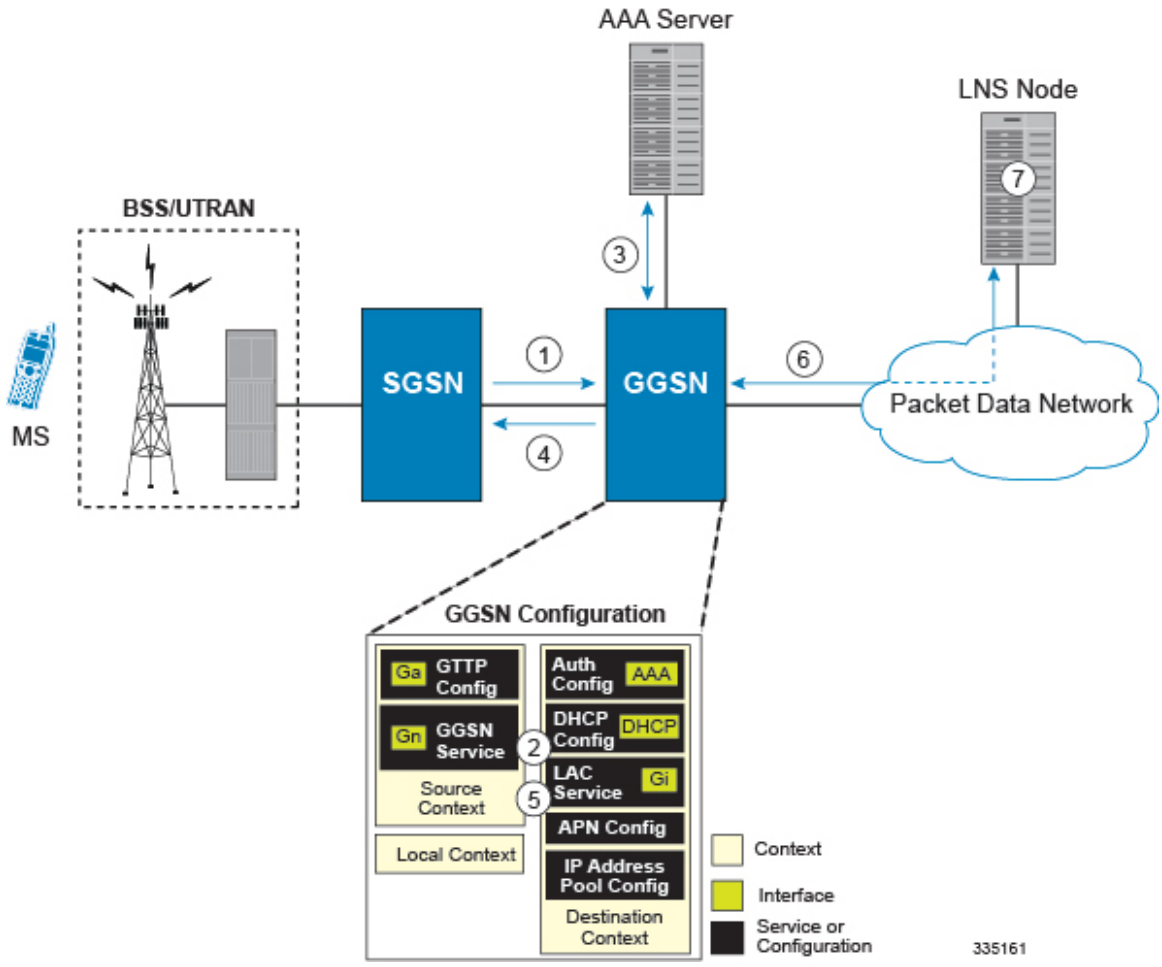
   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber's International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

1. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
2. The GGSN passes data received from the MS to a LAC service.
3. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
4. The LNS un-encapsulates the packets and processes them as needed. The processing includes IP address allocation.

Non-transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 91: Non-transparent IP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.

2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber\'s username is sent to the peer LNS.

3. The GGSN service authenticates the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.

   As part of the authentication, the RADIUS server returns an Access-Accept message.

   The message may include attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

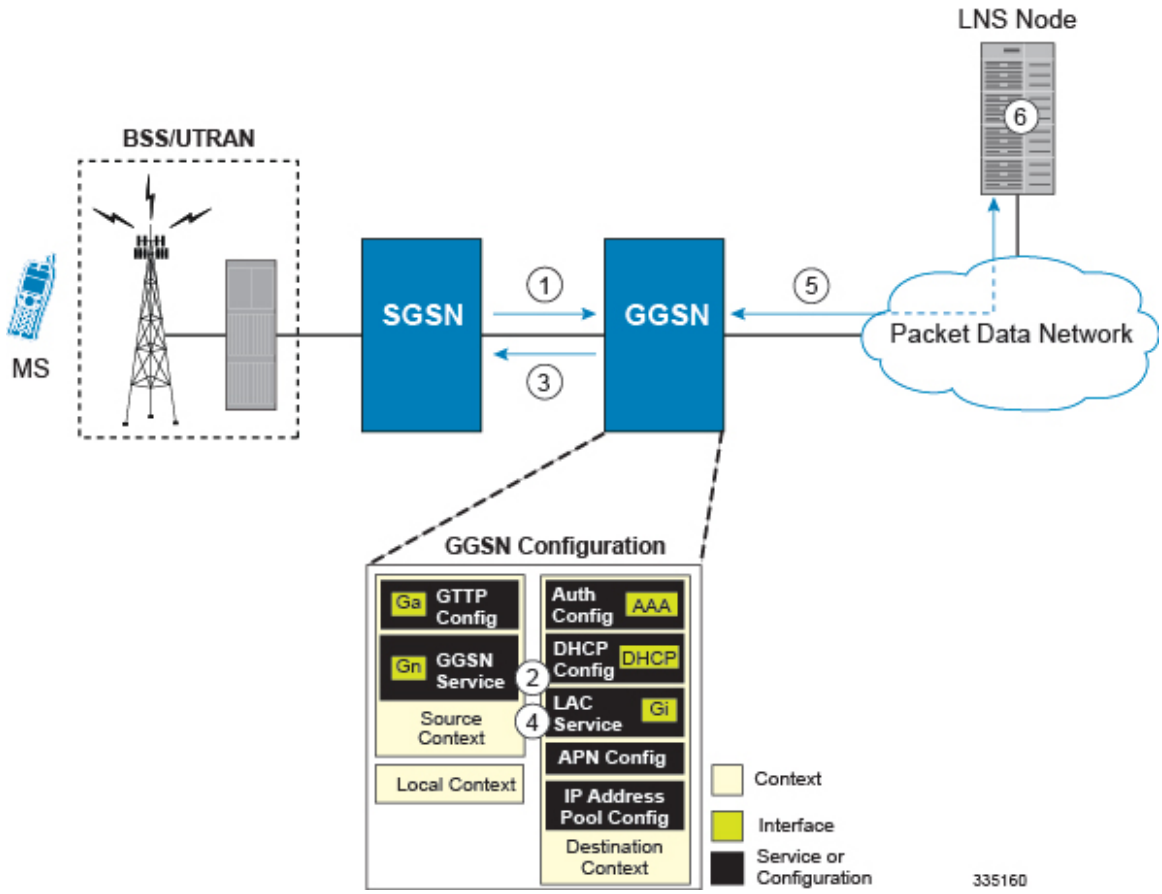
   If these attributes are supplied, they take precedence over those specified in the APN template.

4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
5. The GGSN passes data received from the MS to a LAC service.
6. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
7. The LNS un-encapsulates the packets and processes them as needed.The processing includes authentication and IP address allocation.

PPP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 92: PPP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured.

   Note that L2TP support could also be configured in the subscriber\'s profile. If the APN is not configured for L2TP tunneling, the system will attempt to authenticate the subscriber.The tunneling parameters in the subscriber\'s profile would then be used to determine the peer LNS.
3. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
4. The GGSN passes the PPP packets received from the MS to a LAC service.
5. The LAC service encapsulates the PPP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
6. The LNS un-encapsulates the packets and processes them as needed. The processing includes PPP termination, authentication (using the username/password provided by the subscriber), and IP address allocation.

Configuring the GGSN or P-GW to Support L2TP

This section provides a list of the steps required to configure the GGSN or P-GW to support L2TP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a GGSN or P-GW.

Procedure

Step 1 Configure the APN template to support L2TP tunneling according to the information and instructions located in the *Modifying APN Templates to Support L2TP* section of this chapter.

Important
L2TP tunneling can be configured within individual subscriber profiles as opposed/or in addition to configuring support with an APN template. Subscriber profile configuration is described in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

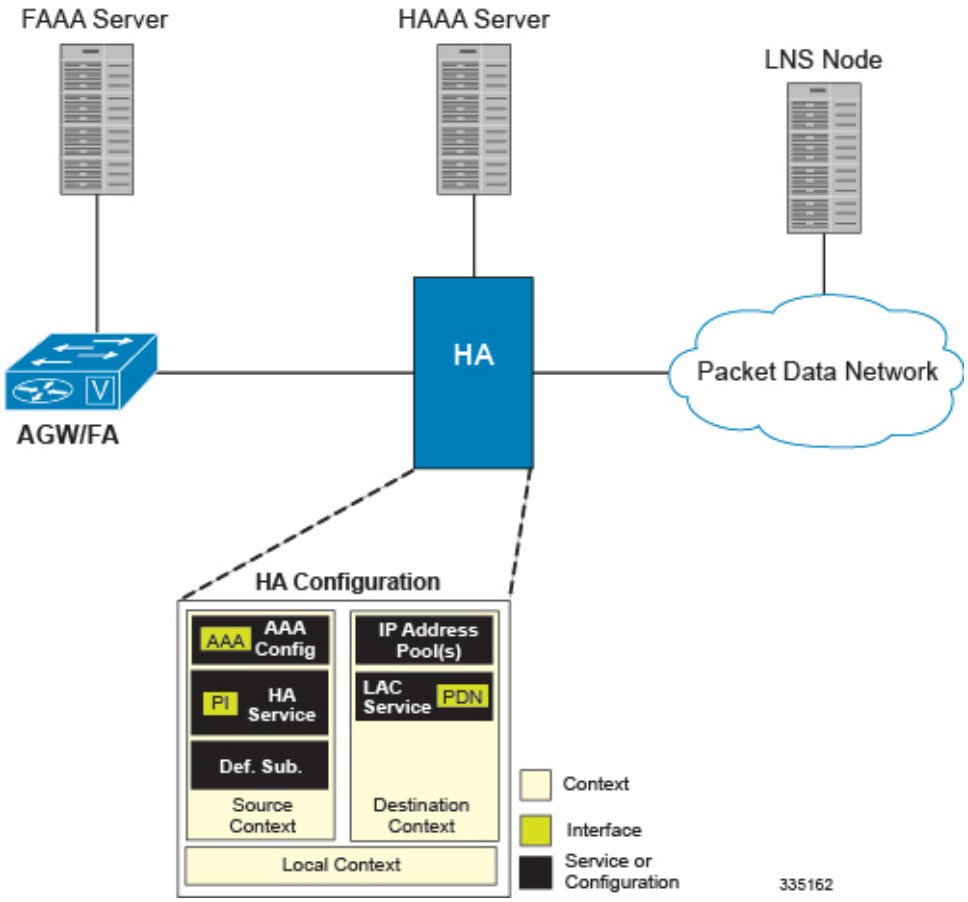
Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Supported LAC Service Configuration for Mobile IP

LAC services can be applied to incoming MIP sessions using attribute-based tunneling. Attribute-based tunneling is used to encapsulate PPP packets for specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

Each LAC service is bound to a single system interface within the same system context. It is recommended that this context be a destination context as displayed in figure below.

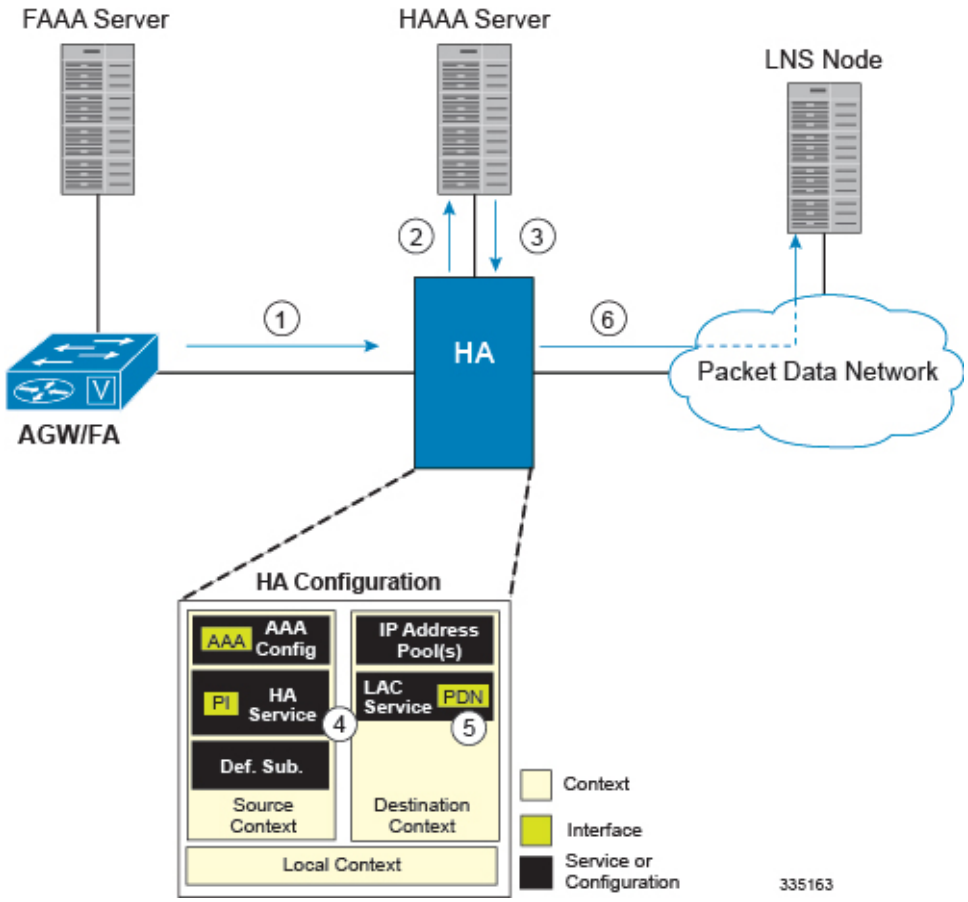
Figure 93: LAC Service Configuration for MIP



How The Attribute-based L2TP Configuration for MIP Works

The following figure and the text that follows describe how Attribute-based tunneling for MIP is performed using the system.

Figure 94: Attribute-based L2TP Session Processing for MIP



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The HA service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for HA Mobile IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with HA Mobile IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as an HA.

Procedure

Step 1 Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

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 Subscriber Profiles for L2TP Support

This section provides information and instructions on the following procedures:

- RADIUS and Subscriber Profile Attributes Used, on page 908
- Configuring Local Subscriber Profiles for L2TP Support, on page 910
- Configuring Local Subscriber, on page 911
- Verifying the L2TP Configuration, on page 911

Important Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

RADIUS and Subscriber Profile Attributes Used

Attribute-based L2TP tunneling is supported through the use of attributes configured in subscriber profiles stored either locally on the system or remotely on a RADIUS server. The following table describes the attributes used in support of LAC services. These attributes are contained in the standard and VSA dictionaries.

Table 94: Subscriber Attributes for L2TP Support

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Type	tunnel l2tp	Specifies the type of tunnel to be used for the subscriber session	L2TP

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Server-Endpoint	tunnel l2tp peer-address	Specifies the IP address of the peer LNS to connect tunnel to.	IPv4 address in dotted-decir format, enclosed in quotatio
Tunnel-Password	tunnel l2tp secret	Specifies the shared secret between the LAC and LNS.	Alpha and or numeric string to 63 characters, enclosed in quotation marks
Tunnel-Private-Group-ID	tunnel l2tp tunnel-context	Specifies the name of the destination context configured on the system in which the LAC service(s) to be used are located. **Important** If the LAC service and egress interface are configured in the same context as the core service or HA service, this attribute is not needed.	Alpha and or numeric string to 63 characters, enclosed in quotation marks
Tunnel-Preference	tunnel l2tp preference	Configures the priority of each peer LNS when multiple LNS nodes are configured. **Important** This attribute is only used when the **loadbalance-tunnel-peers** parameter or **SN-Tunnel-Load-Balancing** attribute configured to prioritized.	Integer from 1 to 65535
SN-Tunnel-Load-Balancing	loadbalance-tunnel-peer	A vendor-specific attribute (VSA) used to provides a selection algorithm defining how an LNS node is selected by the RADIUS server when multiple LNS peers are configured within the subscriber profile.	• **Random** - Random LN selection order, the **Tunnel-Preference** att not used in determining LNS to select. • **Balanced** - LNS select sequential balancing th across all configured L nodes, the **Tunnel-Pref** attribute is not used in determining which LN select. • **Prioritized** - LNS sele made based on the prio assigned in the **Tunnel-Preference** att

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Client-Endpoint	local-address	Specifies the IP address of a specific LAC service configured on the system that to use to facilitate the subscriber\'s L2TP session. This attribute is used when multiple LAC services are configured.	IPv4 address in dotted decimal notation. (xxx.xxx.xxx.xxx)

RADIUS Tagging Support

The system supports RADIUS attribute tagging for tunnel attributes. These "tags" organize together multiple attributes into different groups when multiple LNS nodes are defined in the user profile. Tagging is useful to ensure that the system groups all the attributes used for a specific server. If attribute tagging is not supported by your specific RADIUS server, the system implicitly organizes the attributes in the order that they are listed in the access accept packet.

Configuring Local Subscriber Profiles for L2TP Support

This section provides information and instructions for configuring local subscriber profiles on the system to support L2TP.

Important The configuration of RADIUS-based subscriber profiles is not discussed in this document. Please refer to the documentation supplied with your RADIUS server for further information.

Important This section provides the minimum instruction set for configuring local subscriber profile for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to provide L2TP support to subscribers:

Procedure

Step 1 Configure the "Local" subscriber with L2TP tunnel parameters and the load balancing parameters with action by applying the example configuration in the *Configuring Local Subscriber* section.

Step 2 Verify your L2TP configuration by following the steps in the *Verifying the L2TP Configuration* 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*.

Configuring Local Subscriber

Use the following example to configure the Local subscriber with L2TP tunnel parameters. Optionally you can configure load balancing between multiple LNS servers:

```
configure
   context <ctxt_name> [-noconfirm]
      subscriber name <subs_name>
         tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [
encrypted ] secret <secret_string> | tunnel-context <context_name> | local-address
 <local_ip_address> }
         load-balancing { random | balanced | prioritized }
         end
```

Notes:

- <*ctxt_name*> is the system context in which you wish to configure the subscriber profile.
- <*lns_ip_address*> is the IP address of LNS server node and <*local_ip_address*> is the IP address of system which is bound to LAC service.

Verifying the L2TP Configuration

These instructions are used to verify the L2TP configuration.

Procedure

Verify that your L2TP configurations were configured properly by entering the following command in Exec Mode in specific context:

show subscriber configuration username *user_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes

As with other services supported by the system, values for subscriber profile attributes not returned as part of a RADIUS Access-Accept message can be obtained using the locally configured profile for the subscriber named default. The subscriber profile for default must be configured in the AAA context (i.e. the context in which AAA functionality is configured).

As a time saving feature, L2TP support can be configured for the subscriber named default with no additional configuration for RADIUS-based subscribers. This is especially useful when you have separate source/AAA contexts for specific subscribers.

To configure the profile for the subscriber named default, follow the instructions above for configuring a local subscriber and enter the name default.

Feature Description

When a multicast service is set up for the mobile Customer Premises Equipment (CPE), the APN is configured with L2TP tunnel and P-GW works as L2TP Access Concentrator (LAC). To set up the multicast session, the video client/mobile CPE need to send or receive the PIM (Protocol Independent Multicast) message (with TTL=1) to or from Video headend server over SGi L2TP tunnel.

The P-GW follows the default L2TP LAC to inspect and process the encapsulated IP traffic inside the L2TP tunnel. This process prevents certain applications between CPE and LNS that sends TTL=1 traffic to function. Prior to 21.21.1 release, when an IP packet is sent, the Time to Live (TTL) value (for example, 255) was decremented by 1 at each hop. The P-GW dropped the packet with TTL value 0 or 1, decremented (when TTL > 1) the TTL value and the new checksum for the data packet was calculated. In this release, by enabling multicast session over L2TP feature through CLI:

- P-GW ignores the TTL value and forwards the packet.
- The L2TP and regular packets gets differentiated by L2TP tunnel type at sessmgr_ipv4.c and it verifies the CLI configuration mode enabled.

Configuring LAC Services

Important Not all commands, keywords and functions may be available. Functionality is dependent on platform and license(s).

This section provides information and instructions for configuring LAC services on the system allowing it to communicate with peer LNS nodes.

Important This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Procedure

Step 1 Configure the LAC service on system and bind it to an IP address by applying the example configuration in the *Configuring LAC Service* section.

Step 2 *Optional*. Configure LNS peer information if the Tunnel-Service-Endpoint attribute is not configured in the subscriber profile or PDSN compulsory tunneling is supported by applying the example configuration in the *Configuring LNS Peer* section.

Step 3 Verify your LAC configuration by following the steps in the Verifying the LAC Service Configuration section.

Step 4 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 LAC Service

Use the following example to create the LAC service and bind the service to an IP address:

```
configure
   context <dst_ctxt_name> [-noconfirm]
      lac-service <service_name>
         bind address <ip_address>
         end
```

Notes:

- <*dst_ctxt_name*> is the destination context where you want to configure the LAC service.

Configuring Multicast Services over L2TP

Use the following CLI commands to enable or disable the multicast session over L2TP feature. By default, this feature is disabled.

```
configure
   context context_name
      lac-service service_name
         ttl-ignore
         end
```

Notes:

- **ttl-ignore**: Ignores the TTL value and forwards the packets.

Configuring LNS Peer

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      lac-service <service_name>
         tunnel selection-key tunnel-server-auth-id
         peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
{[encrypted] isakmp-secret <secret> }] [description <text>] [ preference <integer>]

         load-balancing { random | balanced | prioritized }
         end
```

Notes:

- <*dst_ctxt_name*> is the destination context where the LAC service is configured.

Verifying the LAC Service Configuration

These instructions are used to verify the LAC service configuration.

Procedure

Verify that your LAC service configurations were configured properly by entering the following command in Exec Mode in specific context:

show lac-service name *service_name*

The output given below is a concise listing of LAC service parameter settings as configured.

```
Service name: vpn1
Context:                          isp1
Bind:                             Done
Local IP Address:                 192.168.2.1
First Retransmission Timeout:     1 (secs)
Max Retransmission Timeout:       8 (secs)
Max Retransmissions:              5
Max Sessions:                     500000      Max Tunnels: 32000
Max Sessions Per Tunnel:          512
Data Sequence Numbers:            Enabled     Tunnel Authentication:  Enabled
Keep-alive interval:              60          Control receive window: 16
Max Tunnel Challenge Length:      16
Proxy LCP Authentication:         Enabled
Load Balancing:                   Random
Service Status:                   Started
Newcall Policy:                   None
```

Modifying PDSN Services for L2TP Support

PDSN service modification is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but cannot determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.



Important This section provides the minimum instruction set for modifying PDSN service for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Procedure

Step 1 Modify the PDSN service to support L2TP by associating LAC context and defining tunnel type by applying the example configuration in the *Modifying PDSN Service* section.

Step 2 Verify your configuration to modify PDSN service by following the steps in the *Verifying the PDSN Service for L2TP Support* 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*.

Modifying PDSN Service

Use the following example to modify the PDSN service to support L2TP by associating LAC context and defining tunnel type:

```
configure
   context <source_ctxt_name> [ -noconfirm ]
      pdsn-service <pdsn_service_name>
         ppp tunnel-context <lac_context_name>
         ppp tunnel-type { l2tp | none }
         end
```

Notes:

- <*source_ctxt_name*> is the name of the source context containing the PDSN service, which you want to modify for L2TP support.
- <*pdsn_service_name*> is the name of the pre-configured PDSN service, which you want to modify for L2TP support.
- <*lac_context_name*> is typically the destination context where the LAC service is configured.

Verifying the PDSN Service for L2TP Support

These instructions are used to verify the PDSN service configuration.

Procedure

Verify that your PDSN is configured properly by entering the following command in Exec Mode in specific context:

```
show pdsn-service name pdsn_service_name
```

The output of this command is a concise listing of PDSN service parameter settings as configured.

Modifying APN Templates to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.



Important This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Procedure

Step 1 Modify the APN template to support L2TP with LNS server address and other parameters by applying the example configuration in the *Assigning LNS Peer Address in APN Template* section.

Step 2 Optional. If L2TP will be used to tunnel transparent IP PDP contexts, configure the APN\'s outbound username and password by applying the example configuration in the *Configuring Outbound Authentication* section.

Step 3 Verify your APN configuration by following the steps in the *Verifying the APN Configuration* section.

Step 4 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*.

Assigning LNS Peer Address in APN Template

Use following example to assign LNS server address with APN template:

```
configure
   context <dst_ctxt_name> [-noconfirm]
      apn <apn_name>
         tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret
<l2tp_secret> ] [ preference <integer> ] [ tunnel-context <l2tp_context_name> ] [
local-address <local_ip_address> ] [ crypto-map <map_name> { [ encrypted ]
isakmp-secret <crypto_secret> } ]
         end
```

Notes:

- <*dst_ctxt_name*> is the name of system destination context in which the APN is configured.
- <*apn_name*> is the name of the pre-configured APN template which you want to modify for the L2TP support.
- <*lns_address*> is the IP address of LNS server node and <*local_ip_address*> is the IP address of system which is bound to LAC service.

Configuring Outbound Authentication

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      apn <apn_name>
         outbound { [ encrypted ] password <pwd> | username <name> }
         end
```

Notes:

- <*dst_ctxt_name*> is the destination context where APN template is is configured.
- <*apn_name*> is the name of the pre-configured APN template which you want to modify for the L2TP support.

Verifying the APN Configuration

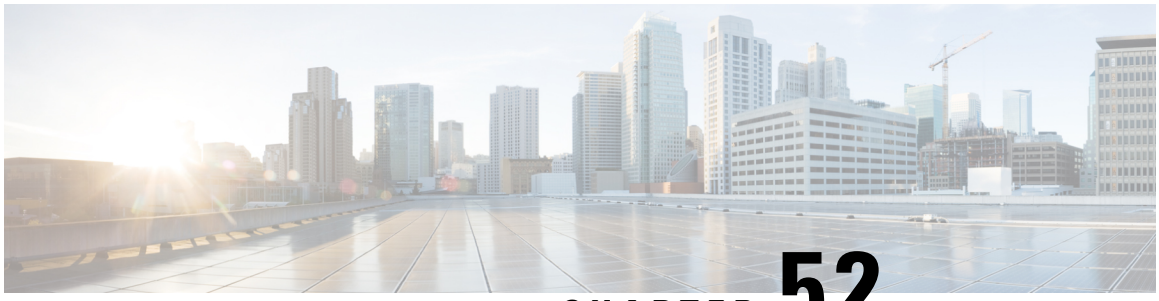
These instructions are used to verify the APN configuration.

Procedure

Verify that your APN configurations were configured properly by entering the following command in Exec Mode in specific context:

show apn name *apn_name*

The output is a concise listing of APN parameter settings as configured.



CHAPTER 52

LBO Restriction on Downlink and Uplink Data Volume Transfer

This chapter describes the following topics:

- Feature Summary and Revision History, on page 919
- Feature Description, on page 920
- How It Works, on page 920
- Configuring the LBO Restriction on Downlink and Uplink Data Volume Transfer, on page 920
- Monitoring and Troubleshooting the LBO Restriction on Downlink and Uplink Data Volume Transfer, on page 921

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.5

Feature Description

After the subscriber quota is exhausted, all the ongoing download of files must be terminated and the UE must be allowed access to only user-defined servers (Self-Care Portal).

This feature achieves the functionality of Local Break Out (LBO) restriction on Downlink and Uplink data volume transfer by CLI-controlled mechanism.

How It Works

Following is a brief overview of how the feature works:

1. User is redirected to the portal and enters an OTP. The subscriber session continues after authentication.
2. Internet rule and Default rules are installed by PCRF and quota is granted by the OCS.
3. After the subscriber quota is exhausted, the PCRF installs a Self-Care Readdress rule and removes the previously installed Internet rule.
4. After the Readdress rule is applied:
   - For UDP: The ongoing Downlink packets are discarded while all the new uplink packets are readdressed to Self-Care Portal.
   - For TCP: All the existing flows matching the Internet rule are terminated by sending FIN to UE and RST to the server.

Limitation

Post installation of readdress rule, first packet is charged but not sent to the UE. Subsequent packets are not charged or sent to the UE.

Configuring the LBO Restriction on Downlink and Uplink Data Volume Transfer

This section provides information about the CLI commands available in support of the feature.

Enabling the LBO Restriction on Downlink and Uplink Data Volume Transfer

Use the following configuration in ACS Rulebase Configuration Mode to enable the feature.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      ip readdress failure-action terminate
      { default | no } ip readdress failure-action
      end
```

NOTES:

- **ip readdress**: Configures the IP Readdress options.
- **failure-action**: Configures the failure action for IP Readdress.
- **terminate**: Terminates the flow
- If previously configured, use the **{ default | no } ip readdress failure-action** CLI command to disable the feature.

Monitoring and Troubleshooting the LBO Restriction on Downlink and Uplink Data Volume Transfer

This section describes the CLI commands available to monitor and/or troubleshoot the feature.

Show Commands and/or Outputs

show active-charging rulebase statistics

The output of this CLI command has been enhanced in support of the feature. The following existing counters will be updated when Readdressing fails for UDP:

- Total Readdressing Failures
- Dropped Pkts

show active-charging sessions full all

The output of this CLI command has been enhanced in support of the feature. The following existing counter will be updated when Readdressing fails for TCP flow:

- Flow action Terminated Flows

show active-charging charging-action statistics name *<charging_action_name>*

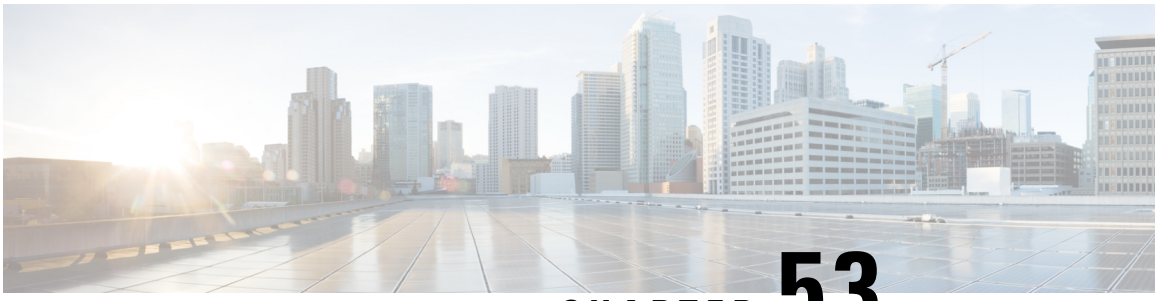
The output of this CLI command has been enhanced in support of the feature. The following existing counter will be updated when Readdressing fails for TCP flow:

- Terminate Flow

show active-charging service statistics

The output of this CLI command has been enhanced in support of the feature. The following existing counter will be updated when Readdressing fails for UDP:

- Dropped Pkts



CHAPTER 53

LTE to Wi-Fi (S2bGTP) Seamless Handover

This chapter describes the following topics:

- Feature Summary and Revision History, on page 923
- Feature Description, on page 924
- How It Works, on page 924
- Configuring LTE to Wi-Fi Seamless Handover, on page 926
- Monitoring and Troubleshooting, on page 926

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History



Important Revision history details are not provided for features introduced before release 21.2 and N5.1.

Revision Details	Release
With this release, support has been added for seamless handover of subscribers from LTE to Wi-Fi (S2bGTP).	21.8
First introduced.	Pre 21.2

Feature Description

When handover is initiated from LTE to Wi-Fi, the Delete Bearer Request (DBR) is sent over the LTE tunnel immediately when the Create Session Response (CSR) is sent on the Wi-Fi tunnel. This causes some packet loss because of the IPSec tunnel establishment delay at the ePDG. To address the issue of packet loss, an enhancement is introduced, in Release 21.8, that holds both the tunnels (LTE and Wi-Fi) and sends the Delete Bearer Request on LTE tunnel only when uplink data is seen on the Wi-Fi tunnel or on expiry of the configured handover timer (when there is no uplink data), whichever is earlier. As long as the LTE tunnel is active, uplink and downlink data is exchanged on the LTE tunnel. When handover is complete, uplink and downlink data is exchanged on the Wi-Fi tunnel. This prevents packet loss.

With this enhancement, the following benefits can be seen:

- Minimum packet loss during LTE to Wi-Fi (S2bGTP) handover and making the handover seamless (that is, MAKE before BREAK).
- LTE procedures are handled gracefully over the LTE tunnel when both tunnels are established with the P-GW.
- Wi-Fi procedures are handled gracefully over the Wi-Fi tunnel when both tunnels are established with the P-GW.
- When there are two tunnels (LTE and Wi-Fi) established for the same subscriber, GTP-U error indication and GTP-U path failure on the LTE or Wi-Fi tunnel (default or dedicated bearer) are handled properly during the transition period.

How It Works

The LTE to Wi-Fi (S2bGTP) Seamless Handover works as explained in the following sections.

LTE to Wi-Fi Handoff

The LTE to Wi-Fi handoff occurs as follows:

1. The P-GW delays sending the DBR to the S-GW until:

- CSR expiry is sent to the ePDG (default behavior).
- Uplink data is sent on the Wi-Fi tunnel.
- Handover timer has expired. If timer expires, the ePDG does not send the Modify Bearer Request (MBR) to notify handoff completion.

2. After CSR for LTE to Wi-Fi handoff is received, Control Plane GTPv2 (GTP-C) messages from LTE access are not handled at the P-GW. These messages are blocked at the EGTPC.
3. LTE tunnel carries GTP-U traffic during the transition period. Transition period is defined as time between CSR (for LTE to Wi-Fi handoff is received) and handover completion. MBR for handoff completion is not expected in this scenario.
4. In case of multiple outstanding CCR-Us being supported, all requests before the handoff request are dropped. This is done at IMSA.
5. During the transition period:
   - If Modify Bearer Command (MBC) is received in Wi-Fi, it is rejected with Service-Denied message.
   - If Delete Bearer Command for dedicated bearer is received in LTE, it is discarded.
   - If PCRF sends RAR for policy change, it is processed after handover is complete.
   - New tunnel (that is, Wi-Fi) does not carry any GTP-U traffic. Any GTP-U traffic that is received on the Wi-Fi during the transition period is dropped or ignored. Similarly, any downlink traffic that is received on the Wi-Fi is sent on an older tunnel (that is, LTE tunnel) until DBR is sent on the Wi-Fi tunnel. This is true even when CSR is sent on the Wi-Fi tunnel. Any uplink traffic that is received on the Wi-Fi tunnel before timer expiry triggers the handover completion, and from then on all traffic is forwarded only through the Wi-Fi tunnel.
   - Any pending transactions on LTE access are discarded. For example, if CBR or UBR is sent for LTE access and handoff is initiated before completion of CBR or UBR transaction, then CBR or UBR is ignored at the P-GW. PCRF is not notified about failure.
   - If ASR is received, then call drop occurs and both tunnels go down.
   - If session-release occurs from PCRF, then call is dropped and CSR is sent with cause as “no-resources”.
   - GTP-U or GTP-C path failure over LTE leads to call drop for LTE access while the Wi-Fi call continues.
   - GTP-U or GTP-C path failure over Wi-Fi leads to call drop. Both tunnels are cleared.
   - If the user moves back to LTE (that is, back to back handoff from LTE to Wi-Fi to LTE) with HO-Ind set to 1 (after guard timer), then the HO is processed successfully and user session is moved to LTE again.
   - If the user moves back to LTE (that is, back to back handoff from LTE to Wi-Fi to LTE) with HO-Ind set to 0, then it leads to context replacement. Old call is cleared on Wi-Fi access with reason as context replacement and call is processed like a new call over LTE.

Session Recovery and ICSR

During the transition period, old access is considered as stable state and Full Checkpoint is triggered once handover is complete from LTE to Wi-Fi (S2bGTP). This is done for both Session Recovery and ICSR.

Configuring LTE to Wi-Fi Seamless Handover

The following section provides information about the CLI commands available to enable or disable the feature.

Configuring LTE to Wi-Fi Handover Timer

Use the following CLI commands to configure LTE to Wi-Fi handover timer.

```
configure
  context context_name
    apn apn_name
      lte-s2bgtp-first-uplink timeout
      { default | no } lte-s2bgtp-first-uplink
      end
```

NOTES:

- **default**: Enables the LTE to Wi-Fi handover completion to occur when the Create Session Response is sent on the Wi-Fi tunnel.
- **no**: Disables the feature and handover completion occurs on Create Session Response.
- **lte-s2bgtp-first-uplink** *timeout*: Configures LTE to S2bGTP handover completion timeout in multiples of 100 milliseconds. The valid range is from 100 to 3000. The recommended configuration is 1000 milliseconds.
- By default, the LTE to Wi-Fi handover completion happens when Create Session Response is sent on the Wi-Fi tunnel. However, after handover timeout is configured, the handover is delayed until timeout or on receipt of uplink data on the Wi-Fi tunnel.

Monitoring and Troubleshooting

This section provides information regarding CLI commands available in support of monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

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

show apn statistics name <name>

The output of this CLI command has been enhanced to display the following new fields for the APN:

- LTE-to-S2bGTP handover Succeeded on First Uplink Data on S2b tunnel – Specifies the number of handovers due to uplink packets.

- LTE-to-S2bGTP handover Succeeded on Timer Expiry – Specifies the number of handovers due to timer expiry.

NOTES:

The new fields, introduced as part of this feature, are also displayed for the following CLI commands:

- **show pgw-service statistics name** *service_name* **verbose**
- **show pgw-service statistics all verbose**
- **show saegw-service statistics all function pgw verbose**

Bulk Statistics

The following statistics are included in support of this feature.

APN Schema

The following bulk statistics are added for APN in the APN schema in support of the LTE to Wi-Fi Seamless Handover feature.

Bulk Statistics	Description
apn-handoverstat-ltetos2bgtpsucc-timerexpiry	Number of LTE to S2bGTP handover succeeded on Timer Expiry.
apn-handoverstat-ltetos2bgtpsucc-uplnkdata	Number of LTE to S2bGTP handover succeeded on Uplink Data on the S2b tunnel.

P-GW Schema

The following bulk statistics are added for P-GW in the P-GW schema in support of the LTE to Wi-Fi Seamless Handover feature.

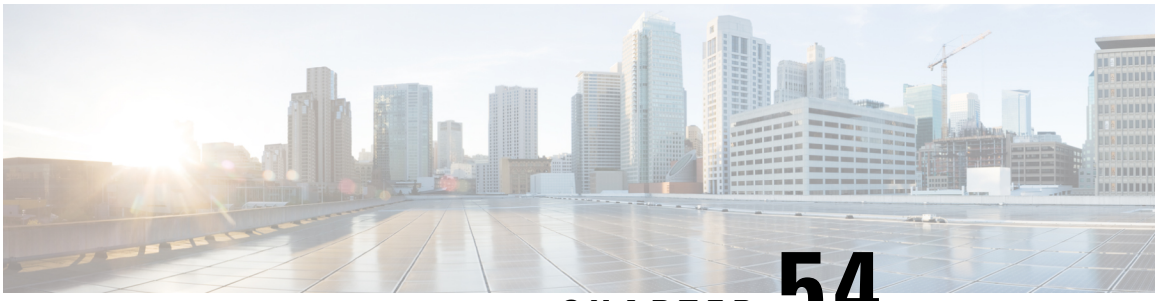
Bulk Statistics	Description
handoverstat-ltetos2bgtpsucc-timerexpiry	Handover Statistics - Number of LTE to GTP S2b successful handovers on Timer Expiry.
handoverstat-ltetos2bgtpsucc-uplnkdata	Handover Statistics - Number of LTE to GTP S2b successful handovers on Uplink Data on S2b tunnel.

SAEGW Schema

The following bulk statistics are added for SAEGW in the SAEGW schema in support of the LTE to Wi-Fi Seamless Handover feature.

Bulk Statistics	Description
pgw-handoverstat-ltetos2bgtpsucc-timerexpiry	P-GW Handover Statistics - Number of LTE to GTP S2b successful handover on Timer Expiry.

Bulk Statistics	Description
pgw-handoverstat-ltetos2bgtpsucc-uplnkdata	P-GW Handover Statistics - Number of LTE to GTP S2b successful handover on Uplink Data on S2b tunnel.



CHAPTER 54

LTE-M RAT Type Support on SAEGW, P-GW, and S-GW Services

- Feature Summary and Revision History, on page 929
- Feature Description, on page 930
- How it Works, on page 931
- Configuring Virtual-APN, on page 933
- Configuring qci-qos-mapping, on page 933
- Monitoring and Troubleshooting, on page 934

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled-Always-On
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administartion Guide*

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

LTE-M (LTE-MTC low-power-wide area (LPWA)) is a new cellular radio access technology specified by 3GPP that addresses low power-wide area connectivity solutions. It specifically refers to a specific category of LTE UEs that are suitable for IoT LTE-M, which supports IoT through lower device complexity and provides extended coverage, while allowing the reuse of the LTE installed base.

The RAT type IE is present in various call flows across many interfaces. When a Create Session Request is received with an unknown RAT Type, as the RAT Type is a Mandatory IE in this message, S-GW or P-GW may reject a create session request.

In this StarOS 21.24 release, LTE-M RAT (Radio Access Technology) type for S-GW, P-GW, and SAEGW products are supported.

The RAT type is present either as an IE (for example, in GTPv2-C, GTPP), AVP (on Diameter-based interfaces) or as an attribute (for example in EDRs) across many interfaces.

The LTE-M solution for S-GW, P-GW, and SAEGW supports the following new LTE-M RAT type attribute value in the following Interfaces protocols and dictionaries:

- GX-interface: Diameter Protocol
- GY-interface: Diameter Protocol
- GZ/RF- interface: GTPP/Diameter/Radius
- S6B- Interface: Diameter Protocol
- S11/ S5/S8-Interface: GTPv2-C
- Dictionaries Radius AVPs, and dictionaries.
- Rf interface for CDR generation
- Attributes in EDRs

Enhancements to the Existing Features

The following existing features are enhanced to support the new RAT-TYPE LTE-M.

- **Virtual APN Selection Based on RAT Type**: Virtual APNs allow differentiated services within a single APN. The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters. APN configuration dictates all aspects of a session at the P-GW, where different policies imply different APNs.

  You can select the virtual APN by configuring directly under the base APN. This APN selection is done based on RAT Types. In this release, support is added through CLI to select the virtual APN for the LTE-M RAT type.

- **Qci and Qos Mapping**: P-GW supports QCI and QoS mapping association with APN based on RAT type LTE-M. This QCI and QoS mapping allow you to perform quick actions on the QoS Class Index (QCI) to QoS Mapping Configuration Mode, which is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur in Serving Gateway (S-GW), and/or the PDN Gateway (P-GW) in an LTE network.
- **PCRF-based Handling**: P-GW informs the RAT type changes to PCRF through Credit Control Request -Initial and Updated messages, and PCRF provides a new PCC rule. Allows you to create a Bearer by enforcing a new Policy and Charging Control (PCC) rule from Policy and Charging Rules Function (PCRF).

How it Works

Architecture

The following table specifies the field and its value for various interfaces with support of LTE-M RAT type. Only Standard dictionaries and customized dictionaries are modified.

Table 95:

		P-GW Product		
x	RAT-Type (1032) Diameter	M -)	E T 7 0 0 1 (	• Credit Control Request-Initial • Credit Control Request - Updated
y	3GPP-RAT-Type (21) Diameter	M -)	E T 9 (	• Credit Control Request-Initial • Credit Control Request - Updated
SU3	3GPP-RAT-Type (21)	M -)	E T 9 (	• Accounting Request -Start • Accounting Request- Stop • Account request -Interim
f	3GPP-RAT-Type (21) Diameter	M -)	E T 9 (	• Accounting Request -Start • Accounting Request- Stop • Account request -Interim
b	3GPP-RAT-Type (1032) Diameter	M -)	E T 9 (	• Authentication • Authorisation • Request

Field	Type	Message	Value
RAT-Type	M	E T L	9 (
RAT-Type (30) GTPP	M	E T L	9 (• Gtpp Data Record • Transfer Request
S-GW Product			
RAT-Type (30)	M	E T L	9 (• Gtpp Data Record • Transfer Request

Limitations

Following are the known limitations for new LTE-M RAT type feature:

- Rule matching at ECS
- Ruledef matching at Local-Policy

Supported Standards

Cisco's implementation of the LTE RAT type complies with the following standards:

- 3GPP 23.401 – eGPTC Interface
- 3GPP 29.274 Release 15.4.0 – 3GPP GTPv2 Protocol Specification Reference table for LTE-M Rat type support; RAT Type IE details are given in the following table for egtpc IEs encoding and decoding :
  - Table 7.2.1-1: Information Elements in a Create Session Request
  - Table 7.2.7-1: Information Elements in a Modify Bearer Request
  - Table 7.2.7-1: Information Elements in a Modify Bearer Request
- 3GPP 23.401 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 32.299 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).
- 3GPP 29.060 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface.
- 3GPP 29.061 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)

- 3GPP 32.298 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP 29.212 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).

Configuring Virtual-APN

Use the following configuration to display an additional option (LTE-M) “RAT-Type” based Virtual-APN selection .

```
configure
  context context_name
    apn apn_name
       virtual-apn preference value apn apn_name rat-type lte-m
       end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **virtual-apn preference** *value* **apn** *apn_name* : Configures the virtual-apn (virtual.ipv4).
- **rat-type lte-m**: Enables LTE-M as an additional RAT-type.

Configuring qci-qos-mapping

Use the following configuration to configure QCI-QOS mapping in the APN Configuration mode and associate additional RAT type (LTE-M).

```
configure
  context context_name
    apn apn_name
      qci table
       qci-qos-mapping
           qci qci_val non-gbr { downlink user-datagram dscp-marking value
}
           end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **qci-qos-mapping**: Configures the qci-qos-mapping for APN.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 80, 82, and 83.
    - **downlink**: Specifies the direction of traffic on which this QoS configuration needs to be applied.

Associate Qci-Qos-Mapping

Use the configuration to select the qci-qos-mapping RAT Type.

```
configure
  context context_name
    apn apn_name
      associate  qci-qos-mapping table rat-type lte-m
      end
```

NOTES:

- **associate qci-qos-mapping table rat-type lte-m** : Associates apn qci-qos-mapping based on the RAT type.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the LTE-M RAT Type support on the SAEGW, P-GW and S-GW Services.

Show Commands and Output

This section provides information on show commands and their corresponding outputs for the LTE-M RAT type feature.

show apn name

The following output is displayed if the Virtual-APN is selected based on the RAT-Type, during the Session-Setup.

Output:

```
show apn name <>
Virtual APN Configuration:
  Preference  Selected-APN           Rule-Definition
  10          verizon.ipv4           CC Profile Index = 3
   RAT Type = lte-m [local]qvpc-si# show configuration
```

show apn all

The output of **show apn all** and **show apn name** *apn_name* **all** commands has been enhanced to monitor the APN configuration for qci-qos-mapping on RAT type **lte-m**:

Example:

```
show apn name <>
qci-qos-mapping Name for RAT-Type:
GERAN :N/A             UTRAN :N/A
EUTRAN : N/A           LTE-M : table
Stats Profile Name : N/A
```

show qci-qos-mapping table all

Following example is the sample output before associating the qci-qos-mapping table based on additional RAT Type (LTE-M).

```
QCI-QOS Table Name: table

 Qci:  1
  uplink: n/a
  downlink: user-datagram           dscp-marking 0x3e
  maximum packet delay:  n/a        maximum error rate:  n/a
  delay class:  n/a           precedence class:     n/a
  reliability class:  n/a           qci type:   non-gbr
  volte:   n/a                      traffic policing interval:  n/a

 Qci:  2
  uplink: n/a
  downlink: internal-qos priority 1
  maximum packet delay:  n/a        maximum error rate:  n/a
  delay class:     n/a              precedence class:  n/a
  reliability class:     n/a        qci type:   gbr
  volte:     n/a                    traffic policing interval:  n/a
```

show configuration

The **virtual-apn preference** *value* **apn** *apn_name* **rat-type lte-m** output is displayed when the Virtual APN is configured with the LTE-M RAT type. Following is the sample output:

```
[local]qvpc-si# show configuration
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      accounting-mode radius
      ims-auth-service ims-ggsn-auth
      ip access-group acl4-1 in
      ip access-group acl4-1 out
      authentication pap 1 chap 2 allow-noauth
      ip context-name egress
      virtual-apn preference 10 apn verizon.ipv4 rat-type lte-m
      ipv6 access-group acl6-1 in
      ipv6 access-group acl6-1 out
      active-charging rulebase prepaid
    exit
```

Similarly, the **associate qci-qos-mapping table rat-type lte-m** output is displayed for the qci-qos association changes based on RAT type. Following is the sample output

```
 [local]laas-setup# show configuration
                apn intershat
                context ingress
               subscriber default
                nexthop-forwarding-address
                exit
                apn intershat
                associate qci-qos-mapping table rat-type lte-m
                exit
```

show subscribers full

The output of this show command is used for monitoring the subscriber call. The RAT type of the call is displayed as LTE-M. A new field **LTE-M** is added under Access Technology. Following is the sample output:

```
[local]laas-setup# show subscribers all
Access  (X) - CDMA 1xRTT                (E) - GPRS GERAN    (I) - IP
||    Tech:       (D) - CDMA EV-DO      (U) - WCDMA UTRAN   (W) - Wireless LAN
||                (A) - CDMA EV-DO REVA (G) - GPRS Other    (M) - WiMax
```

```
||                (C) - CDMA Other      (J) - GAN           (O) - Femto IPSec
||                (P) - PDIF            (S) - HSPA          (L) - eHRPD
||                (T) - eUTRAN          (B) - PPPoE         (F) - FEMTO UTRAN
||                (N) - NB-IoT          (Q) - WSG           (R)- LTE-M
                  (.) - Other/Unknown
```

show subcscribers full all

The output of the following show commands are used for monitoring the subscriber call. The Access Technology of the call is displayed as LTE-M.

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Tue Mar 23 04:33:55 2021 call duration: 00h00m46s
  idle time: 00h00m40s                idle time left:  n/a
```

show subs pgw-only full / show subs pgw-only full all

The **show subs pgw-only full** / **show subs pgw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
Access Type: gtp-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                   pgw-service-name: PGW21
  Callid: 02fb3ea2                     IMSI: 404005123456789
  MSISDN: 9890098900                   External ID: n/a
  Interface Type: S5S8GTP              Low Access Priority: N/A
  TWAN Mode: N/A
  eMPS Bearer: No
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
```

show subs sgw-only full / show subs sgw-only full all

The **show subs sgw-only full** / **show subs sgw-only full all** scommands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Card/Cpu        : 1/0         Sessmgr Instance : 11
  Idle time       : 00h05m47s
  MS TimeZone     : n/a                  Daylight Saving Time: n/a

  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                           sgw-service-name: SGW21
  Callid: 02fb3ea1                       IMSI: 404005123456789
  MSISDN: 9890098900
  eMPS Bearer: No
```

show subs saegw-only full / show subs saegw-only full all

The **show subs saegw-only full** / **show subs saegw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Callid   : 02fb3ea3                    IMSI                : 404005123456789
  Card/Cpu          : 1/0                          Sessmgr Instance    : 11
  Source context    : EPC2                         Destination context : ISP1
  Bearer Type       : Default                      Bearer-Id           : 5
  Access Type       : gtp-pdn-type-ipv4-ipv6       Network Type        : IPV4+IPv6
```

```
  Access Tech       : LTE-M                       saegw-service-name  : SAEGW21
  MSISDN            : 9890098900                  External ID         : n/a
  TWAN Mode         : N/A
  eMPS Bearer       : No
  WPS Bearer        : No
```

show subs pgw-only all

The **show subs pgw-only all** command displays the following output:.

```
|+------Access     (U) - UTRAN     (G) - GERAN
||       Tech:     (W) - WLAN                (J) - GAN
||                 (U) - HSPA Evolution      (E) - eUTRAN
||                 (H) - eHRPD               (.) - Unknown
||                 (N) - NB-IoT              (R) - LTE-M
```

show subs sgw-only all

The **show subs sgw-only all** command displays the following output:

```
|+----Access    (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:     (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||              (.) - Unknown          (N) - NB-IoT          (R) - LTE-M

||
```

show subs saegw-only all

The **show subs saegw-only all** command displays the following output:

```
|+----Access    (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:     (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||              (H) - eHRPD            (.) - Unknown         (N) - NB-IoT
||              (R) - LTE-M
```

show subscribers callid

The **show subscribers callid** *callid*command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
|+----Access  (X) - CDMA 1xRTT(E) - GPRS GERAN      (I) - IP
||    Tech:   (D) - CDMA EV-DO          (U) - WCDMA UTRAN     (W) - Wireless LAN
||            (A) - CDMA EV-DO REVA     (G) - GPRS Other      (M) - WiMax
||            (C) - CDMA Other          (J) - GAN             (O) - Femto IPSec
||            (P) - PDIF                (S) - HSPA            (L) - eHRPD
||            (T) - eUTRAN              (B) - PPPoE           (F) - FEMTO UTRAN
||            (N) - NB-IoT              (Q) - WSG             (R) - LTE-M

||            (.) - Other/Unknown
```

show session subsystem

The following output displays the session related statistics:

```
LTE-M Data Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
LTE-M Connection Statistics
```

```
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

Similarly, the **show session subsystem full** is enhanced to display the Data packets and subscribers count per RAT type.

show session subsystem verbose

The **show session subsystem verbose** command displays the following output:

```
NB-IoT Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

LTE-M Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

 NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
 LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

show session summary

The **show session summary** command displays the following output:

```
4G LTE (EUTRAN): 0
2G (GERAN): 0
3G (UTRAN): 0
WiFi (WIRELSS LAN): 0
eHRPD: 0
3G HA: 0
NB-IoT: 2
LTE-M: 0
Others: 0
```

show subscribers subscription full

The **show subscribers subscription full** command displays the following output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Wed Mar 17 09:59:47 2021 call duration: 00h01m19s
  idle time: 00h01m13s                idle time left:  n/a
  session time left:  n/a
```

show subscribers activity all

The **show subscribers activity all** command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
```

```
  Access Tech: LTE-M                    Access Network Peer ID: n/a
  callid: 02fb3ea1                      msid: 404005123456789
```

show apn statistics all-name

The show output command displays the statistics per APN and also displays number of initiated sessions and active sessions with LTE-M RAT Type per APN. Following is the sample output:

```
Initiated Sessions per RAT Type:
    EUTRAN:  0    UTRAN:   0
    GERAN:   0    EHRPD:   0
    S2A GTP: 0    S2B GTP: 0
    S2B PMIP:0    NB-IoT:  0
    LTE-M :  0

  Active Sessions per RAT Type:
   EUTRAN: 0   UTRAN: 0
   GERAN:  0   WLAN:  0
   HSPA:   0   NB-IoT:0
   LTE-M:  0   OTHER: 0
```

show saegw-service statistics all-name

The show output command displays the statistics per SAEGW service and also displays Current subscribers, the Current PDNs with NB-IoT RAT Type per SAEGW Service. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    NB-IoT:                         0
  LTE-M:                            0    OTHER:                          0

Current PDNs By RAT-Type:
    EUTRAN:                         0    UTRAN:                        0
    GERAN:                          0    NB-IoT:                       0
    LTE-M:                          0    OTHER:                        0
```

show pgw-service statistics all-name

The show output command displays statistics for each P-GW Services, the number of initiated PDNs, and current PDNs with NB-IoT RAT Type for each P-GW Services. Following is the sample output:

```
Initiated PDNs By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    EHRPD:                          0
  S2A GTP:                          0    S2B GTP:                        0
  S2B PMIP:                         0    NB-IoT:                         0
  LTE-M                         0

Current PDNs By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    WLAN:                           0
  NB-IoT:                           0    LTE-M                           0
  OTHER:                            0
```

show sgw-service statistics

This show command displays statistics for each S-GW Services. This CLI is enhanced to display Current Subscribers and Current PDNs with NB-IoT RAT type for each S-GW Services. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                           0    UTRAN:                           0
  GERAN:                            0    NB-IoT:                          0
  LTE-M:                            0    OTHER:                           0
Current PDNs By RAT-Type:
    EUTRAN:                         0    UTRAN:                           0
    GERAN:                          0    NB-IoT:                          0
    LTE-M:                          0    OTHER:                           0
```

Bulk Statistics

The following statistics are added in support of the LTE-M RAT type feature

APN Schema

The following LTE-M RAT type feature-related bulk statistics are available in the APN schema.

Bulk Statistics	Description
active-lte-m-sessions	The total number of active LTE-M sessions per APN with RAT type LTE-M.
initiated-lte-m-sessions	The total number of initiated LTE-M sessions.

P-GW Schema

The following LTE-M RAT type feature related bulk statistics available in the P-GW schema.

Bulk Statistics	Description
sesstat-pdn-rat-lte-m	The total number of active PDN Type Statistics – LTE-M.
sessstat-rat-init-lte-m	The total number of initiated LTE-M PDNs (with RAT Type LTE-M).

S-GW Schema

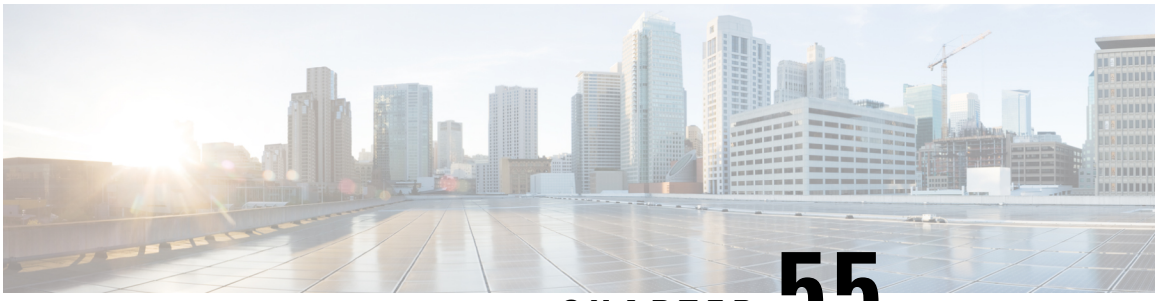
The following LTE-M RAT type feature related bulk statistics available in the S-GW schema.

Bulk Statistics	Description
sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sessstat-totcur-pdn-lte-m	The total number of active PDNs with LTE-M RAT type.

SAEGW Schema

The following LTE-M RAT type feature related bulk statistics available in the SAE-GW schema.

Bulk Statistics	Description
sgw-sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sgw-sessstat-totcur-pdn-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sesstat-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sessstat-pdn-rat-init-lte-m	The total number of initiated LTE-M PDNs.
saegw-sgw-anchor-pdn-rat-lte-m	The total number of LTE-M PDNs (SGW anchored) with RAT Type LTE-M.
saegw-pgw-anchor-pdn-rat-lte-sm	The total number of LTE-M PDNs (PGW anchored) with RAT Type LTE-M.
saegw-collapsed-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.



CHAPTER 55

Maximum Receive Unit Configuration Support

- Feature Summary and Revision History, on page 943
- Feature Description, on page 944
- How It Works, on page 944
- Configuring the MRU Feature, on page 944

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

Prior to MRU Configuration support, the Maximum Receive Unit (MRU) setting was equal to the Maximum Transmission Unit (MTU).

When the MTU of eNB on the S1-U interface was increased to 2000 bytes but no changes were made on the MTU on S1-U interface on SAE-GW, packets were received at SAE-GW with size more than 1500 bytes. This resulted into those packets getting dropped at the S1-U interface on the SAE-GW with **Lport_MRU_exceeded** exception. This was affecting UEs that were trying to set up IKE Tunnels.

This Configure MRU feature allows you to configure MRU separately from MTU.

How It Works

To handle MRU independently of MTU, changes are made in Network Processing Unit (NPU), NPUSIM, NPUMGR, and CLI.

Configuring the MRU Feature

This section describes how to configure the MRU of the IP interface along with MTU using the **ip mtu** keyword under interface configuration.

Configuring MRU

To configure the MTU and MRU in the Ethernet Interface Configuration mode, use the following sample configuration.

```
config
  context context_name
    interface interface_name broadcast
    ip mtu mtu_size [ mru mru_size ]
    end
```

NOTES:

- **ip mtu** *mtu_size*: Specify the MTU size. *mtu_size* must be an integer in the range of 5762048 bytes.
- **mru** *mru_size*: Specify the MRU size. *mru_size* must be an integer in the range of 5762048 bytes.
- Use the **no ip mtu** command to disable the MTU configuration.
- The maximum configurable value for MTU is 2048 bytes.. If MTU is not configured, the default value is 1500 bytes.
- MRU attribute is optional and when it is not configured, MRU is set to the same value as MTU.
- MRU optional attribute is not applicable to VPC-DI and VPC-SI platforms. This attribute is only visible on ASR 5500.
- On CUPS or ICUPS, the following error is displayed you when you try to configure MRU on an interface.

```
Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
enabled!
```

- Although the product allows configuring asymmetric MTU and MRU values on the same interface is not advised as it may result into undesirable behavior on the network.

Configuring the MRU Feature when no MTU is specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     bfd interval 300 min_rx 300 multiplier 3
     #exit
#exit
```

Configuring the MTU Feature when no MRU is specified

MRU = Configured MTU for backward compatibility. MRU = MTU = 1970 bytes.

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1970
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Configuring the MTU Feature when both MTU and MRU are specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1600 mru 1700
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Verifying the Configured MRU

The output of the is enhanced to display the configured MRU value.

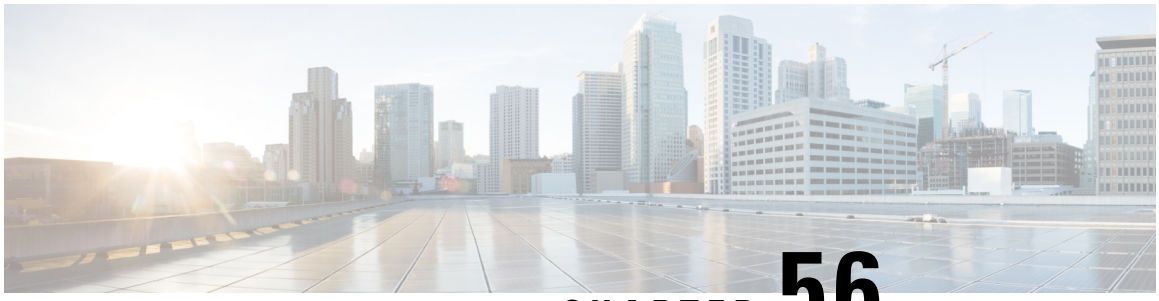
For example:

```
[EPC2]26kl-chassis# config
[EPC2]26kl-chassis(config)# context EPC2
[EPC2]26kl-chassis(config-ctx)# interface TO-EPC2-SGW-INGRESS
[EPC2]26kl-chassis(config-if-eth)# ip mtu 1500 mru 1970
```

```
[EPC2]26kl-chassis(config-if-eth)# end
[EPC2]26kl-chassis# show ipv6 interface
Intf Name: TO-EPC1-SGW-INGRESS
Intf Type: Broadcast
Description:
VRF: None
IP State: UP (Bound to 5/20 vlan id 190, 802.1P prior 0, ifIndex 85196802)
Router Advertisement: disabled MTU: 1500 MRU: 1970
IPv6 Link-Local Address: fe80::d272:dcff:fea3:8543/64
IPv6 Global Unicast Address: 2001::1:21/64
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 5
IPv6 Address: 2001::1:31/64
IPv6 Address: 2001::1:205/64
IP Address: 10.10.10.21 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.31 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.200 Subnet Mask: 255.255.255.0
```

NOTES:

- Use the **show ipv6 interface** command to verify if the Configurable MTU configuration is enabled or disabled.
- **no ip mtu**: Disables the Configurable MTU configuration.



CHAPTER 56

Message Priority Indication over GTPC

This chapter describes the following topics:

- Feature Summary and Revision History, on page 947
- Feature Description, on page 948
- How It Works, on page 950
- Configuring the Message Priority over GTP Feature, on page 952
- Monitoring and Troubleshooting, on page 954

Feature Summary and Revision History

Summary Data

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

Revision History



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

Revision Details	Release
The Message Priority Indication over GTP feature provides support to set the GTPC MP flag and Message Priority value for GTPC messages and Gx DRMP AVP for Gx messages for eMPS and non-eMPS sessions.	21.4
First introduced.	21.3

Feature Description

The GTPC Message Priority or Gx Diameter Routing Message Priority (DRMP) AVP indicate priority of a message. This addresses the purpose of deciding the message priority without having to open the complete message.

The Message Priority Indication over GTP feature provides support to set the GTPC MP flag and Message Priority value. The MP flag and Message Priority values can be set for GTPC messages and Gx DRMP AVP for Gx messages for eMPS and non-eMPS sessions.

GTPC Message Priority and DRMP AVP do not indicate that session is an Enhanced Multimedia Priority Service (eMPS).

This feature supports the following behavior of the GTPC messages:

1. Incoming GTPC messages having MP flag set and Message Priority set as 0 for eMPS sessions are excluded from the GTP demux incoming throttling. This is CLI controlled.

   Incoming GTPC messages for eMPS sessions are excluded from throttling due to Load Overload control, that is, self-overload protection (this is already supported).

   Therefore, overall incoming GTPC messages having MP flag set and Message Priority as 0 for eMPS sessions are excluded from:

   - demux incoming throttling
   - throttling due to Load Overload control (self-overload protection)

2. In the GTPC Request messages, the GTPC MP flag is set to “1” and GTPC Message Priority value is set to “0” in the GTP header. This is applicable to the messages that the P-GW sends when network-initiated procedures (PCRF) trigger these for eMPS sessions or those leading to toggling of eMPS status of the session. (That is, eMPS upgrade or downgrade scenarios.) This is CLI controlled.

3. In the GTPC Request messages, the GTPC MP flag and GTPC Message Priority value is set to the same respective values in the GTP header as were received in the corresponding incoming “command” message. This is applicable to the messages that the P-GW sends when triggered because of UE initiated procedures (that is, due to an incoming command" message) for all sessions (eMPS and non-eMPS). This is not CLI-controlled.

   Note the behavior in the following two scenarios for an incoming command message.

   - If the response from the peer for a GTPC Request message is received with cause “Temporarily rejected due to handover/TAU/RAU procedure in progress”, then reattempt to send the GTPC request message does not carry the GTPC MP flag and GTPC Message Priority value of the incoming command message. This is applicable to the messages that the P-GW sends when triggered because

of UE initiated procedures (that is, due to an incoming command" message). Hence, behavior explained in point number 2 is applicable for such messages.

- If the incoming command message is a bearer resource command that creates or updates the bearer where the size of the TFT exceeds the maximum size that can be sent in Create or Update Bearer Request message, then it prompts two request messages to be sent. That is, either Create Bearer Request followed by Update Bearer Request or Update Bearer Request followed by Update Bearer Request message (this is the legacy P-GW behavior). In this case, the first request message is sent with the GTPC MP flag and GTPC Message Priority value of the incoming command message. However, the second request message does not carry the GTPC MP flag and GTPC Message Priority value of the incoming command message. Hence, behavior explained in point number 2 is applicable for such messages.

4. In the GTPC Response messages, the GTPC MP flag and GTPC Message Priority value is set to the same respective values in the GTP header as were received in the corresponding incoming request message. This is applicable to the messages that the P-GW sends for all sessions (eMPS and non-eMPS). This is not CLI-controlled.
5. Outgoing Gx messages (CCR-I/U/T) for eMPS sessions or those because of toggling of the eMPS status of the session (that is, eMPS upgrade or downgrade scenarios) have the DRMP AVP value set as 0. This is CLI controlled.
6. Outgoing Gx RAA messages match the DRMP value sent in RAR from PCRF, irrespective of the CLI configuration for session prioritization.

The Message Priority Indication over GTP feature can be configured using the following commands:

- **emps-profile**: This is an existing CLI command.
- **message-priority**: This is a new CLI command introduced in support of this feature.
- **gtpc overload-protection ingress**: This is an existing CLI command to which the new priority-message keyword is added.
- **diameter session-prioritization**: This is an existing CLI command whose behavior is modified in support of this feature.

  The **diameter session-prioritization** CLI command populates the Gx Credit Control Request (Initial, Update, and Terminate) messages for eMPS sessions and eMPS upgrade and downgrade with DRMP AVP with value 0. This helps the intermediate nodes to route the messages with higher priority. The encoding is applied to eMPS enabled sessions and on eMPS upgrade or downgrade of the sessions.

  The **diameter session-prioritization** CLI command initially controlled the prioritization of Gx messages for eMPS sessions for eMPS upgrade and downgrade transactions.

  The **diameter session-prioritization** CLI command now also controls sending DRMP AVP with a value of 0 in the Credit Control Request (Initial, Update, and Terminate) messages over the Gx interface for eMPS sessions and for eMPS upgrade and downgrade transactions.

Note

- For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPS bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.
- For supplemental information related to Gx support for eMPS, refer to the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

Important This feature is license controlled. Contact your Cisco account representative for information on how to obtain a license.

Relationships to Other Features

This feature is related to eMPS profile, Load Overload Control, Gx RLF throttling, and Max-outstanding configuration features, and one or more among these features may require additional license key to be installed.

How It Works

The following section provides a brief overview of how this feature works.

GTP Incoming Throttling Bypass

GTP Incoming Throttling Bypass is applicable for incoming GTPC request messages landing on the demux Manager (egtpinmgr) at the P-GW ingress interface.

- **High Priority Messages:** Incoming GTPC messages with “MP” flag set and “Message Priority” value set as 0 on the P-GW ingress interface.
- **High Priority CSReq Messages:** Incoming CSReq messages with “MP” flag set and “Message Priority” value set as 0 on the P-GW ingress interface.
- **Low Priority Messages:** All other Incoming GTPC messages without the MP flag.

If the new **exclude priority-message** CLI keyword is configured, it applies the following behavior to bypass incoming throttling for high priority messages:

- High priority messages, the default configuration for “msg-rate” and “queue-size” of demux are applicable (even if they are configured with a different value). The default value for “msg-rate” is 0, which implies that High Priority setting is disabled. The default value for “queue-size” is 10000.
- There is no throttling applied due to the “delay-tolerance” parameter for High Priority messages.
- Also High Priority Create Session Request (CSReq) messages are prioritized over other messages. However, High Priority CSReq messages are processed in sequence.
- When a High Priority message is received and the queue is overloaded then a Low Priority message is discarded from the queue to accommodate the High Priority message.

- In a rare scenario where all the messages in the queue are High Priority and the queue is overloaded, then the new High Priority message may get dropped.
- If ingress throttling is configured using "gtpc overload-protection ingress" with "exclude priority-message" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on the demux message queue size, the default queue size value of 10,000 is used. (This is the same behavior if **exclude sgw-interface** is selected.)
- If ingress throttling is configured using "gtpc overload-protection ingress" without the "exclude" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on demux message queue size, the configured queue-size value is used.

The following table describes the behavior when the **exclude priority-message** is configured:

GTPC Incoming Throttling Demux Queue-size Configuration (100 to 10000)	Is "exclude priority-message" configured	Demux Queue-size used for GTPC Incoming Throttling for S-GW/GGSN/ "Low Priority" P-GW messages	Demux Queue-size used for "High Priority messages" P-GW messages	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW
No configuration/Default configuration	No	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
No configuration/Default configuration	Yes	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
5000 (or any configured value from 100 to10000)	No	5000 (or the configured value)	5000 (or the configured value)	Configured_congestion_threshold * 5000 (default)
5000 (or any configured value from 100 to10000)	Yes	5000 (or the configured value)	10000 (because "exclude priority-message" is configured)	Configured_congestion_threshold * 10000 (this is the behavior change for congestion control, if "exclude priority-message" is configured)

Gx DRMP AVP Encoding

The Gx DRMP AVP is encoded when the **diameter session-prioritization** CLI is enabled in IMS Authorization Policy Control Configuration mode for policy control application. The following table summarizes the DRMP AVP values that are sent based on the different configurations and scenarios.

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
Off	Any	CCR Messages	Not Encoded

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
Any	Any	RAA response to RAR with DRMP X	Encoded/X
Off	eMPS	CCR Messages	Not Encoded
On	Yes	CCR Messages	Not Encoded
On	eMPS	CCR Messages	Encoded/0
On	Non-eMPS	CCR-U generated on eMPS state change from disabled to enabled.	Encoded/0
On	eMPS	CCR-U generated on eMPS state change from enabled to disabled.	Encoded/0
On	Non-eMPS	eMPS Upgrade failed and CCR-U follows	Encoded/0

Configuring the Message Priority over GTP Feature

The following section provides the configuration commands to enable or disable the feature.

emps-profile

In the eMPS Profile Configuration mode, the emps-profile command now supports the eMPS profile to identify or mark a bearer or session as an eMPS bearer or session.

To set the eMPS profile, enter the following commands:

```
configure
 emps-profile emps_profile_name
  earp earp_value earp_value
  end
```



Note For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPS bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

priority-message

The **gtpc overload-protection ingress** CLI command is provided with a new keyword, **priority-message**. This keyword enables bypassing of demux incoming throttling for incoming GTPC request messages where the “MP” flag is set as 1 and Message Priority value set as 0 in the GTP header.

To enable the priority of a message, enter the following commands:

```
configure
 context context_name
  gtpc overload-protection ingress { msg-rate msg_rate  }  delay-tolerance
dur ] [ queue-size size ] [ exclude { sgw-interface [ priority-message ] }
 | { priority-message [ sgw-interface ] } ]
  end
```

Notes:

priority-message: Bypasses incoming throttling at the P-GW ingress interface for GTPC incoming messages that have the message priority flag set and message priority value as 0 in the GTP header. The message queue that is considered for the Congestion Control feature for P-GW, S-GW, and GGSN is reset to the default value of 10,000 if this keyword is configured.

This CLI is disabled by default.

The **priority-message** keyword is applicable only for the P-GW.

message-priority

This new command enables setting of the GTPC MP flag to “1” and GTPC Message Priority value to “0” in the GTPC header. This is applicable to GTPC Request messages that the P-GW sends because of network-initiated procedures (PCRF) for eMPS sessions or those leading to toggling of eMPS status of the session (that is, eMPS upgrade or downgrade scenarios).

To enable message priority, enter the following commands:

```
configure
 emps-profile profile_name
  [ no ]  message-priority
  end
```

Notes:

- **no:** Disables the command.
- **message-priority:** Sets the MP flag to 1 and Message Priority value to 0 in GTPC header of all request messages sent by P-GW triggered because of network-initiated procedure (PCRF) in any of the following scenarios:
  - On an eMPS session
  - Non-eMPS session to eMPS session
  - eMPS session to non-eMPS session
- This CLI is disabled by default.

diameter session-prioritization

In the IMS Authorization Service Configuration mode, the **diameter session-prioritization** CLI command is enhanced to populate the Gx Credit Control Request (Initial, Update, and Terminate) messages for eMPS sessions and eMPS upgrade and downgrade with DRMP AVP with value 0. This helps the intermediate nodes to route the messages with higher priority. The encoding is applied to eMPS enabled sessions and on eMPS upgrade or downgrade of the sessions. Also the existing behavior of prioritization of Gx messages for eMPS sessions and eMPS upgrade and downgrade continues.

To set the DRMP AVP value in the CCR message, enter the following commands:

```
context context_name
 ims-auth-service service_name
  policy control
   [ no ] diameter session-prioritization
   end
```

Notes:

- **no:** Disables prioritization of Gx messages for eMPS sessions and eMPS upgrade and downgrade. It also disables encoding of DRMP AVP (value 0) in Credit Control Request (Initial, Update, and Terminate) messages for eMPS sessions and eMPS upgrade and downgrade.
- **session-prioritization:** Prioritizes and sets the DRMP AVP values as 0 for Credit Control Request messages of eMPS sessions.
- This CLI is disabled by default.

Monitoring and Troubleshooting

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

Show Commands and/or Outputs

The output of the following CLI commands has been enhanced in support of the feature:

show emps-profile

The output of the show emps-profile name *name* and show emps-profile all CLI commands now include the message-priority field in support of this feature.

When "message-priority" is not configured or "no message-priority" is configured: show emps-profile name

```
show emps-profile name abcd
eMPS Profiles
---------------------------------
  eMPS Profile Name : abcd
  earp configured : None
  dscp-marking configured : None
  message-priority : Disabled
```

When "message-priority" is not configured or "no message-priority" is configured: show emps-profile name all

```
show emps-profile name all
eMPS Profiles
---------------------------------
  eMPS Profile Name : xyz
  earp configured :  2 3
  dscp-marking configured : None
  message-priority : Disabled
```

When “message-priority” is configured: show emps-profile name

```
show emps-profile name abcd
eMPS Profiles
---------------------------------
  eMPS Profile Name : abcd
  earp configured : None
  dscp-marking configured : None
  message-priority : 0
```

When “message-priority” is configured: show emps-profile name all

```
show emps-profile name all
eMPS Profiles
---------------------------------
  eMPS Profile Name : xyz
  earp configured :  2 3
  dscp-marking configured : None
  message-priority : 0
```

show pgw-service

The output of the show pgw-service name *name* and show pgw-service all CLI commands now include the Priority message Excluded field in support of this feature.

Default configuration: show pgw-service name

```
show pgw-service name pgw_service
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
```

```
  SGW interface Excluded:          Yes
  Priority message Excluded:       No

  Queue size for Congestion Control : 10000
```

Default configuration: show pgw-service all

```
show pgw-service all
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Outgoing Throttling:        Disabled
  RLF Template Name:               N/A
  Throttling override:             Disabled
  Throttling override Policy:      N/A

  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
 Priority message Excluded:       No

  Queue size for Congestion Control : 10000
```

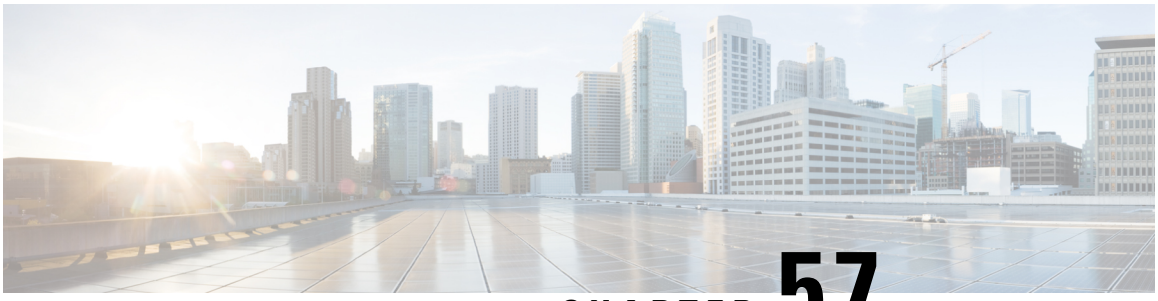
When “exclude priority-message” is configured: show pgw-service name

```
show pgw-service name pgw_service
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
```

```
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
  Priority message Excluded:       Yes

  Queue size for Congestion Control : 10000
```

When “exclude priority-message” is configured: show pgw-service all

```
show pgw-service all
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Outgoing Throttling:        Disabled
  RLF Template Name:               N/A
  Throttling override:             Disabled
  Throttling override Policy:      N/A

  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
  Priority message Excluded:       Yes
  Queue size for Congestion Control : 10000
```



CHAPTER 57

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, on page 959
- Configuring Registration Revocation, on page 960

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
```

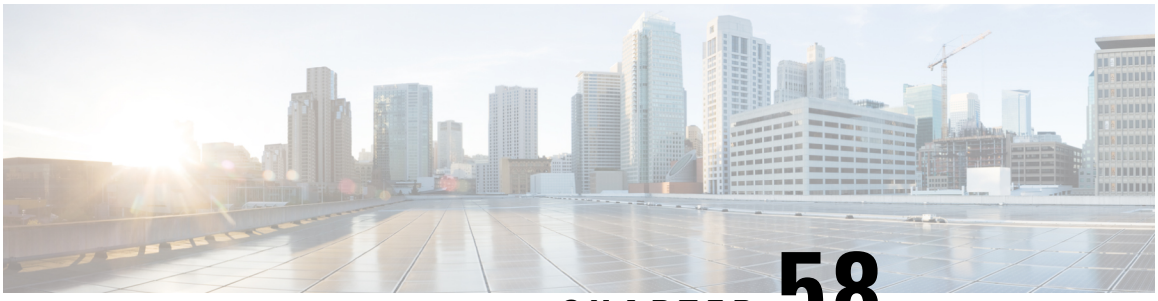
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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*.



CHAPTER 58

Mobile Hotspot Usage on RADIUS Accounting

- Feature Summary and Revision History, on page 963
- Feature Description, on page 963
- Configuring MHS Usage on RADIUS Accounting, on page 964
- Monitoring and Troubleshooting, on page 966

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ICUPS • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, P-GW supports Mobility Hotspot (MHS) usage on RADIUS accounting.	21.23

Feature Description

In RADIUS Accounting, the subscriber data usage is monitored using the Type Length Values (TLV) namely Acct-Input-Octets and Acct-Output-Octets to receive a cumulative data usage report. In this StarOS 21.23 release, to identify Data usage differentiation effectively in RADIUS accounting for 4G Mobile Hotspot (MHS) data usage, 5G MHS data usage, and 5G composite data usage the following new TLVs are introduced:

- 4G_MHS_Acct_Input_Octets
- 4G_MHS_Acct_Output_Octets
- 5G_MHS_Acct_Input_Octets
- 5G_MHS_Acct_Output_Octets
- 5G_Comp_Acct_Input_Octets
- 5G_Comp_Acct_Output_Octets

RADIUS interim and stop messages report MHS data usage . MHS data usage reporting is allowed per bearer. These TLVs comprises of the cumulative values from the previous interim messages and raw bytes.

When MHS data usage reporting is dynamically enabled or disabled, the change takes effect only for the new calls.

Note Only EUTRAN and NB_IOT Radio Access Technology (RAT) types are supported for MHS data usage reporting.

The PRA IDs that are configured in a PRA profile which are associated with APN level are used to identify 5G data usage.

Relationship with Other Features

This feature is related to Smartphone Tethering Detection Support feature. For more information about Smartphone Tethering Detection support, refer the *PDN Gateway Overview* chapter in the *P-GW Administration Guide*.

License Requirements

The Mobile Hotspot usage on RADIUS Accounting feature requires enabling of Tethering Detection License. Contact your 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 is the known limitations of the feature:

- The MHS supports only dictionary custom76.

Configuring MHS Usage on RADIUS Accounting

This section provides information on configuring MHS Usage on RADIUS accounting.

Configuring PRA Profiles

Use the following command to configure PRA profiles to differentiate traffic.

```
configure
          context context_name
            pra-profile pra_profile_name
             [ no ] pra-id pra_id_value traffic-map-type type_value
          end
```

NOTES:

- **pra-profile**: Configures PRA profiles to differentiate traffic.
- **pra-id**: Configures the PRA ID.
- **no**: Removes the PRA ID.
- **traffic-map-type** : Configures the traffic map type.
- **type_value**: Enter enum values - 5G.

NOTES:

A maximum of three PRA IDs per PRA list and associate PRA list in APN level are allowed to differentiate 5G traffic.

Associating PRA Profiles at APN Level

Use the following CLI commands to associate PRA profiles at APN level:

```
configure
  context context_name
    apn apn_name
      [ no ] pra-profile profile_value
 exit
```

NOTES:

- **apn**: Configures the APN.
- **pra-profile**: Associates PRA profiles at APN level.
- **no**: Removes PRA profiles at APN level.

Configuring AAA Group

Use the following commands to configure AAA Group for the newly-added TLVs to send RADIUS Accounting messages.

```
configure
          context context_name
            aaa group group_name
              [ no ] radius accounting mhs-traffic enable
```

```
    radius dictionary custom76
end
```

NOTES:

- **mhs-traffic**: Specifies MHS data usage reporting.
- **enable**: Enables MHS data usage reporting.
- **no**: Disables MHS data usage reporting.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available to support this feature.

Show Commands and Output

This section provides information regarding show commands and their outputs for this feature.

show subscribers pgw-only full all

The output of the **show subscribers pgw-only full all** command displays the following details:

Field	Description
4G MHS Input Bytes	The total number of input bytes used with 4G Tethering.
4G MHS Output Bytes	The total number of output bytes used with 4G Tethering.
5G MHS Input Bytes	The total number of input bytes used with 5G Tethering.
5G MHS Output Bytes	The total number of output bytes used with 5G Tethering.
5G Composite Input Bytes	The total number of input bytes used with 5G Composite (Tethering and non-Tethering).
5G Composite Output Bytes	The total number of output bytes used with 5G Composite (Tethering and non-Tethering).

show subscribers saegw-only full all

The output of the **show subscribers saegw-only full all** command displays the following details:

Field	Description
4G MHS Input Bytes	The total number of input bytes used with 4G Tethering.
4G MHS Output Bytes	The total number of output bytes used with 4G Tethering.
5G MHS Input Bytes	The total number of input bytes used with 5G Tethering.

Field	Description
5G MHS Output Bytes	The total number of output bytes used with 5G Tethering.
5G Composite Input Bytes	The total number of input bytes used with 5G Composite (Tethering and non-Tethering).
5G Composite Output Bytes	The total number of output bytes used with 5G Composite (Tethering and non-Tethering).

show apn name

The output of the **show apn name** command displays the following details:

Field	Description
pra-profile Name	Specifies the PRA name to be associated in APN for differentiating 5G traffic..

show aaa group name

The output of the **show aaa group name** command displays the following details:

Field	Description
Allow accounting MHS Traffic	Enables reporting MHS Data usage in RADIUS accounting messages.

show pra-profile name

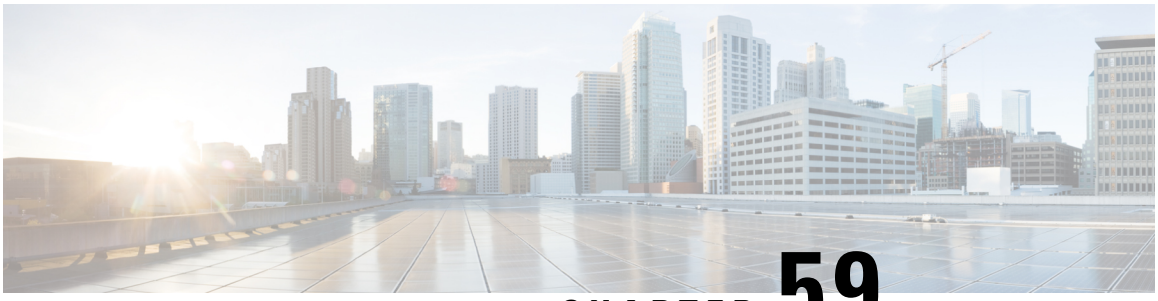
The output of the **show pra-profile name** command displays the following details:

Field	Description
pra profile name	The PRA profile name to be associated in APN for differentiating 5G traffic.
Context	The context name.
PRA Id	The PRA ID to be associated in APN.
Traffic mapping type	The 5G traffic map type.

show pra-profile all

The output of the **show pra-profile all** command displays the following details:

Field	Description
pra profile name	The PRA profile name to be associated in APN for differentiating 5G traffic.
Context	The context name.
PRA Id	The PRA ID to be associated in APN.
Traffic mapping type	The 5G traffic map type.



CHAPTER 59

Multi-Protocol Label Switching (MPLS) Support

This chapter describes the system's support for BGP/MPLS VPN and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on specific systems. 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.

When enabled through a feature license key, the system supports MPLS to provide a VPN connectivity from the system to the corporate's network.

Important This release provides BGP/MPLS VPN for directly connected PE routers only.

MP-BGP is used to negotiate the routes and segregate the traffic for the VPNs. The network node learns the VPN routes from the connected Provider Edge (PE), while the PE populates its routing table with the routes provided by the network functions.

- Overview, on page 969
- Supported Standards, on page 971
- Supported Networks and Platforms, on page 972
- Licenses, on page 972
- Benefits, on page 972
- Configuring BGP/MPLS VPN with Static Labels, on page 972
- Configuring BGP/MPLS VPN with Dynamic Labels, on page 975

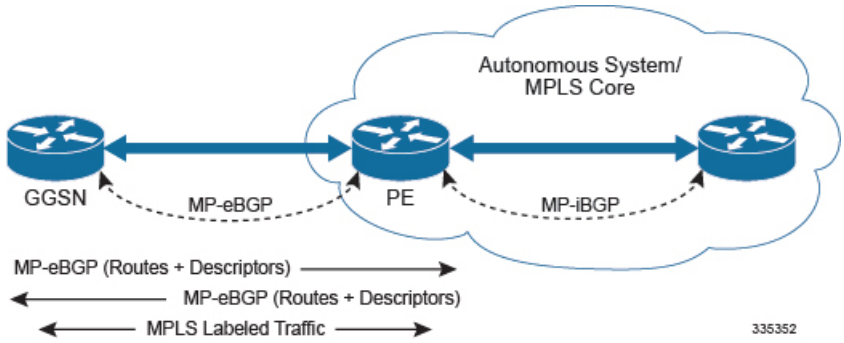
Overview

As seen in the following scenario, the chassis can be deployed as a router while supporting BGP/MPLS-VPN in a network.

- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Provider Edge (PE)
- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Autonomous System Border Router (ASBR)

Chassis as MPLS-CE Connecting to PE

Figure 95: Chassis as MPLS-CE Connected to PE



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the Configuring BGP/MPLS VPN with Static Labels, on page 972 section and refer to Configuring BGP/MPLS VPN with Static Labels, on page 972 for dynamic label configuration.

The system is in a separate autonomous system (AS) from the Provider Edge (PE). It communicates with the PE and all VPN routes are exchanged over MP-BGP. Routes belonging to different VPNs are logically separated, using separate virtual route forwarding tables (VRFs).

Routes for each VPN are advertised as VPN-IPv4 routes, where route distinguishers are prepended to regular IPv4 routes to allow them to be unique within the routing table. Route targets added to the BGP extended community attributes identify different VPN address spaces. The particular upstream BGP peer routing domain (VPN), from which a route is to be imported by the downstream peer into an appropriate VRF, is identified with an extended community in the advertised NLRI.

A unique label is also received or advertised for every VPN route.

The Customer Edge (CE) also advertises routes to the PE using NLRIs that include route distinguishers to differentiate VPNs, an extended community to identify VRFs, and a MPLS-label, which will later be used to forward data traffic.

There is a single MPLS-capable link between the CE and the PE. MP-BGP communicates across this link as a TCP session over IP. Data packets are sent bidirectionally as MPLS encapsulated packets.

This solution does not use any MPLS protocols. The MPLS label corresponding to the immediate upstream neighbor can be statically configured on the downstream router, and similarly in the reverse direction.

When forwarding subscriber packets in the upstream direction to the PE, the CE encapsulates packets with MPLS headers that identify the upstream VRF (the label sent with the NLRI) and the immediate next hop. When the PE receives a packet it swaps the label and forward.

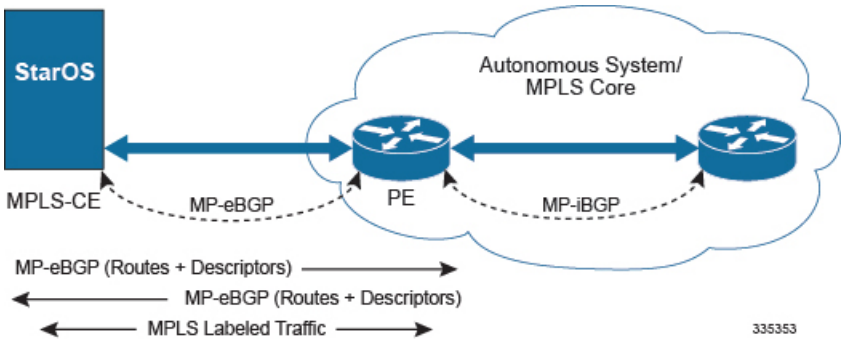
The CE does not run any MPLS protocol (LDP or RSVP-TE).

When receiving data packets in the downstream direction from the PE, the label is checked to identify the destination VRF. Then the packet is de-encapsulated into an IP packet and sent to the session subsystem for processing.

Important MPLS ping/trace route debugging facilities are not supported.

Chassis as MPLS-CE Connected to ASBR

Figure 96: Chassis as MPLS-CE Connected to ASBR



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to Configuring BGP/MPLS VPN with Static Labels, on page 972 and refer to Configuring BGP/MPLS VPN with Dynamic Labels, on page 975 for dynamic label configuration.

This scenario differs from the MPLS-CE with PE scenario in terms of peer functionality even though MPLS-CE functionality does not change. Like the MPLS-CE with PE scenario, MPLS-CE system maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session.

The peer in this scenario is not a PE router but an Autonomous System Border Router (ASBR). The ASBR does not need to maintain any VRF configuration. The PE routers use IBGP to redistribute labeled VPN-IPv4 routes either to an ASBR or to a route reflector (of which the ASBR is a client). The ASBR then uses the eBGP to redistribute those labeled VPN-IPv4 routes to an MPLS-CE in another AS. Because of the eBGP connection, the ASBR changes the next-hop and labels the routes learned from the iBGP peers before advertising to the MPLS-CE. The MPLS-CE is directly connected to the eBGP peering and uses only the MP-eBGP to advertise and learn routes. The MPLS-CE pushes/pops a single label to/from the ASBR, which is learned over the MP-eBGP connection. This scenario avoids the configuration of VRFs on the PE, which have already been configured on the MPLS-CE.

Engineering Rules

- Up to 5,000 "host routes" spread across multiple VRFs per BGP process. Limited to 6,000 pool routes per chassis.
- Up to 2,048 VRFs per chassis.

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 4364, BGP/MPLS IP VPNs
- RFC 3032, MPLS Label Stack Encoding

Important One or more sections of above mentioned IETF are partially supported for this feature. For more information on Statement of Compliance, contact your Cisco account representative.

Supported Networks and Platforms

This feature supports all ASR5500 platforms with StarOS Release 9.0 or later running with network function services.

Licenses

Multi-protocol label switching (MPLS) 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*.

Benefits

MPLS provides networks with a more efficient way to manage applications and move information between locations. MPLS prioritizes network traffic, so administrators can specify which applications should move across the network ahead of others.

Configuring BGP/MPLS VPN with Static Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with static MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.

Important The feature described in this chapter is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

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 BGP/MPLS VPN:

Procedure

Step 1 Create a VRF on the router and assign a VRF name, define the Route-Distinguisher first before you execute the Route Target. For more information on the configuration see the Create VRF with Route-distinguisher and Route-target, on page 973 section.

Step 2 Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in Set Neighbors and Enable VPNv4 Route Exchange, on page 973.

Step 3 Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in Configure Address Family and Redistributed Connected Routes, on page 974. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.

Step 4 Configure IP Pools with MPLS labels for input and output by applying the example configuration in Configure IP Pools with MPLS Labels, on page 974.

Step 5 *Optional*. Bind DHCP service to work with MPLS labels for input and output in corporate networks by applying the example configuration in Bind DHCP Service for Corporate Servers, on page 974.

Step 6 *Optional*. Bind AAA/RADIUS server group in corporate network to work with MPLS labels for input and output by applying the example configuration in Bind AAA Group for Corporate Servers, on page 975.

Step 7 Save your configuration as described in the *System Administration Guide*.

Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second **ip vrf** command creates the route-distinguisher and route-target.

```
configure
   context <context_name> -noconfirm
      ip vrf <vrf_name>
         router bgp <as_number>
            ip vrf <vrf_name>
               route-distinguisher {<as_value> | <ip_address>} <rt_value>
               route-target export {<as_value> | <ip_address>} <rt_value>
               end
```

Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

```
configure
   context <context_name>
      router bgp <as_number>
         neighbor <ip_address> remote-as <AS_num>
         address-family vpnv4
         neighbor <ip_address> activate
         neighbor <ip_address> send-community both
         exit
      interface <bind_intfc_name>
```

```
ip address <ip_addr_mask_combo>
end
```

Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```
configure
  context <context_name>
    router bgp <as_number>
      address-family ipv4 <type> vrf <vrf_name>
        redistribute connected
        end
```



Note StarOS considers the below address range as Martian and hence rejects any BGP updates falling under this range.

Also, StarOS does not allow BGP network command to configure from the below ranges.

- 127.x.x.x
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x

Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with MPLS labels for input and output.

```
configure
  context <context_name> -noconfirm
    ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name> mpls-label input
 <in_label_value> output <out_label_value1> nexthop-forwarding-address
<ip_addr_bgp_neighbor>
    end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with MPLS labels for input and output in Corporate network.

```
configure
  context <dest_ctxt_name>
    interface <intfc_name> loopback
      ip vrf forwarding <vrf_name>
      ip address <bind_ip_address subnet_mask>
      exit
```

```
      dhcp-service <dhcp_svc_name>
         dhcp ip vrf <vrf_name>
         bind address <bind_ip_address> [ nexthop-forwarding-address
<nexthop_ip_address> [ mpls-label input <in_mpls_label_value> output
<out_mpls_label_value1> [ <out_mpls_label_value2> ]]]
         dhcp server <ip_address>
         end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <*ip_address*> **mpls-label input** <*in_mpls_label_value*> **output <** <*out_mpls_label_value1*> applies DHCP over MPLS traffic.

Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with MPLS labels for input and output in Corporate network.

```
configure
   context <dest_ctxt_name>
      aaa group <aaa_grp_name>
         radius ip vrf <vrf_name>
         radius attribute nas-ip-address address <nas_address>
nexthop-forwarding-address <ip_address> mpls-label input <in_mpls_label_value>
output < <out_mpls_label_value1>
         radius server <ip_address> encrypted key <encrypt_string> port <iport_num>

         end
```

Notes:

- *aaa_grp_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.
- Optional keyword **nexthop-forwarding-address** <*ip_address*> **mpls-label input** <*in_mpls_label_value*> **output <** <*out_mpls_label_value1*> associates AAA group for MPLS traffic.

Configuring BGP/MPLS VPN with Dynamic Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with dynamic MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.

Important The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

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 BGP/MPLS VPN:

Procedure

Step 1 Create a VRF on the router and assign a VRF name, define the Route-Distinguisher first before you execute the Route Target. For more information on the configuration see the Create VRF with Route-distinguisher and Route-target, on page 973 section.

Step 2 Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in Set Neighbors and Enable VPNv4 Route Exchange, on page 977.

Step 3 Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in Configure Address Family and Redistributed Connected Routes, on page 977. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.

Step 4 Configure IP Pools with dynamic MPLS labels by applying the example configuration in Configure IP Pools with MPLS Labels, on page 977.

Step 5 *Optional*. Bind DHCP service to work with dynamic MPLS labels in corporate networks by applying the example configuration in Bind DHCP Service for Corporate Servers, on page 977.

Step 6 *Optional*. Bind AAA/RADIUS server group in corporate network to work with dynamic MPLS labels by applying the example configuration in Bind AAA Group for Corporate Servers, on page 978.

Step 7 *Optional*. Modify the configured IP VRF, which is configured to support basic MPLS functionality, for mapping between DSCP bit value and experimental (EXP) bit value in MPLS header for ingress and egress traffic by applying the example configuration in DSCP and EXP Bit Mapping, on page 978.

Step 8 Save your configuration as described in the *System Administration Guide*.

Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second **ip vrf** command creates the route-distinguisher and route-target.

```
configure
   context <context_name> -noconfirm
      ip vrf <vrf_name>
      router bgp <as_number>
         ip vrf <vrf_name>
            route-distinguisher {<as_value> | <ip_address>} <rt_value>
            route-target export {<as_value> | <ip_address>} <rt_value>
            route-target import {<as_value> | <ip_address>} <rt_value>
            end
```

Notes:

- If export and import route targets are the same, alternate command **route-target both** {*<as_value>* | *<ip_address>* } *<rt_value>* can be used in place of **route-target import** and **route-target export** commands.

Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

```
configure
   context <context_name>
      mpls bgp forwarding
      router bgp <as_number>
         neighbor <ip_address> remote-as <AS_num>
         address-family vpnv4
         neighbor <ip_address> activate
         neighbor <ip_address> send-community both
         exit
      interface <bind_intfc_name>
         ip address <ip_addr_mask_combo>
         end
```

Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```
configure
   context <context_name>
      router bgp <as_number>
         address-family ipv4 <type> vrf <vrf_name>
            redistribute connected
            end
```

Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with dynamic MPLS labels.

```
configure
   context <context_name> -noconfirm
      ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name>
      end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with dynamic MPLS labels in Corporate network.

```
configure
   context <dest_ctxt_name>
      interface <intfc_name> loopback
```

```
      ip vrf forwarding <vrf_name>
      ip address <bind_ip_address subnet_mask>
      exit
   dhcp-service <dhcp_svc_name>
      dhcp ip vrf <vrf_name>
      bind address <bind_ip_address>
      dhcp server <ip_address>
      end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.

Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with dynamic MPLS labels in Corporate network.

```
configure
   context <dest_ctxt_name>
      aaa group <aaa_grp_name>
         radius ip vrf <vrf_name>
         radius attribute nas-ip-address address <nas_address>
         radius server <ip_address> encrypted key <encrypt_string> port <iport_num>

         end
```

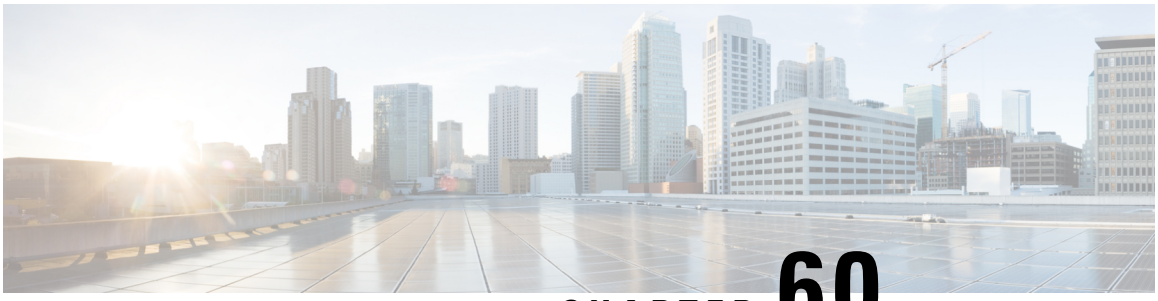
Notes:

- *aaa_grp_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.

DSCP and EXP Bit Mapping

Use this example to modify the configured IP VRF to support QoS mapping.

```
configure
   context <context_name>
      ip vrf <vrf_name>
         mpls map-dscp-to-exp dscp <dscp_bit_value> exp <exp_bit_value>
         mpls map-exp-to-dscp exp <exp_bit_value> dscp <dscp_bit_value>
         end
```



CHAPTER 60

Multiple Customized PCO Support

- Feature Summary and Revision History, on page 979
- Feature Description, on page 980
- How it Works, on page 980
- Configuring PCO, on page 981
- Monitoring and Troubleshooting, on page 983

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Support is added for additional Protocol Configuration Options, Custom6 through Custom10.	21.26

Revision Details	Release
Support is added to display a confirmation message before deleting or modifying an existing Container ID value in the Global Configuration mode.	21.24
Enhanced Protocol Configutaion Options (ePCO) support is added with the existing new operator defined PCO for UWB Indicator.	21.20.22
First introduced.	21.20.16

Feature Description

With the multiple PCO support feature, P-GW and GGSN sends customized Protocol Container Options (PCOs) to MS GTP messages. Custom1 is an existing PCO and its Container ID value is FF00H.

P-GW and GGSN support PCOs ranging from Custom1 through Custom10.

The global PCO container IDs are modified during runtime. This modification affects only the new subscriber sessions and doesn't affect the existing subscriber sessions. The PCO container IDs ranging from FF03 to FFFF are configurable.

Operator Defined PCO for Ultra Wideband (UWB) Indicator

P-GW supports either Protocol Configuration Options (PCO) or Enhanced Protocol Configuration Options (ePCO) based on the EPCOSI indication bit received from an UE in Create Session Request and Modify Bearer Request.

If the EPCOSI bit is set, P-GW sends PCO containers in the ePCO IE. If the EPCOSI bit isn't set, then P-GW sends PCO containers in PCO IE.

Note 3G (UMTS) PCO notification to the UE is added to support the Gn or Gp mode. GGSN doesn't support ePCO IE.

How it Works

This section describes the updation of PCO values using the Gx and Gy interfaces. The term Gateway (GW) is interchangeably used in this chapter for P-GW and GGSN.

Updating PCO Value Using Gx Interface

This section describes the procedure to update PCO values using the Gx interface.

- The Policy and Charging Rules Function (PCRF) sends a request to activate the predefined rules.
- If the activation is successful and if the charging action is configured for PCO, then the retrieved value is sent to the UE.

- If the predefined rule creation is performed during session creation (CCA), then the retrieved PCO is sent to the UE in Create Session Response for P-GW and Create PDP Context Response for GGSN.
- If the predefined rule activation is sent in the middle of the session (CCA-U), then the retrieved PCO is sent to the UE with the next message.
- The PCRF sends a request to deactivate predefined rules.
- If the removal of predefined rules is successful and if PCO is configured for charging action, then the configured value in the APN is returned to UE with the next message.
- If multiple predefined rules are enabled, then the last charging action configured for PCO, in the order of rules sent, is considered as valid and Session Manager is updated with the value.



Note Ensure that the last predefined rule has the correct PCO value for this scenario. The remaining requested rules will follow the regular predefined rule activation procedure.

Updating PCO Value Using Gy Interface

This section describes the procedure to update PCO values using the Gy interface.

- The Online Charging System (OCS) sends a filter ID to enable the corresponding post-processing dynamic rule.
- If the rule activation is successful and if the associated charging action is configured for PCO, then the retrieved value is sent to the Session Manager through the Session Update Indication event.
- The GW sends the PCO value to UE.
- If the OCS sends multiple filter IDs, then the charging action associated with the last filter ID is used for PCO.
- The CRF sends a request to deactivate the predefined rules.
- On successful removal of the predefined rules, if charging action is configured for PCO, then a default PCO value under APN will be returned to UE with the next message.

Configuring PCO

This section describes the PCO configuration. CLI modifications are not permitted when calls are active for APN Configuration mode and Global Configuration mode, but modifications are permitted for active-charging service.

Configuring PCO in Charging Action Mode

Use the following sample configuration to configure multiple PCOs in the ACS Charging Action Configuration Mode.

```
configure
  active-charging service service_name
```

```
      charging-action action_name
         { pco-custom1 | pco-custom2 | pco-custom3 | pco-custom4 |
pco-custom5 | pco-custom6 | pco-custom7 | pco-custom8 | pco-custom9 |
pco-custom10 } custom_value
         end
```

NOTES:

- **pco-custom1 - pco-custom10** *custom_value*: Configures multiple operator-specific PCOs. custom_value must be an integer in the range of 0-255.

Configuring Custom1 PCO in APN Configuration Mode

Use the following sample configuration to configure Custom1 PCO in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-option custom1 [ ue-requested ]
         end
```

NOTES:

- **pco-option custom1**: Configures operator defined PCO container custom1 mode. By default, its container ID value is fixed to 0.
- **ue-requested**: Configures to include Custom PCO Options in PCO IE, only when it requested by UE.
- **no**: Removes custom1 PCO configuration in the APN Configuration mode.

Configuring Multiple PCOs in APN Configuration Mode

Use the following sample configuration to configure multiple PCOs in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-options { { custom1 | custom2 | custom3 | custom4 |
custom5 | custom6 | custom7 | custom8 | custom9 | custom10 } [ ue-requested
 value custom_value | value custom_value ] }
         end
```

NOTES:

- **custom1 - custom10**: Configures APN to include custom PCO options in PCO IE.
- **ue-requested**: Configures to include custom PCO Options in PCO IE, only when it is requested by UE.
- **value** *custom_value* : Configures the default container value of custom PCO. custom_value must be an integer in the range of 0-255.
- **no**: Removes PCO configuration in the APN Configuration mode.

Configuring PCO Container ID in Global Configuration Mode

Use the following sample configuration to configure multiple PCOs in the Global Configuration mode.

```
configure
  [ no ] pco-options { custom2 | custom3 | custom4 | custom5 | custom6 |
 custom7 | custom8 | custom9 | custom10 } container-id container_id_value
  end
```

NOTES:

- **pco-options { custom2 - custom10}**: Configures custom PCO options in PCO IE.
- **container-id** *container_id_value*: Configures the operator defined container ID and the value ranging from FF03 to FFFF.
- **no**: Removes PCO container ID configuration in the Global Configuration mode.

Note The custom1 container ID is not configurable in the Global Configuration mode as its container value is fixed to FF00H.

Note If you delete or modify an existing container ID value for an ongoing session, it affects only the new sessions and does not affect the ongoing or existing sessions.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging charging-action all

The output of this command is enhanced to display the following field.

Table 96: show active-charging charging-action all Command Output Descriptions

Field	Description
PCO-Custom1-10 value	Indicates the action value for multiple operator-specific PCOs. The value can range from 1 to 10.

show active-charging sessions full all

The output of this command is enhanced to display the following fields.

Table 97: show active-charging sessions full all Command Output Descriptions

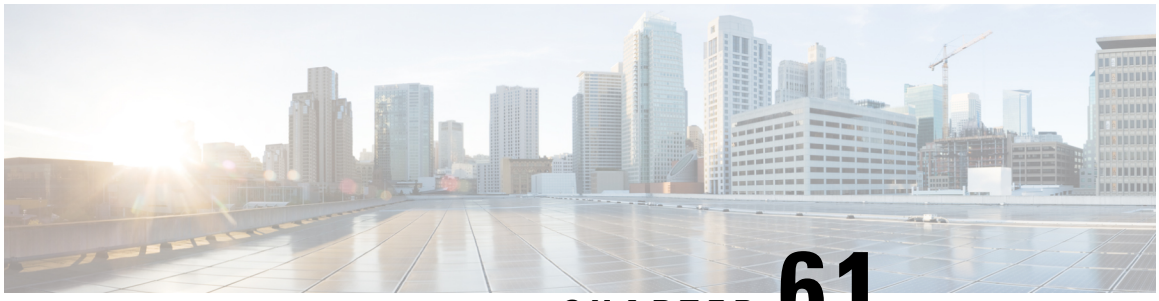
Field	Description
custom	Indicates Operator specific custom option.
Value	Indicates the value used for sending in custom PCO container.
Interface	Indicates the interface such as Gx. Gy or n/a based on the following conditions: • Gx: The charging rule is applied from the Gx interface that has custom PCO value. • Gy: The charging rule is applied from the Gy interface that has custom pco value. • n/a: The configured PCO value which is applied from APN profile.

show apn all

The output of this command is enhanced to display the following fields.

Table 98: show apn all Command Output Descriptions

Field	Description
Custom1-10 value	Specifies the action value for multiple operator-specific PCOs. The value can range from 1 to 10.
UE-Requested	Specifies PCO to the UE, which requested for new PCO option.



CHAPTER 61

Multiple IP Versions Support

This chapter describes the following topics:

- Feature Summary and Revision History, on page 985
- Feature Description, on page 986
- How it Works, on page 986
- Configuring Multiple IP Version Support, on page 988
- Monitoring and Troubleshooting, on page 989

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide*

Revision History



Important Revision history details are not provided for features introduced before release 21.2 and N5.1.

Revision Details	Release
This feature enables P-GW, S-GW, and SAEGW nodes to support the control messages received on all the transport addresses exchanged during the session setup.	21.8
First introduced.	Pre 21.2

Feature Description

This feature enables P-GW, S-GW, and SAEGW nodes to support the control messages received on all the transport addresses exchanged during the session setup.

A new CLI command has been introduced at the egtp-service level to control the behavior of the BRCmd, MBCmd, and DBCmd messages.

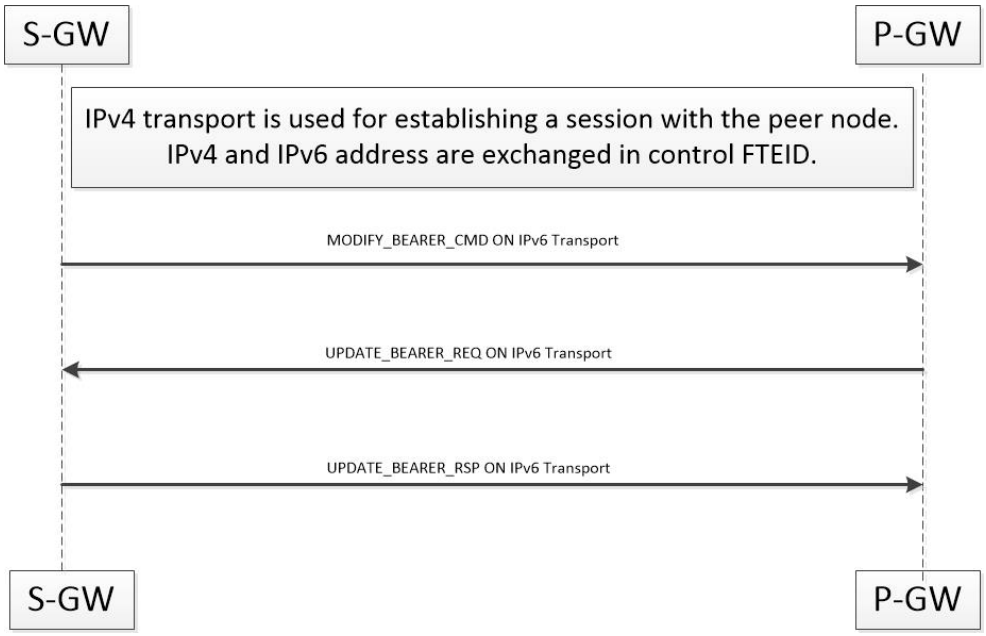
How it Works

This section describes the working of this feature. Following is the sample call flow for MBCmd.

The following figure illustrates call flow when the feature is disabled:



The following figure illustrates the call flow when feature is enabled:



When a session is being established, P-GW, S-GW, and SAEGW node uses the IPv6 address as transport. This transport is used for establishing tunnel with peer node. If IPv4 and IPv6 addresses are exchanged in control FTEID then the node should handle MBCmd, BRCmd, and DBCmd messages on IPv4 transport by the nodes.

When a session is being established, if IPv4 address is used as a transport and is being used for establishing tunnel with peer node, and if IPv4 and IPv6 addresses are exchanged in control FTEID, then the MBCmd, BRCmd, and DBCmd messages are also handled on the IPv6 transport by the nodes.

When a session is being established, if IPv4 and IPv6 addresses are exchanged in data F-TEID by both peers, then the GTP-U data packets get handled on both IPv6 and IPv4 transport.

When a session is being established, if IPv4 address is used as a transport, however, C-TEID does not contain IPv4 address, then that message is rejected by the node. The nodes exhibit similar behavior for IPv6 addresses.

When a session is being established, if IPv4 and IPv6 addresses are exchanged in data F-TEID by both peers, then GTP-U data packets get handled on IPv6 and IPV4 transport both.

The following table displays the message handling behavior in different session establishment scenarios:

Table 99: Message Handling Behavior in Different Session Establishment Scenarios

Messages	Transport Used for Session Establishment	C-FTEID Sent During Session Establishment	Message Sent on Transport
MBR/DSR	IPv6	IPv4/IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv4/IPv6	IPv4
Change Notification	IPv6	IPv4/IPv6	IPv4
Suspend/Resume	IPv6	IPv4/IPv6	IPv4
MBR/DSR	IPv4	IPv4/IPv6	IPv6
MBC/DBC/BRC	IPv4	IPv4/IPv6	IPv6
Change Notification	IPv4	IPv4/IPv6	IPv6
Suspend/Resume	IPv4	IPv4/IPv6	IPv6
MBR/DSR	IPv6	IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv6	IPv4
Change Notification	IPv6	IPv6	IPv4
Suspend/Resume	IPv6	IPv6	IPv4
MBR/DSR	IPv4	IPv4	IPv6
MBC/DBC/BRC	IPv4	IPv4	IPv6
Change Notification	IPv4	IPv4	IPv6
Suspend/Resume	IPv4	IPv4	IPv6

Configuring Multiple IP Version Support

This section provides information on CLI commands available in support of this feature.

By default, this feature is enabled.

```
configure
  context context_name
    egtp-service service_name
      [no] gtpc command-messages dual-ip-stack-support
      end
```

NOTES:

- **no**: Disables the feature.
- **command-messages**: Configures MBC or DBC or BRC messages on S-GW and P-GW.
- **dual-ip-stack-support**: Enables P-GW, S-GW, SAEGW nodes to handle command messages on both IPv4/IPv6 transport, if supported.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the Override Control Enhancement feature.

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the Override Control Enhancement feature.

show configuration

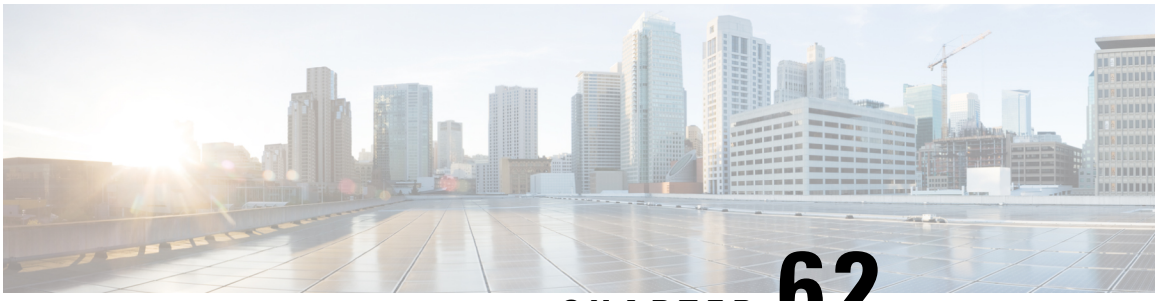
The following new fields are added to the output of this command:

- gtpc command-messages dual-ip-stack-support - Specifies the command messages on both IPv4/IPv6 transport if supported.

show egtp-service all

The following new fields are added to the output of this command:

- GTPC Command Messages Dual IP Support - Specifies the command messages on both IPv4/IPv6 transport if supported.



CHAPTER 62

NetLoc for WiFi EPC

This chapter describes StarOS support for the NetLoc for WiFi EPC feature on the P-GW and SAE-GW.

- Feature Description, on page 991
- How It Works, on page 991
- Configuring the NetLoc for WiFi EPC Feature, on page 993
- Monitoring and Troubleshooting the NetLoc for WiFi EPC Feature, on page 995

Feature Description

With this feature, the IMS network can retrieve location information of the UE from WLAN access network. This improves location related feature and functionality for the operator. This feature also helps in charging subscribers based on location information.

Please note that the support for LTE NetLoc already exists from prior releases. With this release, NetLoc support is extended for WLAN access. Basic implementation is already supported for passing necessary parameter to different internal modules like SM, IMSA and ECS.

How It Works

When the Application Function (AF) requests the PCRF to report the access network information, the PCRF provides the requested access network information indication (for example, user location and/or user timezone information) to the PCEF within the Required-Access-Info AVP which is included in the Charging-Rule-Definition AVP of an appropriate PCC rule.

The PCRF also provides the ACCESS_NETWORK_INFO_REPORT event trigger within the Event-Trigger AVP. If the ACCESS_NETWORK_INFO_REPORT event trigger is set, upon installation, modification and removal of any PCC rule(s) containing the Required-Access-Info AVP, the P-GW determines if it can obtain the required location information for the used IP CAN type.

During bearer deactivation or UE detach procedure, the P-GW provides the access network information to the PCRF within the TWAN-Identifier AVP. The P-GW also provides information on when the UE was last known to be in that location within the User-Location-Info-Time AVP, and/or UE-Local-IP-Address AVP as applicable for S2a/S2b interface:

- For Trusted WLAN, the User Location Information (ULI) is provided in the TWAN Identifier AVP.

- For Untrusted WLAN, the ULI contains the TWAN Identifier, the UE's Local IP address and optionally, UDP source port number (if NAT is detected).

When the ULI is requested by the PCRF and it's not provided to the PCEF, the PCEF provides the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP. And when the time zone is requested by the PCRF, the PCEF provides it within the 3GPP-MS-TimeZone AVP. Please note that the timezone is applicable only for Trusted WLAN interface. For WLAN access, the PCEF also includes the AN-Trusted AVP while reporting access network information.

During the IP-CAN session termination procedure, the PCEF will, if ACCESS_NETWORK_INFO_REPORT event trigger is set, provide the access network information to the PCRF by including the ULI (if it was provided to the PCEF), the information on when the UE was last known to be in that location within User-Location-Info-Time AVP (if it was provided to the PCEF), the PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP (if the user location information was not provided to the PCEF) and the timezone information within the 3GPP-MS-TimeZone AVP.

The WLAN location information received from S2a/S2b interface is reported on all the P-GW supported interfaces (Gx, Gy, and Gz).

Accounting Requirements

As part of accounting requirements, the following Dictionaries are used:

- Gx: r8-gx-standard
- Gy:
  - S2a: custom-8 with Rel-11
  - S2b: custom-8 with Rel-13
- Gx:
  - S2a: custom-48 and custom-52
  - S2b: custom-52

The following fields in PGW-CDRs are introduced as part of Gz requirement:

- custom-52 dictionary (as part of uWANUserLocationInfo):
  - uELocalIPAddress
  - uDPSourcePort
  - sSID
  - bSSID

The custom-52 is a new standard dictionary introduced in compliance with 3GPP Release 13.

Limitations

This section identifies the known limitations/restrictions of this feature.

- The User Location Information (ULI) on S2b includes UE local IP address and optionally, UDP source port number (if NAT is detected). It also includes WLAN Location Information (and its age). Location change is considered if any of the following information changes: UE local IP address, UDP port, or WLAN Location.
- On Gz, for WLAN location change, the ULI change trigger is used.
- On Gy, for WLAN location change, the location_any trigger is used.
- The Rf and S2a RADIUS, and LI interfaces are not considered as part of this feature.
- There are no changes done over S6b interface.
- Only SSID and BSSID of TWAN/UWAN Identifier are considered as part of this feature.
- UE local IP address field is mandatory on Gz and Gy as part of UWANUserLocationInfo.
- For S2b, when the received UWANUserLocationInfo is different than the previous UWANUserLocationInfo, then below are few error case handling:
  - For Gy, if the received parameters doesn't contain IP Address, the P-GW doesn’t generate a ULI-Change report.
  - For Gz, the container with 'ULI change' is closed only when the UWANUserLocationInfo value corresponding to the container contains the IP-Address.
- This feature is controlled by NetLoc and Wifi Integration License.
- In case of S2b interface, UE Local IP Address and Port, WLAN ID and WLAN Timestamp are reset to 0 if they are not received in CSReq/CBRsp/UBRsp/DBRsp.
- As per 3GPP TS 32.298, TWAN Identifier is present at Record level in Gz.
- The WLAN-timestamp is not sent over Gy and Gz interface.
- The UE-location-IP-Address change event trigger is not part of this feature.
- The EPC_Routed Feature (Reference 3GPP TS 29.212) is not supported.

Configuring the NetLoc for WiFi EPC Feature

The following sections provide the configuration commands to enable the feature.

Configuring the NetLoc TWAN for Gx

The commands illustrated below configures the NetLoc trusted WLAN feature over Gx interface.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features netloc-trusted-wlan
        end
```

Notes:

- **no diameter encode-supported-features**: Disables the feature.
- This command takes effect when Gx is enabled on S2b call.
- By default, the feature is disabled and TWAN information will not be sent over Gx.

Configuring the NetLoc UWAN for Gx

The commands illustrated below configures the NetLoc untrusted WLAN feature over Gx interface.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features netloc-untrusted-wlan
        end
```

Notes:

- **no diameter encode-supported-features**: Disables the feature.
- This command takes effect when Gx is enabled on S2b call.
- By default, the feature is disabled and UWAN information will not be sent over Gx.

Configuring the NetLoc UWAN for Gy

The commands illustrated below configures dictionary control of the AVPs that need to be added based on 3GPP Rel.13.

```
active-charging service service_name
  credit-control
    diameter update-dictionary-avps 3gpp-rel13
    end
```

Notes:

- **no diameter update-dictionary-avps**: Disables the feature.
- This command takes effect when Gy is enabled on S2b call.
- By default, the feature is disabled and UWAN information will not be sent over Gy.

Configuring the NetLoc UWAN for Gz

The commands illustrated below configures the NetLoc untrusted WLAN feature over Gz interface.

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute uwanuli
      end
```

Notes:

- **no gtpp attribute uwanuli**: Disables the feature.
- This command takes effect when Gz is enabled on S2b call.
- By default, the feature is disabled and UWAN information will not be sent over Gz.

Monitoring and Troubleshooting the NetLoc for WiFi EPC Feature

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

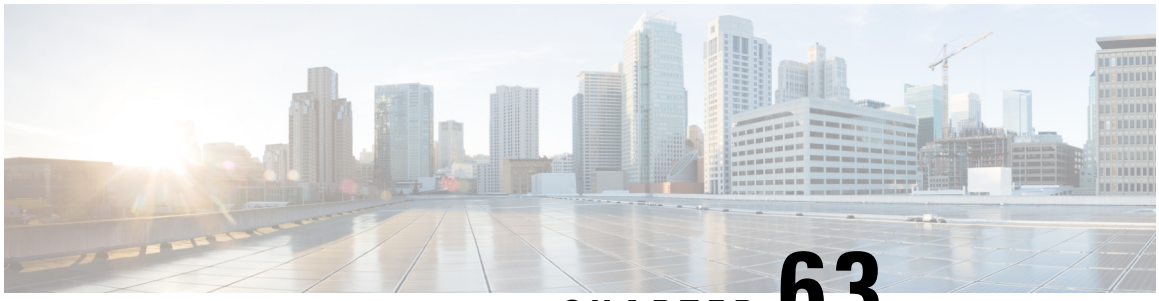
Show Commands and/or Outputs

The following table lists the CLI commands that will help to monitor and/or troubleshoot this feature.

CLI Commands	Description

show subscribers pgw-only full all
show subscriber saegw-only full all
	Displays the following newly introduced fields for which the values will be populated on S2a/S2b calls:
	`TWAN User Location Information:`
	`SSID:`
	`BSSID:`
	`UWAN User Location Information:`
	`UE Local IP Address:`
	`UDP Port:`
	`SSID:`
	`BSSID:`

show ims-authorization service all verbose	Displays the following newly introduced fields for which the values will be populated when they are configured as Supported Features AVP in IMS Authorization Service Configuration mode: • **netloc-trusted-wlan** • **netloc-untrusted-wlan**
show gtpp group all	Displays the following newly introduced field for which the value will be populated when the **gtpp attribute uwanuli** CLI command is configured in the GTPP Server Group configuration mode: • **UWAN User Location Information present:**



CHAPTER 63

Network Mobility (NEMO)

This chapter describes the system's support for 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 *Cisco ASR 5500 Packet Data Network Gateway Administration Guide*, before using the procedures in this chapter.

- NEMO Overview, on page 997
- NEMO Configuration, on page 1004

NEMO Overview

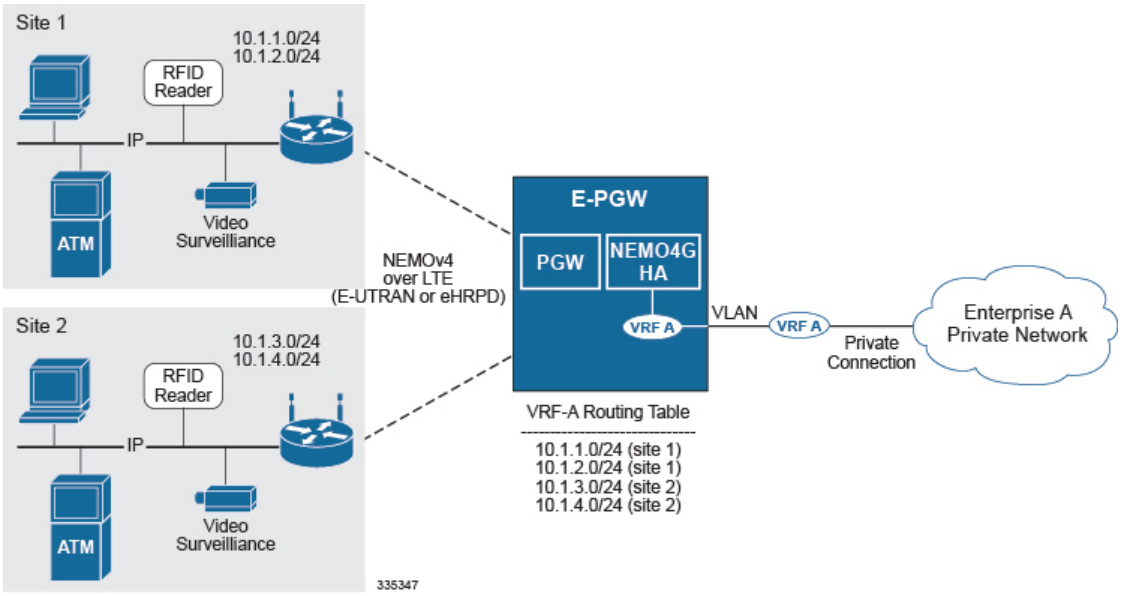
When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on 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).

Multiple HA service configuration is required when a mobile network is multihomed, that is when there is more than one point of attachment between the mobile network and internet.

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

Figure 97: NEMO Overview



Use Cases

The following use cases are supported by NEMO in LTE:

1. **Stationary** - Applications, like branch offices, with a mobile router that does not require mobility.
2. **Nomadic** - Applications that use a mobile router that does not move while in service, but that may be moved to a different location and brought back on service (e.g. a kiosk showing up in a mall one day and in a different location the next day or month).
3. **Moveable** - Applications that need to maintain Dynamic Mobile Network Routing (DMNR) service operational while moving and crossing PDSN boundaries, such as public safety vehicles. Service continuity is handled by the mobility protocols (Mobile IP in 3G and GTP in LTE).

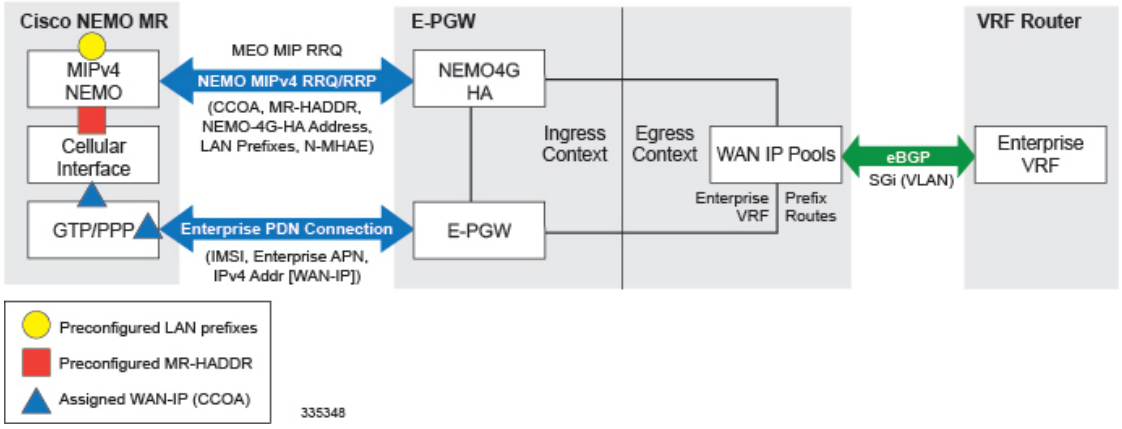
Features and Benefits

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 98: 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).

- 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 eight prefixes per mobile router. Anything beyond eight prefixes shall be silently discarded.
  - NEMO4G-HA supports any prefix length (including /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). E-PGW 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 eight). E-PGW 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 supports private and overlapping IP addressing across multiple Enterprises for the WAN IP pools, MR-HADDR, and LAN prefixes.

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 via either local configuration (APN parameter) or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter is supported to enable NEMO permission at the APN/PDN level within the P-GW service.

MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client.

NEMO4G-HA processes the first of three Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The three Cisco-specific NVSEs are placed after the MIPv4 "Identification" field and before the mandatory MIPv4 "Mobile-Home-Authentication-Extension." NEMO4G-HA accepts the LAN prefixes (up to eight) encoded in the first Cisco-specific NVSE (vendor-type = 9). NEMO4G-HA is not expected to process the other two Cisco-specific NVSEs with vendor-type = 49, which carry the Internal Interface ID of the MR's Roaming Interface and the MR's Roaming Interface Bandwidth in Kbps, respectively.

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 E-PGW.

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 E-PGW 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 eHRPD or LTE access.

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 E-PGW).
- 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 E-PGW 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 both 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 E-PGW 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.

Forced Fragmentation

E-PGW forces IP packet fragmentation even for IP packets with the DF-bit set.

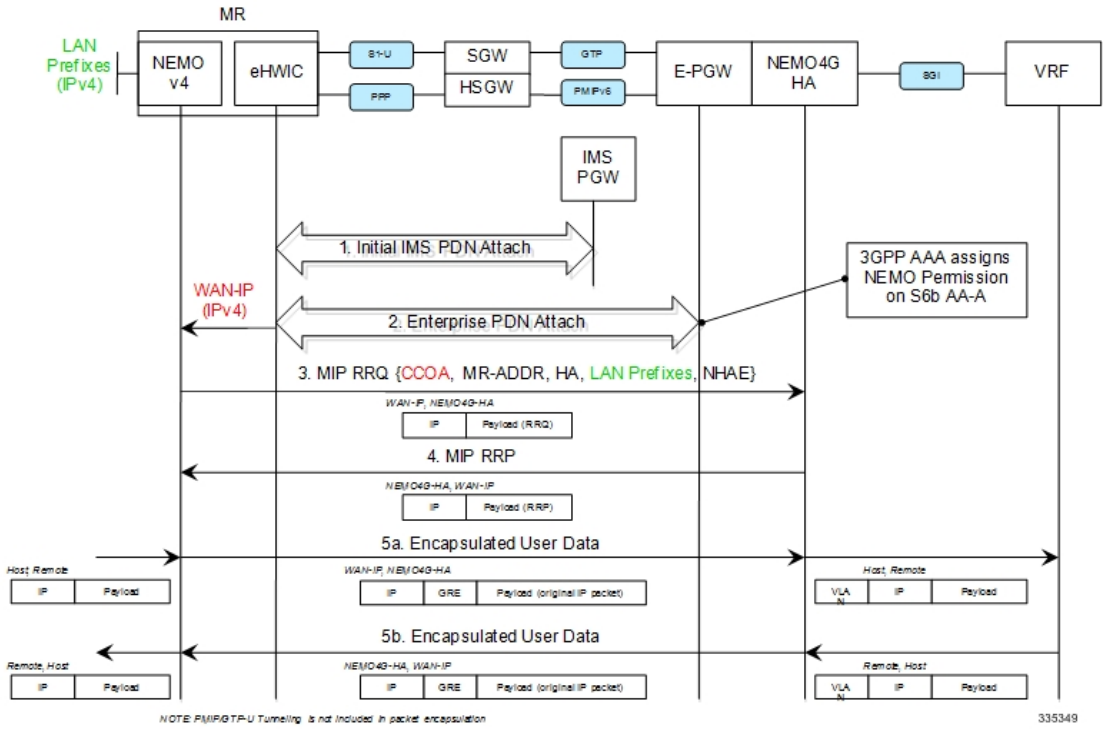
Redundancy/Reliability

The LTE NEMO solution supports intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.

LTE NEMO Call Flow

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

Figure 99: 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 E-PGW to allow NEMO service at the PDN/Enterprise level.
   - E-PGW assigns the MR eHWIC an IPv4 address from the Enterprise IPv4 pool assigned during PDN authentication.
   - E-PGW creates the proper flows internally to forward packets to the corresponding VRF external to the E-PGW 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 will 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:

- 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.
     - 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 8 prefixes. Anything beyond 8 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. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table to route all traffic through the LTE connection.
   - 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.

Engineering Rules

- Up to 5,000 host routes spread across multiple VRFs per BGP process. Limited to 6,000 pool routes per chassis.
- Up to 2,048 VRFs per chassis.

Supported Standards

- IETF RFC 3025 (February 2001) "Mobile IP Vendor/Organization Specific Extensions"
- IETF RFC 1191 (November 1990) "Path MTU Discovery"

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-ID by applying the example configuration in Create a VRF.
2. Set the neighbors and address family to exchange routing information with a peer router by applying the example configuration in Set Neighbors and Address Family, on page 1006.
3. Redistribute connected routes between routing domains by applying the example configuration in Redistribute Connected Routes, on page 1006.
4. Allow the P-GW to use the NEMO service by applying the example in Configure and Enable NEMO in APN Profile, on page 1006.
5. Create a NEMO HA by applying the example in Create a NEMO HA, on page 1007.
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*.

Sample Configuration

```
configure
  context <egress_context_name>
  interface <interface_name_outbound>
    ip address <ipv4_address> <ipv4_mask>
    exit
  ip vrf <vrf_name>
  ip vrf-list first-list permit vrf <vrf_name>
  mpls bgp forwarding
  ip pool <pool_name> <pool_address> private vrf <vrf_name>
  nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>
  router bgp <as_number>
    neighbor <ip_address> remote-as <as_number>
    timers bgp keepalive-interval <seconds> holdtime-interval <seconds>
    address-family <type>
      redistribute connected
    #exit
    address-family <type>
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
    #exit
    ip vrf <vrf_name>
      route-distinguisher <asn_value> <rd_value>
      route-target both <asn_value> <rt_value>
    #exit
    address-family address-family ipv4 vrf <vrf_name>
      redistribute connected
    #exit
  #exit
  apn <apn_name>
    permission nemo
    ip context-name <egress_context_name>
    ip address pool name <pool_name>
    exit
  exit
  context <inress_context_name>
    interface <interface_name_inbound>
      ip address <ipv4_address> <ipv4_mask>
      exit
    ha-service <ha_service_name>
      mn-ha-spi spi-number <spi_number> encrypted secret <enc_secret>
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address <ip_address>
      end
```

Refer *Command Line Interface Reference* for detail information about the CLIs and keywords/variables.

Create a VRF

Use this example to first create a VRF on the router and assign a VRF-ID.

```
configure
   context <context_name> -noconfirm
      ip vrf <vrf_name>
      ip pool <pool_name> <pool_address> private vrf <vrf_name>
      nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>
      end
```

Set Neighbors and Address Family

Use this example to set the neighbors and address family to exchange routing information with a peer router.

```
configure
   context <context_name>
      ip vrf <vrf_name>
         router bgp <as_number>
         ip vrf <vrf_name>
            neighbor <ip_address> remote-as <AS_num>
            address-family <type>
            neighbor <ip_address> activate
            end
```

Redistribute Connected Routes

Use this example to redistribute connected routes between routing domains.

```
configure
   context <context_name>
      ip vrf <vrf_name>
         router bgp <as_number>
         ip vrf <vrf_name>
            address-family <type> vrf <vrf_name>
               redistribute connected
               end
```

Configure and Enable NEMO in APN Profile

Use this example to configure and enable NEMO in an APN profile.

```
configure
   context <context_name>
      apn <apn_name>
         permission nemo
         ip context-name <name>
         ip address pool name <pool_name>
         end
```

Create a NEMO HA

Use this example to create a NEMO HA.

```
configure
  context <context_name>
    ha-service <ha_service_name>
      mn-ha-spi spi-number <number> encrypted secret <enc_secret>
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address <ip_address>
      end
```

Monitoring and Troubleshooting

This section provides information on CLI commands that are available for monitoring and troubleshooting of Network Mobility.

Monitor Protocol

When using the monitor protocol command, enable option 26 to see all NEMO messages.

Show Commands and/or Outputs

This section provides information about show CLI commands that are available in support of Network Mobility.

- **show ha-service all**: Use this command to view the information about the configured HA service to make sure that the service starts along with all the key parameters of the CLI configured for this service.

Note Use the following show command CLIs from the context where IP VRF configuration is done, in the following case the CLIs are for context egress.

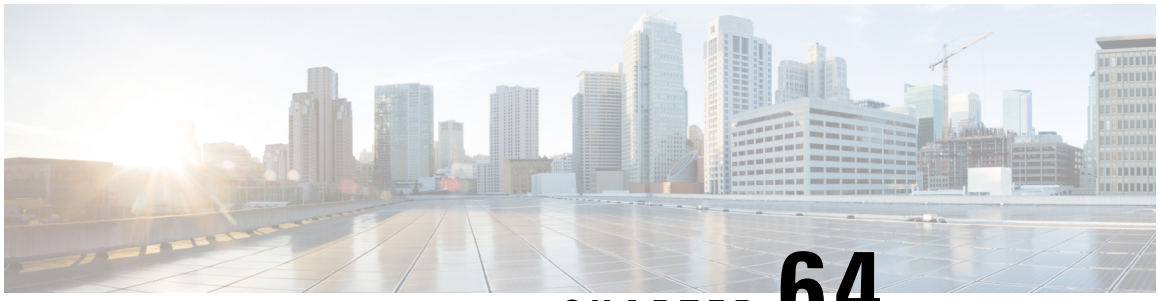
Use the following commands to view the information about the prefix and routes assigned as shown in the following output.

```
show ip bgp vpnv4 vrf <vrf-name>:
Network          Next Hop   Metric  LocPrf   Weight  Path
*> 15.1.1.0/32   0.0.0.0    0              32768  ?
*> 15.1.1.1/32   0.0.0.0    0              32768  ?
*> 15.1.1.2/32   0.0.0.0    0              32768  ?
*> 15.1.1.3/32   0.0.0.0    0              32768  ?
*> 15.1.1.4/32   0.0.0.0    0              32768  ?
*> 15.1.1.5/32   0.0.0.0    0              32768  ?
*> 15.1.1.6/32   0.0.0.0    0              32768  ?
*> 15.1.1.7/32   0.0.0.0    0              32768  ?
*> 80.240.0.0/20 0.0.0.0      0              32768  ?
*> 192.168.232.0/24 31.100.101.1    0        0     2000 ?
```

```
show ip route vrf <vrf-name>:
Destination   Nexthop  Protocol  Prec  Cost Interface
*15.1.1.0/32   0.0.0.0  connected   0        0
*15.1.1.1/32   0.0.0.0  connected   0        0
*15.1.1.2/32   0.0.0.0  connected   0        0
*15.1.1.3/32   0.0.0.0  connected   0        0
*15.1.1.4/32   0.0.0.0  connected   0        0
```

```
*15.1.1.5/32   0.0.0.0  connected   0        0
*15.1.1.6/32   0.0.0.0  connected   0        0
*15.1.1.7/32   0.0.0.0  connected   0        0
*80.240.0.0/20   0.0.0.0  connected   0       0 pool cust101-a
*192.168.232.0/24 31.100.101.1   bgp        20      0 19/1-sub101 (nhlfe-ix:8)
```

```
show mipha full all
MSID: -
Home Address: XX.XX.XX.XX  HA Address: XXX.XXX.XXX.X
Total Prefix: 16   Multi-VRF: NO
VRF #1: vrf-cust101   CtxtID: 0x43 GRE: 0x0
15.1.1.0/32    15.1.1.1/32
15.1.1.2/32    15.1.1.3/32
15.1.1.4/32    15.1.1.5/32
15.1.1.6/32    15.1.1.7/32
15.1.1.8/32    15.1.1.9/32
15.1.1.10/32    15.1.1.11/32
15.1.1.12/32    15.1.1.13/32
15.1.1.14/32    15.1.1.15/32
Send NAI Extension in Revocation Message: NO
Binding #1:  Care of Address: XX.XXX.X.XX
  FA Address/Port: XX.XXX.X.XX/XXX
  Lifetime: 00h01m15s   Remaining Life: 00h00m26s
  Reverse Tunneling: On   Encapsulation Type: Keyless-GRE
  GRE Key(Fwd): n/a   IPSec Required: No
  GRE Key(Rev): n/a
  IPSec Ctrl Tunnel Estab.:No  IPSec Data Tunnel Estab.: No
  Revocation Negotiated: NO  Rev I Bit Negotiated: NO
  Colocated COA: YES   NAT Detected: NO
  MN-HA-Key-Present: TRUE  MN-HA-SPI: 256
  FA-HA-Key-Present: FALSE  FA-HA-SPI: n/a
  HA-RK-KEY-Present: FALSE  HA-RK-SPI: n/a
  HA-RK-Lifetime: n/a   HA-RK-Remaining-Lifetime: n/a
```



CHAPTER 64

NEMO-LMA Heartbeat

- Feature Information, on page 1009
- Feature Description, on page 1010
- How It Works, on page 1010
- Configuring NEMO-LMA Heartbeat, on page 1010
- Monitoring and Troubleshooting the NEMO-LMA Heartbeat, on page 1011

Feature Information

Summary Data

Status	New Feature
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)	CSCuw08182
Related Changes in This Release	NEMO PMIPv6 Heartbeat on LMA (SAEGW)
Related Documentation	Command Line Interface 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

Path management mechanism through Heartbeat messages between the Mobile Router (MR) and Network Mobility-Local Mobility Anchor (NEMO-LMA) is important to know the availability of the peers, to detect failures, quickly inform peers if recovery from the node fails and allow a peer to take appropriate action.

How It Works

The MR and the LMA exchange Heartbeat messages at regular intervals to detect the status of availability between them. The NEMO-LMA initiates a Heartbeat exchange with the MR, by sending a Heartbeat Request message, to check if the MR is reachable. The NEMO-LMA records the sequence number of the last Heartbeat Request message and is used to match the corresponding Heartbeat Response. The NEMO-LMA responds to a Heartbeat Request message with a Heartbeat Response message, irrespective of whether there is PMIPv6 session with the corresponding peer.

Binding Error

When the Binding Error message, with status set to 2, is received in response to a Heartbeat Request message, the NEMO-LMA does not use Heartbeat messages further with the corresponding peer.

Failure Detection

When the LMA node does not receive the Heartbeat response for the configurable parameter **max-heartbeat-retransmission** <*value*> **exceed-action drop-session**, the NEMO-LMA concludes that the peer is not reachable. As such, the Heartbeat request to the peer is stopped and clears the NEMO-LMA session without any traps.

Restart Detection

If the restart counter value is different from the previous received value, then it assumes that the peer had crashed and recovered. And so, the existing NEMO-LMA sessions are cleared.

License Requirements

Use of NEMO requires that a valid license key be installed. Contact your Cisco account or Support representative for information on how to obtain a license.

Configuring NEMO-LMA Heartbeat

Use the following commands under LMA Service Configuration Mode to clear NEMO-LMA sessions without generating traps:

```
configure
   context context_name
      lma-service service_name
         heartbeat retransmission max number [ exceed-action drop-session ]
         end
```

Notes:

- **retransmission max**: The maximum number of heartbeat retransmissions allowed. The *number* must be an integer from 0 to 15. Default: 3
- **exceed-action**: Specifies the action to be taken after the maximum number of Heartbeat retransmissions is reached.
- **drop-session**: Used for dropping the session when path failure is detected.
- The **exceed-action** and **drop-session** keywords are valid only for NEMO-LMA sessions and takes effect if the Heartbeat feature is enabled.

Monitoring and Troubleshooting the NEMO-LMA Heartbeat

The following sections describe commands available to monitor and troubleshoot the feature.

monitor protocol

When using the **monitor protocol** command, enable option **48** to monitor the Heartbeat Request/Reply messages.

show lma-service statistics

Use this command to see the statistics related to Heartbeat messages. The output generated appears similar to the following:

```
Total Disconnects:          1
   Lifetime expiry:         0      Deregistrations:     0
      Admin Drops:          0      Path Failure Drops:  1
      Other Reasons:        0
```

show session disconnect-reasons

Use this command to see the call disconnected due to heartbeat path failure. The output generated appears similar to the following:

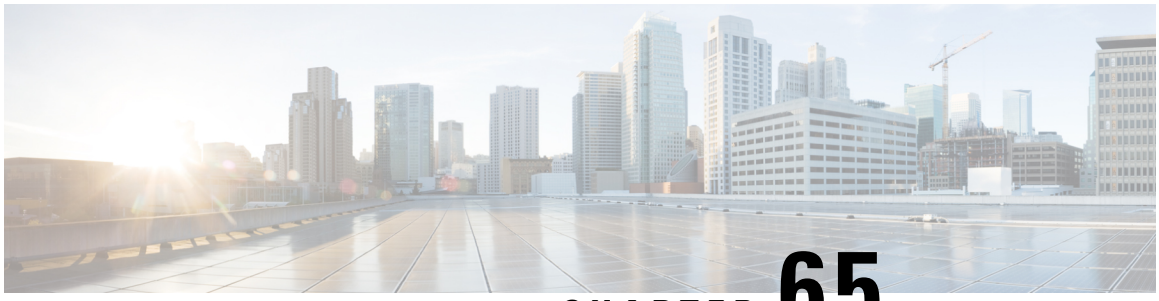
```
mme-guti_realloc_failed-detach(615)          0        0.00000
mme-pcscf-rest-detach(616)                   0        0.00000
Reject-ho-old-tun-path-failure(617)          0        0.00000
mip-path-failure(618)                        0        0.00000
```

Bulk Statistics

LMA Schema

The following new bulk statistics variable is added to the LMA schema in support of this feature:

- lma-pathfailsessionscleared – If any path failures/restarted counter value changes for the NEMO-LMA Heartbeat feature, the sessions disconnection counter is incremented.



CHAPTER 65

Network Service Headers (NSH)

This chapter describes the following topics:

- Feature Summary and Revision History, on page 1013
- Feature Description, on page 1014
- How It Works, on page 1014
- Configuring Support for NSH Framework, on page 1016
- Show Commands and Outputs, on page 1023

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
In this release, NSH-based Traffic Identification with Traffic Steering is supported.	21.9
First introduced.	21.4

Feature Description

Network Services Headers (NSH), a new service chaining protocol, is added to the network traffic in a packet header to create a dedicated service plane that is independent of the underlying transport protocol. In general, NSH describes a sequence of service nodes that a packet is routed through before reaching the destination address. The NSH includes meta-data information about the packet and service chain in an IP packet. The NSH protocol addresses the growing requirement to deploy various services functions external to the gateway.

This feature introduces NSH protocol support for P-GW and SAEGW products and supports the following:

- Encoding and decoding of NSH format in the P-GW/SAEGW.
- Configurable parameters to be included for encoding in the variable header.
- NSH treatment for selective traffic based on configuration.
- Configuring the tag values for parameters present in the variable header.
- Selective configuration of policies for acting on the decode parameters received in the NSH.
- Configuring the intelligence of encoding the NSH information in every packet of a flow or only once per flow.
- NSH-based Traffic Identification with Traffic Steering.



Important In this release, selective encryption of parameters is not supported.

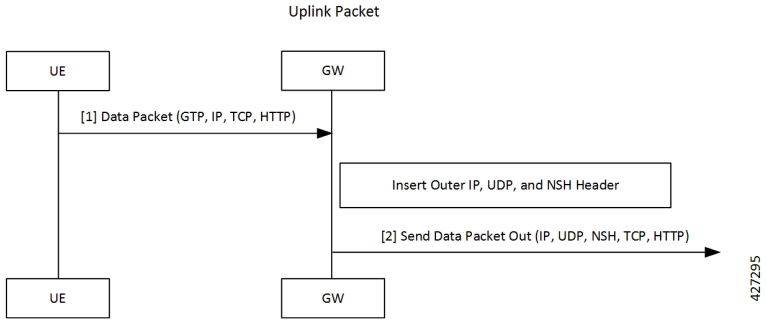
How It Works

This section describes the working of NSH protocol support in Cisco's P-GW/SAEGW products.

- **The Uplink Packet**

  For the uplink packet, P-GW/SAEGW adds the NSH, if the flow matches the specified criteria. NSH has a variable length context header also.

  Following call flow shows the NSH protocol support in the Cisco PGW/SAEGW products for an uplink packet.

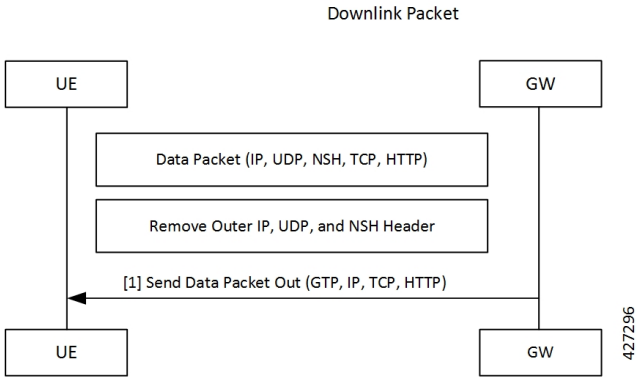


For an uplink packet, if the call flow matches the specified criteria, PGW or SAEGW adds the NSH header to the data packet. NSH header may have variable length context header, which can be encrypted if specified in the configuration.

- **The Downlink Packet**

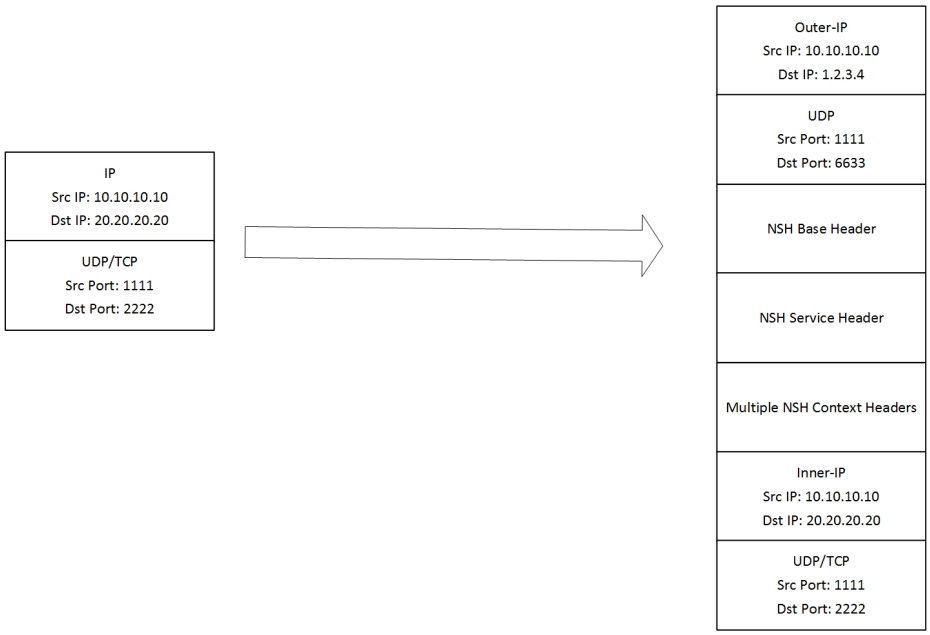
  For the downlink packet, P-GW/SAEGW processes and removes the NSH and applies policies based on the extracted NSH parameters.

  Following call flow shows the NSH protocol support in the Cisco PGW/SAEGW products for a downlink packet.



  For a downlink packet, PGW or SAEGW processes and removes NSH header. Then, PGW or SAEGW apply policies based on the extracted NSH parameters.

- Source and destination IP address for the outer IP packet is taken from the inner IP packet.
- By default, NSH encapsulated packets use the port number 6633.



Configuring Support for NSH Framework

This section covers configuration steps used in this feature for adding support for NSH framework.

Charging Action Association

Service chain is associated to charging action in the following way:

```
configure
  active-charging service service_name
    charging-action charging_action_name
      service-chain service_chain_name
      end
```

Notes:

- **charging-action**: Defines charging action.

  charging_action_name: Specifies name of the charging action. This is entered as an alphanumeric string of 1 through 64 characters.

- **service-chain**: Defines service chain association.

  service_chain_name: Specifies name of the service chain. This is entered as an alphanumeric string of 1 through 64 characters.

Service Chain Association

A new CLI command **nsh-format** is added to the **service-chain** command for service-chain association.

```
configure
   service-chain <service_chain_name>
      nsh-format <nsh_format_name>
      end
```

Notes:

- **service-chain**: Defines service chain association.

  service_chain_name: Specifies name of the service chain. This is entered as an alphanumeric string of 1 through 64 characters.

- **nsh-format**: Associates NSH format with the service chain.

Service Scheme Association

A new CLI command **nsh-response-received** has been added to the **trigger** command to the ACS service scheme configuration mode.

```
configure
  active-charging service service_name
     service-scheme service_scheme_name
        [ no ] trigger { bearer-creation | flow-create | loc-update |
nsh-response-received | sess-setup }
       end
```

Notes:

- **service-scheme**: Enables the association of service-scheme based on subscriber class.

  service_scheme_name: Specifies name of the service scheme. This is entered as an alphanumeric string of 1 through 64 characters.

- **no**: Disables the trigger action for the service-scheme.
- **trigger**: Specifies the trigger action for service-scheme.
- **bearer-creation**: Triggers for every new bearer.
- **flow-create**: Triggers for every new flow.
- **loc-update**: Triggers whenever location changes of the subscriber.
- **nsh-response-received**: Triggers on NSH response packet.
- **sess-setup**: Triggers at session setup.

NSH Configuration Mode

The Network Service Header (NSH) configuration mode is a sub-mode of the Global Configuration mode. This NSH mode is used to encode or decode NSH.

Exec > Global Configuration> Network Service Entity - IP Configuration

```
configure
   nsh
   end
```

Entering the above command sequence results in the following prompt:

[local]host_name(nsh)#

NSH Fields Configuration Mode

The NSH Fields configuration mode is a sub-mode of the NSH Configuration mode. This NSH Fields configuration mode is used to tag value to the NSH fields.

Exec > Global Configuration> Network Service Header > Network Service Header - Fields Configuration

```
configure
   nsh
     nsh-fields fields_name
     end
```

Entering the above command sequence results in the following prompt:

[local]host_name(nsh-nshfields)#

tag-value

This new CLI command is added to the NSH Fields Configuration mode to associate a tag value to a NSH field.

```
configure
  nsh
    nsh-fields fields_name
      tag-value tag_value { content-type | enterprise-id | imei | imsi |
msisdn | rating-group | rulebase | tdf-app-id }
      end
```

Notes:

- **nsh-fields**: Defines NSH fields tag values.

  fields_name: Specifies name of the *nsh-field*. This is entered as an alphanumeric string of 1 through 64 characters.

- **tag-value** Associates a tag to a field.

  tag_value : Tag value for the NSH field.

- **content-type**: Specifies content type of payload.
- **enterprise-id**: Specifies the enterprise-ID to be sent in NSH context header.
- **imei**: Specifies IMEI of the subscriber.
- **imsi**: Specifies IMSI of the subscriber.
- **msisdn**: Specifies MSISDN of the subscriber.

- **rating-group**: Specifies rating-group applied for the traffic.
- **rulebase**: Specifies rule-base of the subscribers.
- **tdf-app-id**: Specifies TDF Application ID applied to the traffic.

NSH Format Configuration Mode

The NSH Format Configuration mode is a sub-mode of the NSH Configuration mode. This NSH Format mode is used to encode or decode NSH.

Exec > Global Configuration> Network Service Header > Network Service Header - Format

```
configure
   nsh
     nsh-format format_name
     end
```

Entering the above command sequence results in the following prompt:

[local]host_name(nsh-nshformat)#

encode

This new CLI command is added to the NSH Format configuration mode. This command defines the NSH encoding fields to be associated with the NSH format.

```
configure
  nsh
    nsh-format format_name
       encode nsh-fields fields_name
       end
```

Notes:

- **nsh-format**: Defines format in NSH header.

  format_name: Specifies name of the *NSH format*. This is entered as an alphanumeric string of 1 through 64 characters.

- **encode**: Associates nsh-fields for encoding.
- **nsh-fields**: Defines nsh fields tag value.

  fields_name: Specifies name of the fields. This is entered as an alphanumeric string of 1 through 64 characters.

encoding-frequency

This command defines frequency of encoding the NSH fields to be associated with the NSH format.

```
configure
  nsh
    nsh-format format_name
```

```
encoding-frequency { always | once-per-flow }
end
```

Notes:

- **encoding-frequency**: Defines frequency of encoding nsh-fields.
- **always**: Encodes nsh fields on every hit.
- **once-per-flow**: Encodes nsh fields once per flow.

decode

This command defines the NSH decoding fields to be associated with the NSH format.

```
configure
  nsh
    nsh-format format_name
      decode nsh-fields fields_name
      end
```

Notes:

- **nsh-format**: Defines format in NSH header.

  format_name: Specifies name of the *NSH format*. This is entered as an alphanumeric string of 1 through 64 characters.

- **decode**: Associates nsh-fields for decoding.
- **nsh-fields**: Defines nsh fields tag value.

  fields_name: Specifies name of the fields. This is entered as an alphanumeric string of 1 through 64 characters.

Trigger Condition Configuration Mode Commands

content-type

This command specifies the content type to be matched.

```
configure
  active-charging service service_name
    trigger-condition trigger_condition_name
      content-type { operator condition }
      end
```

Notes:

- **trigger-condition**: Defines ACS trigger conditions.

  trigger_condition_name: Specifies name of the trigger condition. This is entered as an alphanumeric string of 1 through 64 characters.

- **content-type**: Specifies the content type.

- **operator** : Specifies how to match. Operator must be one of the following:
  - **!=**: not equals
  - **!contains**: not contains
  - **!ends-with**: not ends with
  - **!starts-with**: not starts with
  - =: equals
  - **contains**: contains
  - **ends-with**: ends with
  - **starts-with**: starts with
- **condition**: Specifies the condition to match. Condition must be one of the following:
  - FALSE
  - TRUE

tdf-app-id

This command specifies the identifier for application-based rules to be matched.

```
configure
  active-charging service service_name
     trigger-condition trigger_condition_name
        tdf-app-id { operator condition }
        end
```

Notes:

- **trigger-condition**: Defines ACS trigger conditions.

  trigger_condition_name: Specifies name of the trigger condition. This is entered as an alphanumeric string of 1 through 64 characters.
- **tdf-app-id**: Specifies the identifier for application based rules.
- **operator condition**: Specifies how to match. Operator must be one of the following:
  - **!=**: not equals
  - **!contains**: not contains
  - **!ends-with**: not ends with
  - **!starts-with**: not starts with
  - =: equals
  - **contains**: contains
  - **ends-with**: ends with

  - **starts-with**: starts with

- **condition**: Specifies the condition to match. Condition must be one of the following:
  - FALSE
  - TRUE

Sample Configuration for NSH Creation

The following is a sample configuration for this NSH service creation:

```
config
       nsh
         nsh-fields xyz
            tag-val 1 imei
            tag-val 2 imsi
         exit
          nsh-fields abc
            tag-val 4 content-type
         exit
         nsh-format format1
            encoding frequency always
            encode nsh-fields xyz
            decode nsh-fields abc
          exit
    exit
  traffic-steering
  appliance-group firewall
   nsh-format format1
   ip address 1.2.3.4
  #exit
 #exit
 service-chain sch1
  sfp direction uplink service-index 1 appliance firewall
 #exit
 exit
config
    active-charging service ACS
        trigger-action ta1
           throttle-suppress
        exit
        trigger-condition tc1
           content-type contains text
        exit
        service-scheme scheme1
            trigger nsh-response-received
                priority 1 trigger-condition tc1 trigger-action ta1
            exit
        exit
        subs-class class1
            any-match = TRUE
        exit
        subscriber-base base1
            priority 1 subs-class class1 bind service-scheme scheme1
        exit
       charging-action ca1
           service-chain xyz
       exit
```

```
    exit
exit
```

Show Commands and Outputs

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

show nsh statistics

This command has been newly added in this release to display the nsh statistics. Following is the output when you execute this command:

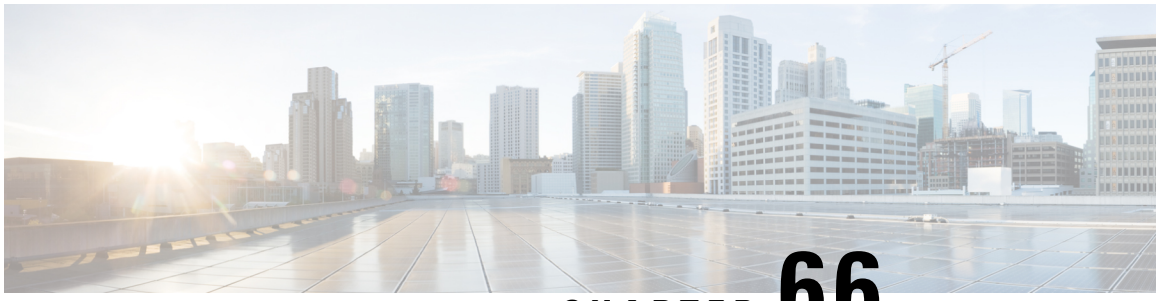
```
Total Encap Successful                :         0
Total Decap Successful                :         0

Total Encap Failed                    :         0
   Memory Allocation                  :         0
   Config Error                       :         0
   Encryption Failed                  :         0

Total Decap Failed                    :         0
   Config Error                       :         0
   Base Header
      Invalid Length                  :         0
      Unsupported Version             :         0
      Unsupported Next Protocol       :         0
      Next Protocol Mismatch          :         0
      Unsupported MD-Type             :         0
   Context Header
      Unsupported MD-Class            :         0
      Unsupported Type                :         0

OAM Packets
   Received                           :         0
   Dropped                            :         0

Unknown Context Header Type           :         0
```

show active-charging trigger-condition statistics

The output of this command includes the following field for this feature:

- NSH-Rsp-Rcvd

This field displays the matching of trigger condition based on NSH response.



CHAPTER 66

Overcharging Protection Support

This chapter describes the Overcharging Protection Support feature 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 *P-GW Administration Guide*, the *S-GW Administration Guide*, or the *SAEGW Administration Guide* before using the procedures in this chapter.

This chapter includes the following sections:

- Overcharging Protection Feature Overview, on page 1025
- License, on page 1026
- Configuring Overcharging Protection Feature, on page 1026
- Monitoring and Troubleshooting , on page 1028

Overcharging Protection Feature Overview

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.



Important This feature is supported on the P-GW, and S-GW. Overcharging Protection is supported on the SAEGW only if the SAEGW is configured for Pure P or Pure S functionality.

P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn't desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.

If the S-GW supports the Overcharging Protection feature, then it will send a CSReq with the PDN Pause Support Indication flag set to 1 in an Indication IE to the P-GW.

If the P-GW supports the Overcharging Protection feature then it will send a CSRsp with the PDN Pause Support Indication flag set to 1 in Indication IE and/or private extension IE to the S-GW.

Once the criterion to signal "stop charging" is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. The MBReq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume charging downlink packets when either of these conditions is met:

- When the S-GW (which had earlier sent "stop charging" in MBReq) sends "start charging" in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).

This feature aligns with the 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) specification.



Important When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

License

Overcharging Protection is a license enabled feature and a new license key has been introduced for Overcharging Protection for P-GW functionality.



Important Contact your Cisco account representative for information on how to obtain a license.

Configuring Overcharging Protection Feature

This section describes how to configure overcharging protection support on the P-GW and S-GW.

Configuring Overcharging Support on the P-GW

This command enables overcharge protection for APNs controlled by this APN profile and configures overcharging protection by temporarily not charging during loss of radio coverage. Each overcharging protection option is a standalone configuration and it does not override the previous option set, if any. Use this command to specify P-GW to pause charging on abnormal-s1-release, DDN failure notification, or if the number of packets or bytes dropped exceeds the configured limit.



Important This configuration sequence is valid for the P-GW only.

```
configure
   apn-profile apn_profile_name
```

```
      overcharge-protection { abnormal-s1-release | ddn-failure |
drop-limit drop_limit_value { packets | bytes } }
     [ remove ] overcharge-protection { abnormal-s1-release | ddn-failure
 | drop-limit }
      end
```

Notes:

- **remove:**

  Removes the specified configuration.

- **abnormal-s1-release:**

  (for future use) If overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if Abnormal Release of Radio Link signal occurs from MME.

- **ddn-failure:**

  If overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

- **drop-limit *drop_limit_value* { packets | bytes } }**

  Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.

  drop_limit_value is an integer from 1 through 99999.

  - **packets:** Configures drop-limit in packets.
  - **bytes:** Configures drop-limit in bytes.

Configuring Overcharging Support on the S-GW

The following configuration is required for overcharging support on the S-GW:

```
configure
   context context_name
      egtp-service service_name
         gtpc private-extension overcharge-protection
         end
```

Notes:

- Enabling this command indicates that the S-GW has to interact with a release 15 P-GW for the overcharging protection feature which does not support 3GPP TS 29.274 Release 12 – *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3*.
- When the **gtpc private-extension overcharge-protection** command is configured, the S-GW includes a Private Extension in the Create Session Request (CSReq) and Modify Bearer Request (MBReq) messages.
- Whenever a P-GW receives a CSReq with an Indication IE with the PDN Pause Support Indication flag set to 1, it responds only with an Indication IE.
- When a CSReq does not have an Indication IE with the PDN Pause Support Indication flag set to 1, but the P-GW supports Overcharging Protection, then it responds with both an Indication and Private Extension IE.

Monitoring and Troubleshooting

P-GW Schema

The following bulk statistics have been added to the P-GW schema for Overcharging Protection:

For descriptions of these variables, see the *Statistics and Counters Reference* guide.

- sessstat-ovrchrgprtctn-uplkpktdrop
- sessstat-ovrchrgprtctn-uplkbytedrop
- sessstat-ovrchrgprtctn-dnlkpktdrop
- sessstat-ovrchrgprtctn-dnlkbytedrop

show apn statistics all

The following counters display overcharging protection stats for this APN:

- UL Ovrchrg Prtctn byte drop
- UL Ovrchrg Prtctn pkt drop
- DL Ovrchrg Prtctn byte drop
- DL Ovrchrg Prtctn pkt drop

show pgw-service all

The following field display configuration information for Overcharging Protection on this P-GW service:

- EGTP Overcharge Protection

show pgw-service statistics all

The following counters display Overcharging Protection for this P-GW node:

- Drops Due To Overcharge Protection
  - Packets
  - Bytes

show sgw-service statistics name <sgw_service_name>

The output of this command shows the total number of PDNs where charging was paused:

- PDNs Total:
  - Paused Charging: <Total number of PDNs where charging was paused>

show subscribers full

The following counters display Overcharging Protection for all subscribers:

- in packet dropped overcharge protection
- in bytes dropped overcharge protection
- out packet dropped overcharge protection
- out bytes dropped overcharge protection

Important When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own.; separate debug stats have been added for P-GW.

show subscribers pgw-only full all

The following field and counters display Overcharging Protection:

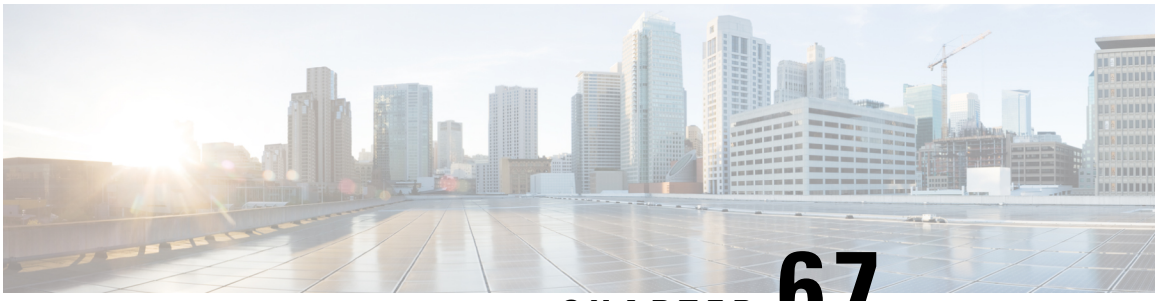
- Bearer State
  - in packet dropped overcharge protection
  - in bytes dropped overcharge protection
  - out packet dropped overcharge protection
  - out bytes dropped overcharge protection

show subscribers summary

The following counters display overcharging protection for all subscribers:

- in bytes dropped ovrchrgPtn
- in packet dropped ovrchrgPtn
- out bytes dropped ovrchrgPtn
- out packet dropped ovrchrgPtn

Important When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own; separate debug stats have been added for P-GW.



CHAPTER 67

Online Charging Support without Waiting for Credit Control Answer

- Feature Summary and Revision History, on page 1031
- Feature Description, on page 1032
- How it works, on page 1032
- Configuring Online Response Required Parameter, on page 1033
- Monitoring and Troubleshooting, on page 1033

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release new CLI for online response is added under the APN level and the feature is fully qualified for this release.	21.20.3
First introduced. **Important**	21.20

Revision Details	Release
This feature is not fully qualified in this release and is available only for testing purposes. For more information, contact your Cisco Account Representative.	

Feature Description

For 5G subscribers, all rating groups and all bearers require to have the online charging flag set to "yes" and a Gy session established to create billing records. In order not to delay a call setup or block data flow for APNs/bearers/rating groups, P-GW supports a new feature to allow charging to be done over Gy but not delay session setup or hold up data. This will mimic 5G-ChF (Charging Function) behavior through OCS.

Policy and Charging Rules Function (PCRF) indicates through the following two AVPs, which bearers need the above behavior:

- Charging Level AVP –**Online-Response-Required** AVP is defined at the Charging level and is available only when the online charging is enabled. This AVP controls if the Session Create Response must "Wait" for CCA or not.
- Override Control AVP–**Online-Response-Required** is defined at the Override Control level and is available only when online charging is enabled. This AVP overrides the new charging AVP that is received from Policy and Charging Rules Function (PCRF).

How it works

The following call flow and procedure describes how the CCR is triggered during session create.

Table 100: Procedure

Step	Description
1	The P-GW receives Session Create Request.
2	Checks the charging AVPs received from PCRF.
3	In the PCRF, either **OnlineResponseRequired** or **Override-OnlineResponseRequired** AVP is activated in the Gx Interface at charging level or Override level with an option to WAIT to DONT_WAIT. The following action happens based on the Rule selection: • If the Session Create Request is received with WAIT rule indicating OnlineResponseRequired, Session Create response waits for CCA-I over Gy interface before sending the Session Create response. • If the Session Create Request is received with DONT_WAIT rule, Session Create response does not wait for CCA-I response.
4	P-GW sends Session Create Response based on the new AVP.

The following scenarios describe how the data flow is processed:

- If there is no quota the P-GW will Assume Positive for that flow.
- If there is Quota:
  - When the Charging level AVP specifies DONT_WAIT, then there is no traffic drop.
  - When the Quota expires, P-GW will Assume positive. Except for the Error Code 4012, if there is any error code P-GW triggers Assume Positive

Configuring Online Response Required Parameter

Use the following commands to configure the Online Response required AVP in the APN configuration mode.

```
configure
   context  context_name
      apn apn_name
         bearer-control-mode  mixed
           use-gx-avp-online-response-required
           no  use-gx-avp-online-response-required
            end
```

Notes:

- **apn** : Specifies the Access Point name.
- **bearer-control-mode mixed** : This keyword indicates that the bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well. By default it is diabled.
- **use-gx-avp-online-response-required**: Enables P-GW to function according to the behavior requested in Gx AVP OnlineResponseRequired or override-OnlineResponseRequired.
- **no**: Disables the OnlineResponseRequired or override-OnlineResponseRequired feature for the specified APN.

Monitoring and Troubleshooting

Show Commands and Output

show-active-charging subscribers

The output of the above command has been enhanced to display the new parameter which shows the online response required rule definition chosen as Don't Wait. For example:

```
Override Control :
  Rule Name :
                       qci3
  Charging Parameters:
    Rating Group     : 555
    Service ID       : 333
    Online Enabled   : TRUE
```

```
   Offline Enabled  : TRUE
   Online Response Required: Don't Wait
 Policy Parameters:
   MBR UL           : 50000
   MBR DL           : 50000
```

show-active-charging-sessions-full-all

The output of the above command has been enhanced to display the new parameter which shows the online response required rule definition chosen as Wait.

```
For example
Dynamic Charging Rule Definition(s) Configured:
Name                 Prior Content-Id Chrg-Type Rule Parameters
-------------------- ----- ---------- --------- ---------------------------
       ruleName_Dean     5         55      Both Gate Status:      Allow All
                                                QoS Class Identifier:     1
                                                ARP Priority Level:       6
                                                Reporting Level: Rating Grp
                                                Metering Method:   Duration
                                                Uplink MBR:        40960000
                                                Downlink MBR:      40960000
                                                Uplink GBR:        40960000
                                                Downlink GBR:      40960000
                                                Filter 1:
                                                Direction:           Uplink
                                                Dst Addr  0.0.0.0/0
                                                Filter 2:
                                                Direction:         Downlink
                                                Src Addr  0.0.0.0/0
                                                Filter 3:
                                                Direction:           Uplink
                                                Dst Addr  ::/0
                                                Filter 4:
                                                Direction:         Downlink
                                                Src Addr  ::/0
                                                Online Response Required: Wait
```

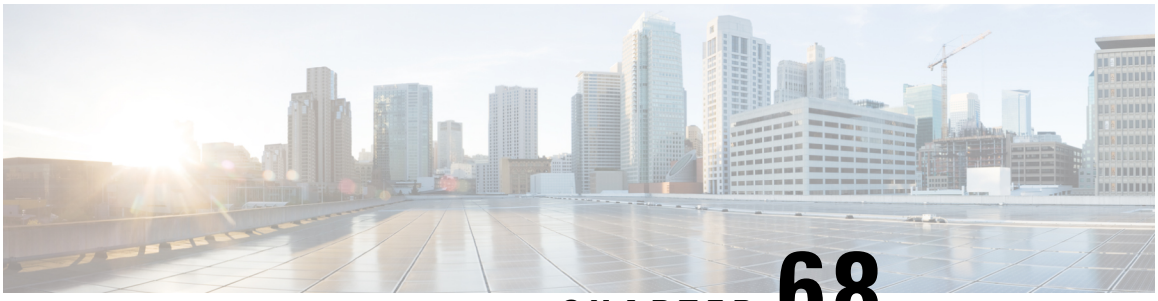
show apn-name

Use the following show apn name command output to verify the command entries.

Table 101:

Field	Description
Access Point Name (APN)	Indicates the name of the access point name (APN) for which counters are displa
Authentication Context	Name of the system context used for authentication for this APN.
Pdp Type	Indicates the type of PDP context. Pdp types are as follows: • IPv4 • IPv6
Emergency	Specifies whether **emergency-apn** option is configured in this APN or not.
Delay Tolerant	Displays whether Delay Tolerant behavior for PDN connection is available for U Power Saving Mode or not

Field	Description
PCO Options	Specifies which customized PCO (Protocol Configuration Options) options ar the network to MS GTP messages. PCO Options are as follows: • Custom1 • Mode • Link MTU • Nonlink MTU • ePDG Selection FQDN
Online Charging without Wait	Shows that the Online charging without Wait is defined at the APN level is di



CHAPTER 68

Packet Count in G-CDR

This chapter describes the following topics:

- Feature Summary and Revision History, on page 1037
- Feature Description, on page 1038
- How It Works, on page 1038
- Configuring Packet Count in G-CDR, on page 1038
- Monitoring and Troubleshooting, on page 1039

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
With this release, the P-GW accepts the Modify Bearer Request message that is without Bearer Context, and with old F-TEID.	21.14

Revision Details	Release
First introduced.	Pre 21.2

Feature Description

When an IoT UE is attached, they send a message, as needed, and go into Power Saving Mode (PSM) until the time they have to transmit the next message. The IoT UE does not detach (that is, session termination) after every message. By assessing the number of such messages through CDRs generated for the IoT UE session, the Operator can implement billing for IoT devices by including the packet counts in offline billing records.

Important This feature is applicable to custom24 GTPP dictionary.

How It Works

As part of this feature, two new attributes are introduced for the packet count: datapacketsFBCDownlink and datapacketsFBCUplink. These two attributes are CLI-controlled and visible only when the CLI is enabled. The existing attributes are not modified or removed.

Configuring Packet Count in G-CDR

This section provides information about the CLI commands available in support of the feature.

Enabling Packet Count in G-CDR

Use the following commands to enable or disable sending of packet counts in G-CDR under the GTPP Server Group Configuration mode.

```
configure
  context context_name
    gtpp group group_name
      [ no ] gtpp attribute packet-count
      end
```

NOTES:

- **no**: Disables sending of uplink and downlink packet count in G-CDR.
- **packet-count**: Specifying this option includes the optional field of "datapacketFBCUplink" and "datapacketFBCDownlink" in the CDR.
- By default, the **gtpp attribute packet-count** CLI command is disabled.

Monitoring and Troubleshooting

This section provides information regarding CLI commands available for monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

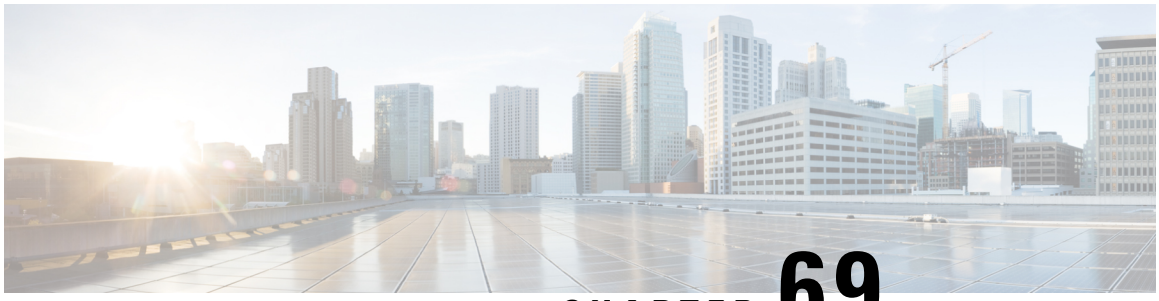
This section provides information regarding show commands and/or their outputs in support of this feature.

show configuration

The output of this CLI command has been enhanced to display the following new field when the feature is enabled: gtpp attribute packet-count

show gtpp group name <name>

The output of this CLI command has been enhanced to display the following new field when the feature is enabled: Packet count present



CHAPTER 69

Paging Policy Differentiation

This chapter describes the Paging Policy Differentiation feature 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 *P-GW Administration Guide*, the *S-GW Administration Guide*, or the *SAEGW Administration Guide* before using the procedures in this chapter.

This chapter includes the following sections:

- Feature Description, on page 1041
- How It Works, on page 1042
- Configuring Paging Policy Differentiation Feature, on page 1043
- Monitoring and Troubleshooting Paging Policy Differentiation, on page 1044

Feature Description

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.



Important P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Relationships

Since P-GW/S-GW support non-standard based DSCP marking, there is a conflict when both standard based PPD feature and non-standard based user-datagram packet DSCP configuration is enabled. To avoid this conflict:

- APN and service level configuration is ignored if PPD feature is enabled.
- S-GW/P-GW can alter the outer GTP-U header DSCP value, even if PPD feature is enabled.
- User-datagram packet DSCP value is unaltered by ECS, P-GW, and S-GW if PPD feature is enabled.
- At P-GW, APN-level configuration is added to enable/disable the PPD feature.
- At S-GW, service-level configuration is added to enable/disable the PPD feature. This is to send DSCP in Paging and Service Information IE of all the DDN messages triggered by either IMS-PDN or Internet-PDN, etc.



Important It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.

- Separate Paging feature and PPD feature co-exist in system. That means, if both features are enabled, both Paging and Service Information IE and Separate-paging IE are sent in DDN.
- Currently on P-GW, the DSCP configuration is getting applied at sub-session level during call setup time. So, when the PPD CLI is enabled for P-GW, it is applicable for new calls.
- Currently on S-GW, the DSCP configuration is getting applied at S-GW service level. So, when PPD CLI is enabled in S-GW service, it is applicable for both new and existing calls.
- Once the PPD CLI is enabled, it exists even after Session Recovery and ICSR switch over.
- The Paging and Service Information IE is used to carry per bearer paging and service information.

License

PPD is a license enabled feature. S-GW Paging Profile license key is required to enable PPD functionality for P-GW, S-GW, and SAEGW.



Important Contact your Cisco account representative for information on how to obtain a license.

How It Works

Architecture

S-GW

When S-GW supports the PPD feature, it shall include new Paging and Service Information IE in the Downlink Data Notification message triggered by the arrival of downlink data packets at the S-GW. The Paging Policy Indication value within this IE will contain the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the P-GW.

At S-GW, service-level configuration enables/disables the PPD feature. Once the PPD is configured, the feature is enabled and applicable for both existing and new calls.

P-GW

User-datagram packet DSCP value is unaltered by P-GW for downlink data. The PPD feature is supported only for S5/S8 interface. For all Handoff scenarios from other interface to S5/S8 interface, the PPD feature will get enabled if APN had it during its call setup time at that interface.

At P-GW, APN-level configuration enables/disables the PPD feature. If PPD feature is enabled for the call and handoff happens from S5/S8 interface to any other interface, PPD feature should get disabled. Now, if handoff happens and this call will come back to S5/S8 interface, PPD feature should become enabled.

SAEGW

To support PPD feature in SAEGW, both S-GW and P-GW configuration is required.

Relationships to Other Features

- The PPD feature is license controlled under the license for S-GW Paging Profile. Once the license is enabled, both features co-exist together and work independently. That means, DDN message might carry both DSCP marking specified by PPD feature and Priority DDN value specified by S-GW Paging Profile feature.
- At S-GW, the user-datagram packet DSCP value is used to send in DDN. S-GW can't change the DSCP, as per the local configuration (APN profile or service level). At eNodeB, the scheduling of the packet is based on the QCI instead of DSCP, however, any EPC node should not change/modify the inner DSCP value.
- If the PPD feature is enabled, none of the EPS nodes should change the user-datagram packet DSCP value. Therefore, ECS should avoid overwriting DSCP value of user-datagram packet when PPD is enabled.

Standards Compliance

The PPD functionality complies with the following standards:

- 29.274, CR-1565, "Paging Policy Indication in Downlink Data Notification Message"
- 23.401, CR-2731 "Paging policy differentiation for IMS voice"

Configuring Paging Policy Differentiation Feature

For the PPD feature to work, it must be enabled for P-GW and S-GW.

Both P-GW and S-GW services apply PPD configuration independently. Therefore, for any downlink data packet from an APN, there could be a case where P-GW does not have PPD configuration but S-GW has PPD configuration. To avoid such a conflict, you must configure the PPD functionality on both P-GW (APN level granularity) and S-GW (service level granularity).

Configuration

The following CLI commands are used to manage the functionality for the PPD feature.

Enabling on P-GW

The following command enables the PPD feature on P-GW at APN level.

```
configure
     context context_name
        apn apn_name
               paging-policy-differentiation
               end
```

Enabling on S-GW

The following command enables the PPD feature on S-GW at service level.

```
configure
     context context_name
        sgw-service service_name
               paging-policy-differentiation
               end
```

Notes:

- This is to send DSCP in Paging and Service Information IE of all the DDN messages triggered by either IMS-PDN or Internet-PDN, etc.
- It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.
- If PPD feature is enabled at S-GW service, it is applicable for all calls irrespective of the APN profiles.

Disabling on P-GW

The following command disables the PPD feature on P-GW at APN level.

```
configure
     context context_name
        apn apn_name
               no paging-policy-differentiation
               end
```

Disabling on S-GW

The following command disables the PPD feature on S-GW at service level.

```
configure
     context context_name
        sgw-service service_name
               no paging-policy-differentiation
               end
```

Monitoring and Troubleshooting Paging Policy Differentiation

This section includes show commands in support of the PPD feature.

P-GW Show Commands

This section provides information regarding P-GW show commands and/or their outputs in support of the PPD feature.

show apn name <apn_name>

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

show subscribers pgw-only full all

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

SAEGW Show Commands

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

show subscribers saegw-only full all

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

S-GW Show Commands

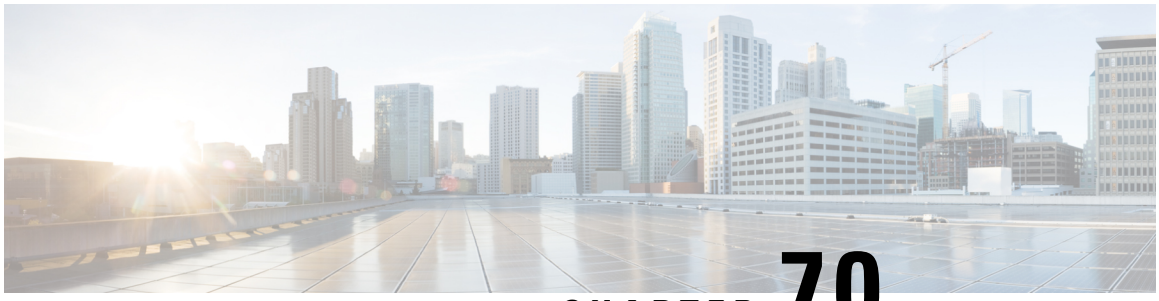
This section provides information regarding S-GW show commands and/or their outputs in support of the PPD feature.

show sgw-service name <service_name>

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

show sgw-service name <service_name>



CHAPTER 70

Password Expiration Notification

- Feature Summary and Revision History, on page 1047
- Feature Description, on page 1048
- Upgrading and Downgrading Procedures Using Save Configuration Command, on page 1049

Feature Summary and Revision History

Summary Data

Applicable Product or Functional Area	All
Applicable Platforms	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
P-GW supports no-lockout password feature after the expiry of user account passwords.	21.26

Revision Details	Release
This feature is enhanced with a new option to the **save config** command. The enhancement supports downgrade and ensures that the user profiles do not get lost after downgrade.	• 21.26 • 21.25.3
First Introduced.	21.23

Feature Description

In StarOS, if the password is not reset before the expiration date, you get locked from the configured GWs. You are allowed to log on back only when the password is reset by the administrators manually.

StarOS is enhanced to provide password expiration notification to Context, AAA, and RADIUS users. The configured GWs such as P-GW, S-GW and so on supports configuration and expiration of passwords for Administrators, Config Administrators, Inspectors, and Operators. The following provisions are supported:

- Specify the password warning interval - It gives a warning to the user about password expiry.
- Specify the password grace interval - During this grace interval the user can change the password by themself rather than approaching the Administrator every time.
- Warning interval and Grace interval have a global configuration under a context. If the user level configuration does not specify either of these values, the global values under the context take effect.

The default values of the parameters are according to Security Guidelines.

- Expiry Interval – Maximum age of the password (90 days default).
- Warn Interval – Warning period before password expiry (30 days default). You get a warning about approaching password expiry. You can continue without changing the password.
- Grace Interval – Days after password expiry, you can use the old password. Beyond the grace period, you are not able to log in with the old password. Admin has to reset the password for you.

For example:

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
```

```
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

Upgrade and Downgrade Process for Password Expiration Notification

The Password Expiry Notification feature keywords in Subscriber configuration supports the **max-age**, **exp-grace-interval**, and **exp-warn-interval**. These new parameters are configured at the Context Global level. Context Global level parameters are used when the per user level configuration is not configured with a default value. For example, for the **max-age** of the password, the default value is 90 days.

For the user profiles with no expiry-date at per user level, startup config takes an expiry date of 90 days for that user. This problem can be solved by manually editing the startup configuration file, but this solution leads to issues when users are distributed across locations.

If downgrade is needed, user profiles are lost as new keywords are not valid for older releases.

Upgrading and Downgrading Procedures Using Save Configuration Command

Use the following upgrade process:

- Before upgrade, add the **[no] password max-age** command at context level, in all contexts where users are configured in the startup configuration.
- When reloading with image using the updated startup config, all users that are configured without an expiry date will pickup the context level configuration by default and set the user level **no-max-age** keyword automatically.

Use the following downgrade process:

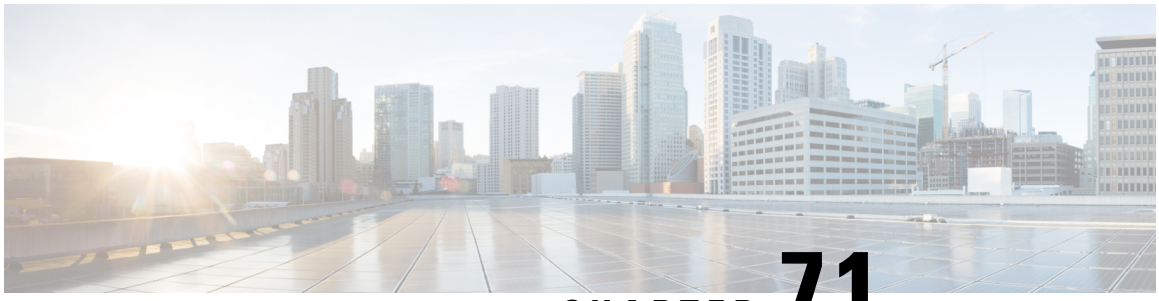
Use the **legacy-password-expiry** CLI command in the **save config** command, based on which new keywords are not saved. Configuration is stored in a format which previous release recognizes.

Use the following configuration under context configuration:

```
configure
   context host_name
      save configuration url [ confd | ignore-locks | obsolete-encryption
| showsecrets | verbose ] [ -redundant ] [ -noconfirm ] [
legacy-password-expiry ]
```

NOTES:

- **save configuration** *url* **legacy-password-expiry**: Generates a backward compatible file by removing the expiry notification keywords. The **save config** command makes the configuration compatible with older versions.



CHAPTER 71

P-GW Buffering Mechanism

- Feature Summary and Revision History, on page 1051
- Feature Description, on page 1052
- How It Works, on page 1052
- Configuring the P-GW Buffering Mechanism Feature, on page 1052

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, P-GW supports Buffering Mechanism feature.	21.23
First introduced.	21.14

Feature Description

The P-GW can buffer a maximum of two policy (PCRF) messages when the Default-Bearer-QoS change is in pending state. With Presence Reporting Area (PRA) related call flows, two or more messages can be received when the Update Bearer Response (UBResp) is in pending state.

The P-GW Buffering Mechanism feature enables the P-GW to gracefully handle the RAR or CCA-U received from the PCRF when P-GW waits for the UBResp. Once the UBResp is received, the pending messages are fetched from the P-GW Buffer Queue for further processing.

How It Works

Under Active Charging Service (ACS) mode, a CLI command - **pending-buffer-size**, is added to increase the buffer size. The PCRF messages are buffered until the P-GW receives a UBResp message while the Default-Bearer-QoS change is in pending state.

Configuring the P-GW Buffering Mechanism Feature

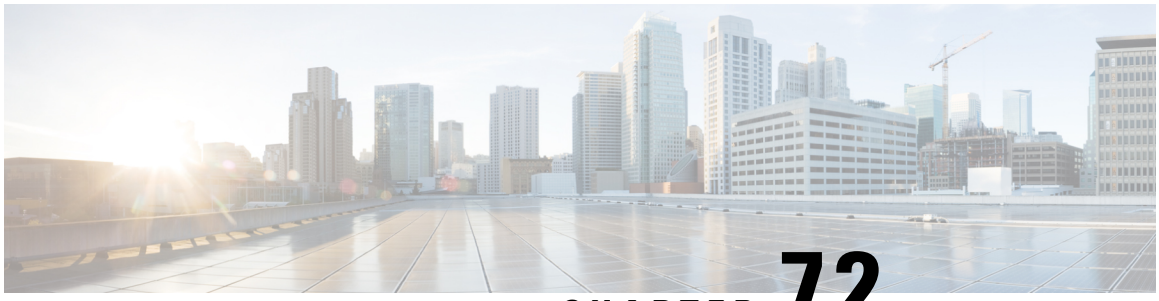
Use the following configuration to increase the buffer size for storing PCRF messages when the Default-Bearer-QoS change status is in pending.

```
configure
  active-charging service service_name
    policy control def-bearer-qos-change pending-buffer-size buffer_size
    end
```

NOTES:

- **def-bearer-qos-change**: Sets the Default-Bearer-QoS change parameters.
- **pending-buffer-size** *buffer_size*: Specifies the buffer size for storing the PCRF messages when Default-Bearer-QoS change is pending. The buffer_size is an integer ranging from 2 through 4.

  The minimum configured value is 2 and maximum is 4.
- The **no policy control def-bearer-qos-change** configures the command with its default setting. Default = 2.
- The default value suffices for most use-cases. However, higher values must be configured based on the use-case basis and by considering the memory usage.
- The CLI command takes effect for new calls.



CHAPTER 72

P-GW Buffering Optimization

- Feature Summary and Revision History, on page 1053
- Feature Description, on page 1054
- Relationship to Other Feature, on page 1054
- How it Works, on page 1054
- Configuring the P-GW Buffering Optimization, on page 1054
- Monitoring and Troubleshooting, on page 1055

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC- DI • VPC- SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, P-GW supports Buffering Optimization to handle PRA messages efficiently.	21.23
First Introduced	21.22.3

Feature Description

The P-GW Buffering Optimization enables the P-GW to handle the Presence Reporting Area (PRA) messages efficiently. When two or more PRAs are received, while UBResp is still pending, there are chances that P-GW buffer queue can become full or even a message drop can happen. This enhancement enables the PRA response from Policy and Charging Rules Function (PCRF) to be handled efficiently as the chances of message drop is less.

When a new message arrives, the P-GW merges the message with the existing similar type of message in the queue. This allows the P-GW to process similar type of messages at the same time without increasing the queue size and reducing the message drop ratio. When messages are read from the queue, the Gx Rule Level Attribute -value pairs (AVPs) defined actions are triggered. The Rule Level AVPs validity is not checked when messages are buffered.

Relationship to Other Feature

The P-GW Buffering Optimization feature is related to P-GW Buffering Mechanism functionality. For details, see the *P-GW Buffering Mechanism* chapter in the *P-GW Administration Guide*.

How it Works

Under Active Charging Service (ACS) mode, a CLI command - **optimze-update** is enabled or disbaled to enable or disable the buffering mechanism.

Configuring the P-GW Buffering Optimization

Use the following configuration to enable or disable the P-GW buffering optimization to process the similar type of messages in the queue.

```
configure
          active-charging service service_name
            [ no ] policy control optimze-update pra-change
        end
```

NOTES:

- **optimize-update**: Enables the optimization for multiple policies received from PCRF, when the earlier response is pending. Default is Disabled.
- **no**: Disables the optimization for multiple policies.
- **pra-change**: Enables policy optimization only during the Presence Reporting Area (PRA) change.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands to support this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show Active-Charging Sessions Full All

The output of the Show Active-Charging Sessions Full All.

Table 102: show active-charging sessions full all Command Output Descriptions

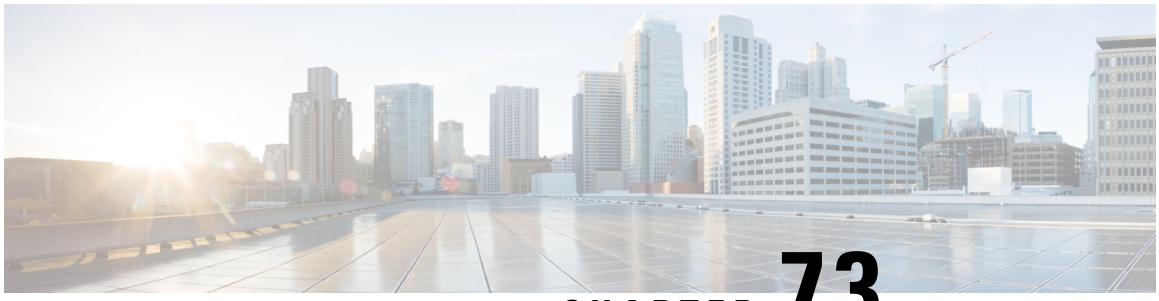
Field	Description
Current P-GW-Buffer Queue Length	Displays the currently utilized queue length.
Total P-GW Buffer Merge Count	Displays the merged count of PRA messages.

show Active-Charging Service All

The output of the Show Active-Charging Service All.

Table 103: show active-charging service all Command Output Descriptions

Field	Description
optimize-update	Enables multiple policy optimization.
pra-change	Enables optimization policies for PRA changes.



CHAPTER 73

P-GW Handoff KPIs for VoWiFi

• P-GW Handoff KPIs for VoWiFi, on page 1057

P-GW Handoff KPIs for VoWiFi

Feature Changes

Currently, there are no statistics to determine the number of new sessions started on a particular RAT technology and to monitor any inter-technology handovers per APN.

This feature introduces new session/handoff KPIs and P-GW VoWifi specific KPIs to monitor the following:

- the number of new sessions started on a particular RAT technology
- the inter-technology handover per APN from and to all access technologies
- subscriber activity for network planning

The statistical information is maintained per APN and per P-GW/SAEGW service type. CLIs are applicable only for P-GW and SAEGW product. If eHRPD/PMIP/GGSN services are associated with a P-GW/SAEGW service, then counters related to these services will be reflected under P-GW/SAEGW service statistics CLI output.

Benefits

With the introduction of this feature, operators can have KPIs to monitor per RAT Initiated Sessions and Inter-technology handovers so that they can gauge 2G/3G/4G/WiFi/eHRPD coverage.

Operators can also:

- get statistics that report on:
  - new access technologies such as Wi-Fi that uses the ePDG
  - how a session has been initiated
  - how many handoffs have been done
- track subscriber activity in the network
- plan network accordingly

Limitations

- Initiated session statistics and handover statistics at APN-level are not maintained or incremented at demux due to memory and CPU constraints. During congestion scenarios, for example, some of the calls are rejected at the demux and so this count will not show up in the APN-level initiated session counter.
- Bulkstats for eHRPD and S2b-PMIP are not supported under SAEGW schema.

Monitoring and Troubleshooting P-GW Handoff KPIs for VoWiFi

The following section describes commands available to monitor P-GW Handoff KPIs for VoWiFi.

HandOff KPIS for VoWiFi Show Commands

The following section describes commands available to monitor Handoff KPIs for VoWiFi.

show apn statistics [all | name *apn_name* | verbose]

This command displays the following output.

```
Initiated Sessions per RAT Type:
    EUTRAN:    0    UTRAN:       0
    GERAN:     0    EHRPD:       0
    S2A GTP:   0    S2B GTP:     0
    S2B PMIP:  0

Inter Technology handover:
  GNGP-to-LTE handover:         LTE-to-GNGP handover:
    Attempted:        0         Attempted:         0
    Succeeded:        0         Succeeded:         0
    Failed:           0         Failed:            0

GNGP-to-S4SGSN handover:       S4SGSN-to-GNGP handover:
    Attempted:       0         Attempted:          0
    Succeeded:       0         Succeeded:          0
    Failed:          0         Failed:             0

S4SGSN-to-LTE handover:        LTE-to-S4SGSN handover:
    Attempted:       0         Attempted:          0
    Succeeded:       0         Succeeded:          0
    Failed:          0         Failed:             0

LTE-to-eHRPD handover:         eHRPD-to-LTE handover:
    Attempted:       0         Attempted:          0
    Succeeded:       0         Succeeded:          0
    Failed:          0         Failed:             0

LTE-to-S2bPMIP handover:       S2bPMIP-to-LTE handover:
    Attempted:       0         Attempted:          0
    Succeeded:       0         Succeeded:          0
    Failed:          0         Failed:             0

eHRPD-to-S2bPMIP handover:     S2bPMIP-to-eHRPD handover:
    Attempted:       0         Attempted:          0
    Succeeded:       0         Succeeded:          0
    Failed:          0         Failed:             0

S2bGTP-to-LTE handover:        LTE-to-S2bGTP handover:
    Attempted:       0         Attempted:          0
```

```
    Succeeded:       0          Succeeded:          0
    Failed:          0          Failed:             0

S2bGTP-to-eHRPD handover:       eHRPD-to-S2bGTP handover:
    Attempted:       0          Attempted:          0
    Succeeded:       0          Succeeded:          0
    Failed:          0          Failed:             0

S2aGTP-to-LTE handover:         LTE-to-S2aGTP handover:
    Attempted:       0          Attempted:           0
    Succeeded:       0          Succeeded:           0
    Failed:          0          Failed:              0
```

show pgw-service statistics { all | name *service_name* }

The command displays the following output:

```
Initiated PDNs By RAT-Type:
    EUTRAN:            0          UTRAN:       0
    GERAN:             0          EHRPD:       0
    S2A GTP:           0          S2B GTP:     0
    S2B PMIP:          0
```

show saegw-service statistics { all | name *service_name* } function pgw

The command displays the following output:

```
Initiated PDNs By RAT-Type:
  EUTRAN:                    0       UTRAN:                    0
  GERAN:                     0       EHRPD:                    0
  S2A GTP:                   0       S2B GTP:                  0
  S2B PMIP:                  0
```

Schema for P-GW Handoff KPIs for VoWifi

This section lists the schemas added in for the P-GW Handoff KPIs for VoWifi Feature.

APN Schema

Initiated Sessions Statistics Information based on RAT Technology:

The following new counters have been added to display the number of Initiated Sessions per RAT type, per Service/APN in this enhancement:

- initiated-eutran-sessions
- initiated-utran-sessions
- initiated-geran-sessions
- initiated-ehrpd-sessions
- initiated-s2a-gtp-sessions
- initiated-s2b-gtp-sessions
- initiated-s2b-pmip-sessions

Inter-Technology Handover Statistics:

The following new counters have been added to display the number of inter-technology handover statistics per APN/Service have been added in this enhancement:

- apn-handoverstat-gngptolteatt
- apn-handoverstat-gngptoltesucc
- apn-handoverstat-gngptoltefail
- apn-handoverstat-ltetogngpatt
- apn-handoverstat-ltetogngpsucc
- apn-handoverstat-ltetogngpfail
- apn-handoverstat-gngptos4sgsnatt
- apn-handoverstat-gngptos4sgsnsucc
- apn-handoverstat-gngptos4sgsnfail
- apn-handoverstat-s4sgsntogngpatt
- apn-handoverstat-s4sgsntogngpsucc
- apn-handoverstat-s4sgsntogngpfail
- apn-handoverstat-s4sgsntolteatt
- apn-handoverstat-s4sgsntoltesucc
- apn-handoverstat-s4sgsntoltefail
- apn-handoverstat-ltetos4sgsnatt
- apn-handoverstat-ltetos4sgsnsucc
- apn-handoverstat-ltetos4sgsnfail
- apn-handoverstat-ltetoehrpdatt
- apn-handoverstat-ltetoehrpdsucc
- apn-handoverstat-ltetoehrpdfail
- apn-handoverstat-ehrpdtolteatt
- apn-handoverstat-ehrpdtoltesucc
- apn-handoverstat-ehrpdtoltefail
- apn-handoverstat-ltetos2bpmipatt
- apn-handoverstat-ltetos2bpmipsucc
- apn-handoverstat-ltetos2bpmipfail
- apn-handoverstat-s2bpmiptolteatt
- apn-handoverstat-s2bpmiptoltesucc
- apn-handoverstat-s2bpmiptoltefail

- apn-handoverstat-ehrpdtos2bpmipatt
- apn-handoverstat-ehrpdtos2bpmipsucc
- apn-handoverstat-ehrpdtos2bpmipfail
- apn-handoverstat-s2bpmiptoehrpdatt
- apn-handoverstat-s2bpmiptoehrpdsucc
- apn-handoverstat-s2bpmiptoehrpdfail
- apn-handoverstat-s2bgtptolteatt
- apn-handoverstat-s2bgtptoltesucc
- apn-handoverstat-s2bgtptoltefail
- apn-handoverstat-ltetos2bgtpatt
- apn-handoverstat-ltetos2bgtpsucc
- apn-handoverstat-ltetos2bgtpfail
- apn-handoverstat-s2bgtptoehrpdatt
- apn-handoverstat-s2bgtptoehrpdsucc
- apn-handoverstat-s2bgtptoehrpdfail
- apn-handoverstat-ehrpdtos2bgtpatt
- apn-handoverstat-ehrpdtos2bgtpsucc
- apn-handoverstat-ehrpdtos2bgtpfail
- apn-handoverstat-s2agtptolteatt
- apn-handoverstat-s2agtptoltesucc
- apn-handoverstat-s2agtptoltefail
- apn-handoverstat-ltetos2agtpatt
- apn-handoverstat-ltetos2agtpsucc
- apn-handoverstat-ltetos2agtpfail

P-GW Schema

Initiated Sessions Statistics Information based on RAT Technology: The following counters have been added to display the number of Initiated Sessions per RAT type, per Service /APN in this enhancement:

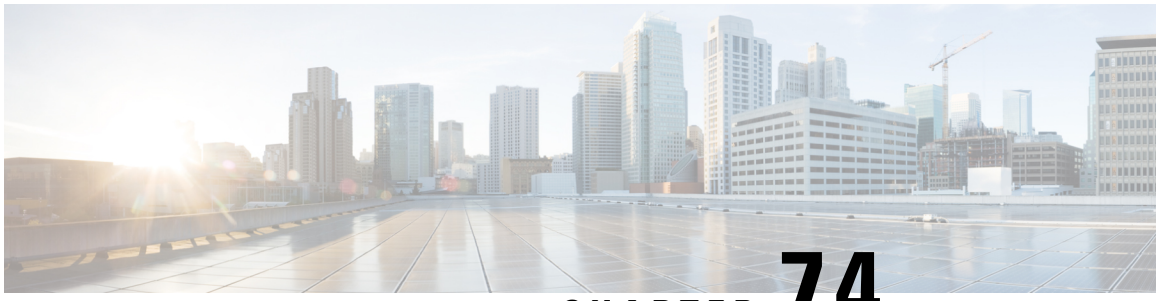
- sessstat-rat-init-eutran
- sessstat-rat-init-utran
- sessstat-rat-init-geran
- sessstat-rat-init-ehrpd
- sessstat-rat-init-s2a-gtp

- sessstat-rat-init-s2b-gtp
- sessstat-rat-init-s2b-pmip

SAEGW Schema

Initiated Sessions Statistics Information based on RAT Technology: The following counters have been added to display the number of Initiated Sessions per RAT type, per Service/APN in this enhancement:

- pgw-sessstat-pdn-rat-init-eutran
- pgw-sessstat-pdn-rat-init-utran
- pgw-sessstat-pdn-rat-init-geran
- pgw-sessstat-pdn-rat-init-s2a-gtp
- pgw-sessstat-pdn-rat-init-s2b-gtp



CHAPTER 74

Presence Reporting Area

This chapter describes the following topics:

- Feature Summary and Revision History, on page 1063
- Feature Description, on page 1064
- How It Works, on page 1064
- Multiple Presence Reporting Area, on page 1067
- Configuring Presence Reporting Area, on page 1068
- Monitoring and Troubleshooting, on page 1069

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

This feature adds support for the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards.

The Presence Reporting Area is an area defined within the 3GPP packet domain for reporting of UE presence within that area. This is required for policy control and in charging scenarios. In E-UTRAN, the PRA may consist in a set of neighbor or non-neighbor Tracking Areas, or eNBs or cells. There are two types of Presence Reporting Areas: "UE-dedicated Presence Reporting Areas" and "Core Network pre-configured Presence Reporting Areas" that apply to an MME pool.

This feature has the following highlights:

- This feature is supported for LTE/S4-SGSN related RAT-type. For any other RAT type, P-GW ignores PRA information received from the PCRF.
- Currently single PRA-ID is supported per session as specification compliance.
- Currently, in P-GW, core network pre-configured presence reporting area is supported.
- For ICSR to N-1 release, PRA feature is not supported.
- PRA-ID is not supported on CDR interface, that is, Gz, Gy and Rf.

How It Works

During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA are required for an IP-CAN session. This determination is made based on the subscriber's profile configuration and the supported AVP features. The parameter CNO-ULI is set for the same. If the reporting is required for the IP-CAN session, the PCRF provides Presence-Reporting-Area-Information AVP, which contains the PRA identifier within the Presence-Reporting-Area-Identifier AVP to the PCEF. For a UE-dedicated PRA, PCRF provides the list of elements consisting of the PRA within the Presence-Reporting-Area-Elements-List AVP to the PCEF. The PCRF might activate the reporting changes of the UE presence in the PRA by subscribing to the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event trigger at the PCEF at any time during the entire IP-CAN session.

When the UE enters or leaves the PRA, PCEF reports the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event. Also, the PCEF also reports the PRA status within the Presence-Reporting-Area-Status AVP and PRA identifier within Presence-Reporting-Area-Identifier AVP included in Presence-Area-Information AVP.

Following table describes the scenario and its associated behavior:

Scenario	Behavior
When PCRF sends a new PRA ID different than the initial call setup.	• P-GW receives the new PRA ID during the initial call setup and stores the PRA ID information. • In RAR, the PRA_EVENT_TRIGGER is registered. • P-GW send PRA_ACTION PRA ID="A", ACTION=start. • In CCA-U, a new PRA ID is received. • P-GW stores new PRA ID information • P-GW sends PRA_ACTION PRA ID = "B", Action=start but does not send Action=stop for the earlier PRA. **Important** Ideally, in above condition, PCRF disables the event triggers first and sends a new PRA-ID=B and enables the event trigger in subsequent message.
When PCRF sends a new PRA ID which is same as the initial call setup.	PRA ID does not send any PRA Action toward S-GW and P-GW ignores this.
PRA ID Decode Behavior	If PRA ID received is "core network pre-configured presence reporting area", then, P-GW ignores the "Element List" coming from PCRF. Otherwise, if PRA ID is "UE-dedicated Presence Reporting Area", then, P-GW parses the "Element List" and forwards it toward the access side.
If PRA ID values from PCRF are 1 octet, 2 octets, and 3 octets.	MSB of the value received from the PCRF is evaluated to find the PRA type. While encoding, GTPC side zeros are prepended to make it 3 octets. For example, if PRA ID = FC (1111 1100) is received from PCRF it is considered as UE-dedicated PRA and while decoding it is decoded as 00 00 FC. P-GW forwards PRA information toward the roaming subscriber if it is received from the PCRF or from UE. **Important** Change of UE presence in the Presence Reporting Area reporting does not apply to the roaming scenario.
Roaming Scenario	Change of UE presence in the Presence Reporting Area reporting does not apply to the roaming scenario. When the serving EPC node (MME, S4-SGSN) is changed, the Presence Reporting Area identifier is transferred for all PDN connections as part of the MM Context information to the target serving node during the mobility procedure. The list of Presence Reporting Area elements are also transferred if they are provided by the P-GW.

Scenario	Behavior
Handover Behavior: How the PRA identifier is communicated from source MME/S4-SGSN to target MME/S4-SGSN.	MME/S4-SGSN gets the PRA Identifier from source MME/S4-SGSN as part of MM Context information. When the serving EPC node (MME, S4-SGSN) is changed, the Presence Reporting Area identifier is transferred for all PDN connections as part of the MM Context information to the target serving node during the mobility procedure. The list of Presence Reporting Area elements are also transferred if they are provided by the P-GW.
Handoff Behavior: How PRA is disabled when the new access type is not supported PRA.	Depending on the access type and internal configuration PCRF deactivates the PRA, if the new access PRA is not supported. During an IP-CAN session, P-GW notifies the PCRF that the UE is located in an access type, where local PCRF configuration is such that the reporting changes of the UE presence in the PRA are not supported. The PCRF unsubscribes to the change of UE presence in the PRA, if previously activated.
Behavior if for E-UTRAN some nodes do not support PRA.	If PRA is enabled from PCRF, then EPC nodes supports it. If all nodes are not supported, then PRA PCRF activates the Location Change Reporting. **Important** For E-UTRAN access, homogeneous support of reporting changes of UE presence in a Presence Reporting Area in a network is assumed. When the PCRF configuration indicates that reporting changes of the UE presence in a PRA is supported for E-UTRAN, this means all P-GWs, all MME, and all S-GW support it, including the MME and S-GW working in the network sharing mode. If the change of UE presence in the PRA reporting is not supported, the PCRF may instead activate the location change reporting at the cell or serving area level.
When access side procedure failure or collision occurs (Create or Update Bearer procedure)	In Update or Create bearer procedure failure where the PRA action was sent in the request message and if PRA information was not received in response message, P-GW attempts to send the PRA action in next control procedure toward the remote peer. In Update or Create bearer procedure failure where PRA action was sent in the request message and if PRA information was not received in the response message, P-GW assumes it as PRA action was successfully communicated toward the remote peer. In the Update or Create bearer collision scenario where PRA action was sent in the request message and Update or Create procedure got aborted, P-GW attempts to send the PRA action in next control procedure toward the remote peer.

Multiple Presence Reporting Area



Important This feature is introduced in release 21.9.1.

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

When the Multiple-PRA feature is supported during the lifetime of the IP-CAN session P-GW handles the change of UE Presence in Reporting Area(s) request from PCRF in PRA-Install AVP including the Presence-Reporting-Area-Information AVP(s) which each contains the Presence Reporting Area Identifier within the Presence-Reporting-Area-Identifier AVP.

P-GW Handling the Event Trigger

CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT from PCRF for the activation of the reporting changes of UE presence in Presence Reporting Area(s).

P-GW handles the PRA Identifier(s) modify request from PCRF with the new PRA within the PRA-Install AVP as described above and/or by removing the existing PRA(s) within the PRA-Remove AVP. In this case, the Presence-Reporting-Area-Identifier AVP of the removed PRA must be included within the Presence-Reporting-Area-Information AVP(s).

P-GW supports PRA-Install and PRA-Remove AVPs from PCRF in the following messages:

- CC-Answer (CCA) Command
- Re-Auth-Request (RAR) Command

The P-GW handles the request from PCRF to unsubscribe to the change of UE presence in Presence Reporting Area wherein PCRF provides the Event-Trigger AVP with the value CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) removed, if previously activated.

P-GW supports the maximum of 4 PRA(s) for a IP-CAN session at any given point of time. The maximum number of PRAs is configurable in PCRF and must be capped to 4. P-GW will ignore the Presence Reporting Area Identifiers entries beyond 4.

When the P-GW receives the presence reporting area information from the serving node over S5/S8 interface indicating that the UE is inside or outside of one or more presence reporting areas or any of the presence reporting areas is set to inactive, the P-GW will check if the reported presence reported area identifier corresponds to a presence reporting area that is relevant for the PCRF. In that case, the P-GW reports the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event in the Event-Trigger AVP additionally, the P-GW also reports the presence reporting area status within the Presence-Reporting-Area-Status AVP and presence reporting area identifier within Presence-Reporting-Area-Identifier AVP included in Presence-Reporting-Area-Information AVP(s) for each of the presence reporting areas reported by the serving node.

The P-GW de-activates the relevant IP-CAN specific procedure for reporting change of UE presence in Presence Reporting Area, when the PCRF and OCS unsubscribe to change of UE presence in Presence Reporting Area.

PRA-Install AVP (3GPP-EPS access type) Definition

The PRA-Install AVP (AVP code 2845) is of type Grouped, and it is used to provision a list of new or updated Presence Reporting Area(s) for an IP-CAN session.

AVP Format:

```
PRA-Install ::= < AVP Header: 2845 >
 *[ Presence-Reporting-Area-Information ]
 *[ AVP ]
```

PRA-Remove AVP (3GPP-EPS access type) Definition

The PRA-Remove AVP (AVP code 2846) is of type Grouped, and it is used to stop the reporting of a list of Presence Reporting Area(s) for an IP-CAN session.

AVP Format:

```
PRA-Remove ::= < AVP Header: 2846 >
 *[ Presence-Reporting-Area-Identifier ]
 *[ AVP ]
```

Configuring Presence Reporting Area

Configuring PRA

Use the following configuration to enable the PRA:

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features cno-uli
            { default | no } diameter encode-supported-features
            end
```

NOTES:

- **diameter encode-supported-features**: Enables or disables encoding and sending of Supported-Features AVP.
- **cno-uli**: Enables Presence Reporting Area Information Reporting feature.
- **no**: Removes the previously configured supported features.
- **default**: Applies the default setting for this command.

Configuring Multiple-PRA

Use the following configuration to enable Multiple Presence Reporting Area (Multiple-PRA) Feature.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features multiple-pra
```

```
{ default | no } diameter encode-supported-features
end
```

NOTES:

- **ims-auth-service** *service_name*: Creates an IMS authentication service. *service_name* must be an alphanumeric string of 1 through 63 characters.
- **policy-control**: Configures Diameter authorization and policy control parameter for IMS authorization.
- **diameter encode-supported-features**: Enables encoding and sending of Supported-Features AVP.
- **multiple-pra**: Enables the Multiple Presence Reporting Area Information Reporting feature.
- **no**: Removes the previously configured supported features.
- **default**: Applies the default setting for this command.

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 this feature.

show ims-authorization service name *<service-name>*

The output of the above command is modified to display the negotiated conditional policy features related information. The modified output is as follows:

```
Context: ha
  IMS Authorization Service name: imsa-Gx
                  ……
  Diameter Policy Control:
    Endpoint: gx.st16.starentnetworks.com
    Origin-Realm: starentnetworks.com
    Dictionary: r8-gx-standard
    Supported Features:
      mission-critical-qcis
      conditional-policy-info-default-qos
cno-uli
    Request Timeout:
        Initial Request   : 100 deciseconds
        Update Request    : 100 deciseconds
        Terminate Request : 100 deciseconds
    Endpoint Peer Select: Not Enabled
    Reauth Trigger: All
    Custom Reauth Trigger:
      QoS-Change
```

show ims-authorization sessions full all

The output of this command includes the following fields:

```
CallId: 00004e26            Service Name: imsa-Gx
  IMSI:  123456789012349
  Session ID: gx.st16.starentnetworks.com;20006;2305;598ab8cf-102
  Bearer Type: GTP
  SGSN IP-Addr: 192.168.23.4
  APN: starent.com
  Bearer Control Mode: UE/NW
  State: Connected
  Negotiated Supported Features:
    3gpp-r8
    conditional-policy-info-default-qos
    cno-uli
  Auth Decision:
    Event Triggers:
      QoS-Change
      RAT-Change
      Change-Of-UE-Presence-In-PRA
      Usage-Report
      Resource-Modification-Request
    multiple-pra
```

show ims-authorization service statistics

The output of the above command is modified to display the PRA feature statistics. The modified output is as follows:

```
IMS Auth Service Statistics Summary:
Total Services:      2
Auth Session:
  Current Active:               1
  Current Fallback Session:     0             Current PCRF Session:          1
  Total Attempted:              1             Total Setup:                   1
  Total Failed:                 0             Total Released:                0
  Total Fallback:               0
Re-Authorization Triggers:
  SGSN Change:                  0             PLMN Change:                   0
  RAT Change:                   0             TFT Change:                    0
  Bearer Recovery:              0             Bearer Loss:                   0
  QoS Change:                   0             Policy Failure:                0
  IP-CAN Change:                0             Resources Limitation:          0
  Max Num of Bearers Rchd:      0             QoS Chng Exceeding Auth:       0
  RAI Change:                   0             User Location Change:          0
  TAI Change:                   0             ECGI Change:                   0
  PCRF Triggered ReAuth:        0             Preservation Changed:          0
  Reactivation Changed:         0             Revalidation Timeout:          0
  AN GW Changed:                0             Out Of Credit Reauth:          0
  Reallocation Of Credit:       0             Def EPS Bearer QoS Chng:       0
  Successful Resource Alloc:    0             Usage Report:                  0
  Service Flow Detection:       0             UE Timezone Change:            0
UE IP Address Allocate:         0             UE IP Address Release:         0
  Resource Modification Req:    0             APN AMBR Mod Failure:          0
  Def Bearer QOS Mod Failure:   0             Tethering Flow Detected:       0
  Chrg Correlation Exchange:    0             Subnet Change:                 0
  Session Recovery:             0             Session Sync:                  0
  Access Nw Info Report:        0             DCCA Failure Report:           0
  Application Start:            0             Application Stop:              0
  Change Of UE Presence In PRA: 1
Local Fallback:
CCRU sent:                      0
```

show subscribers pgw-only full all

The output of this command includes the following fields:

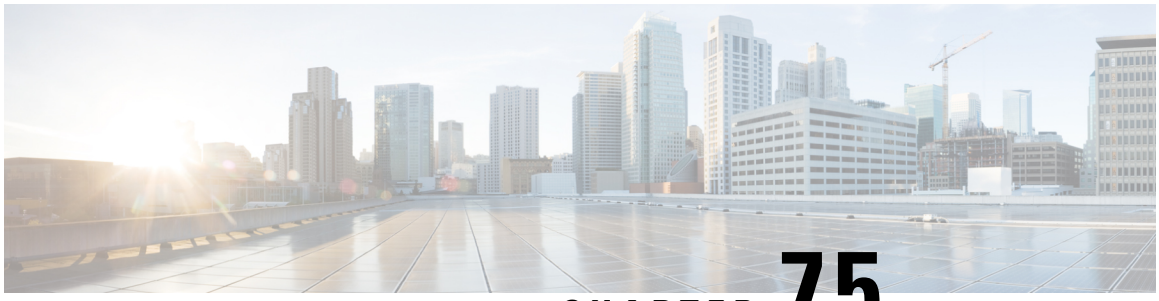
```
Username        : xyz
Subscriber Type : Visitor
Status          : Online/Active
State           : Connected
Connect Time    : Mon Aug 28 07:32:13 2017
Auto Delete     : No
Idle time       : 00h00m06s
MS TimeZone     : n/a                  Daylight Saving Time: n/a
Access Type: gtp-pdn-type-ipv4         Network Type: IP
Access Tech: eUTRAN                    pgw-service-name: pgw1
Callid: 00004e23                       IMSI: 123456789012349
MSISDN: 9326737733
Interface Type: S5S8GTP                Low Access Priority: N/A
TWAN Mode: N/A
eMPS Bearer: No
Emergency Bearer Type: N/A
IMS-media Bearer: No
S6b Auth Status: Enabled
Access Peer Profile: default
Acct-session-id (C1): C0A8170100000003
ThreeGPP2-correlation-id (C2): 00500660 / 002shwI-
Card/Cpu: 2/0                          Sessmgr Instance: 1
ULI:
 TAI-ID:
  MCC: 214  MNC: 365
  TAC: 0x6789
 ECGI-ID:
  MCC: 214 MNC: 365
  ECI: 0x1234567
PRA Information:
 PRA-ID: 0x801204      Action: Start           Status: In
PRA Information:
 PRA-ID: 0xA11202      Action: Start           Status: N/A
```

show subs saegw-only full all

The output of the above command is modified to include the PRA Information such as PRA-ID, PRA Status, and PRA Action. The modified output is as follows:

```
Username          : xyz
SAEGW Call mode   : Co-located
Subscriber Type   : Visitor
Status            : Online/Active
State             : Connected
Bearer State      : Active
Connect Time      : Mon Aug 28 08:21:45 2017

SAEGW UID         : 10001
Idle time         : 00h00m19s
Auto Delete       : No
Callid            : 4e25                       IMSI               : 241460144418770
Card/Cpu          : 2/0                        Sessmgr Instance   : 1
Source context    : ingress                    Destination context : egress
Bearer Type       : Default                    Bearer-Id          : 5
Access Type       : gtp-pdn-type-ipv4          Network Type       : IP
Access Tech       : eUTRAN                     saegw-service-name  : saegw
MSISDN            : 9326737733
```

```
TWAN Mode          : N/A
eMPS Bearer        : No
IPv6 alloc type    : n/a
ECS Rulebase       : prepaid
Chrg Char Sel Mod : Peer Supplied
Restoration priority level : n/a
HLCOM Session      : No
IP Address         : 10.0.0.5
Bearer capable for restoration: No
UE P-CSCF Restoration Support : No

Peer Profile       :
  PGW Access       : default
  SGW Access       : default
  SGW Network      : default

ULI                : TAI-ID
  MCC              : 214                          MNC              : 365
  LAC              : n/a                          TAC              : 0x6789
  SAC              : n/a                          RAC              : n/a
  CI               : n/a                          ECI              : 0x1234567

PRA Information    :
  PRA-ID: 0xFC0104     Action: Start           Status: In

Bearer QoS         :
 QCI               : 5
 ARP               : 0x08
 PCI               : 0 (Enabled)
 PL                : 2
 PVI               : 0 (Enabled)
 MBR Uplink(bps)   : 0                          MBR Downlink(bps)    : 0
 GBR Uplink(bps)   : 0                          GBR Downlink(bps)    : 0
```



CHAPTER 75

Proxy-Mobile IP

This chapter describes system support for 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 before using the procedures in this chapter.

Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:

- Overview, on page 1073
- How Proxy Mobile IP Works in 3GPP2 Network, on page 1076
- How Proxy Mobile IP Works in 3GPP Network, on page 1080
- How Proxy Mobile IP Works in WiMAX Network, on page 1083
- How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication, on page 1087
- Configuring Proxy Mobile-IP Support, on page 1093

Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

Important Proxy Mobile IP 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 Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Table 104: Applicable Products and Relevant Sections

Applicable Product(s)	Refer to Sections
PDSN	• Proxy Mobile IP in 3GPP2 Service, on page 1075 • How Proxy Mobile IP Works in 3GPP2 Network, on page 1076 • Configuring FA Services, on page 1093 • Configuring Proxy MIP HA Failover, on page 1094 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 1095 • RADIUS Attributes Required for Proxy Mobile IP, on page 1095 • Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN, on page 1096 • Configuring Default Subscriber Parameters in Home Agent Context, on page 10
GGSN	• Proxy Mobile IP in 3GPP Service, on page 1075 • How Proxy Mobile IP Works in 3GPP Network, on page 1080 • Configuring FA Services, on page 1093 • Configuring Proxy MIP HA Failover, on page 1094 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 1095 • RADIUS Attributes Required for Proxy Mobile IP, on page 1095 • Configuring Default Subscriber Parameters in Home Agent Context, on page 10 • Configuring APN Parameters, on page 1097
ASN GW	• Proxy Mobile IP in WiMAX Service, on page 1076 • How Proxy Mobile IP Works in WiMAX Network, on page 1083 • Configuring FA Services, on page 1093 • Configuring Proxy MIP HA Failover, on page 1094 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 1095 • RADIUS Attributes Required for Proxy Mobile IP, on page 1095 • Configuring Default Subscriber Parameters in Home Agent Context, on page 10

Applicable Product(s)	Refer to Sections
PDIF	• How Proxy Mobile IP Works in a WiFi Network with Multiple Authenticati page 1087 • Configuring FA Services, on page 1093 • Configuring Proxy MIP HA Failover, on page 1094 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 1095 • RADIUS Attributes Required for Proxy Mobile IP, on page 1095 • Configuring Default Subscriber Parameters in Home Agent Context, on pag

Proxy Mobile IP in 3GPP2 Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

How Proxy Mobile IP Works in 3GPP2 Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 100: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

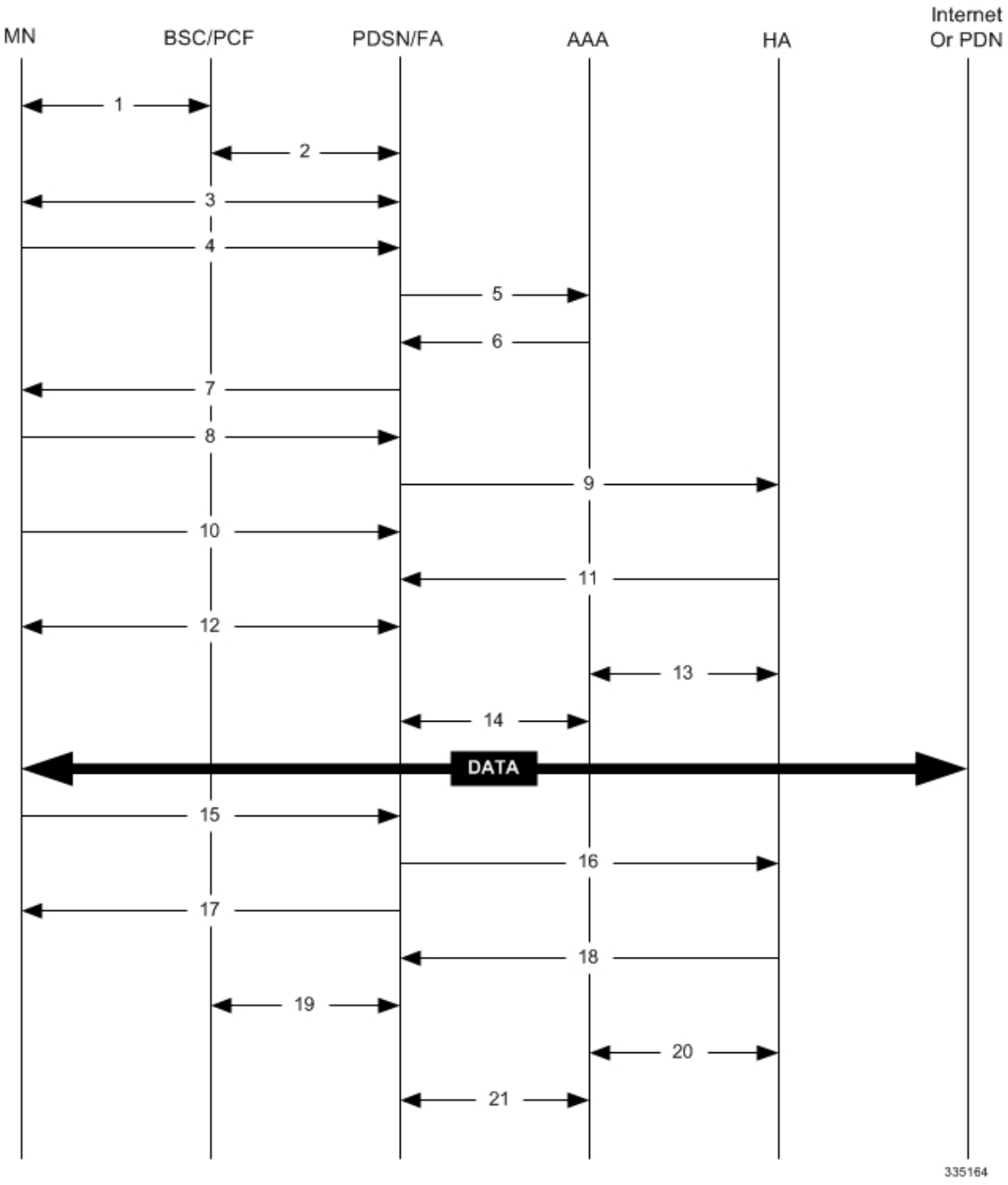


Table 105: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

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/FA establish the R-P interface for the session.

Step	Description
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's H Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fi such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (secu parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messa
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally spec by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 101: HA Assigned IP Address Proxy Mobile IP Call Flow

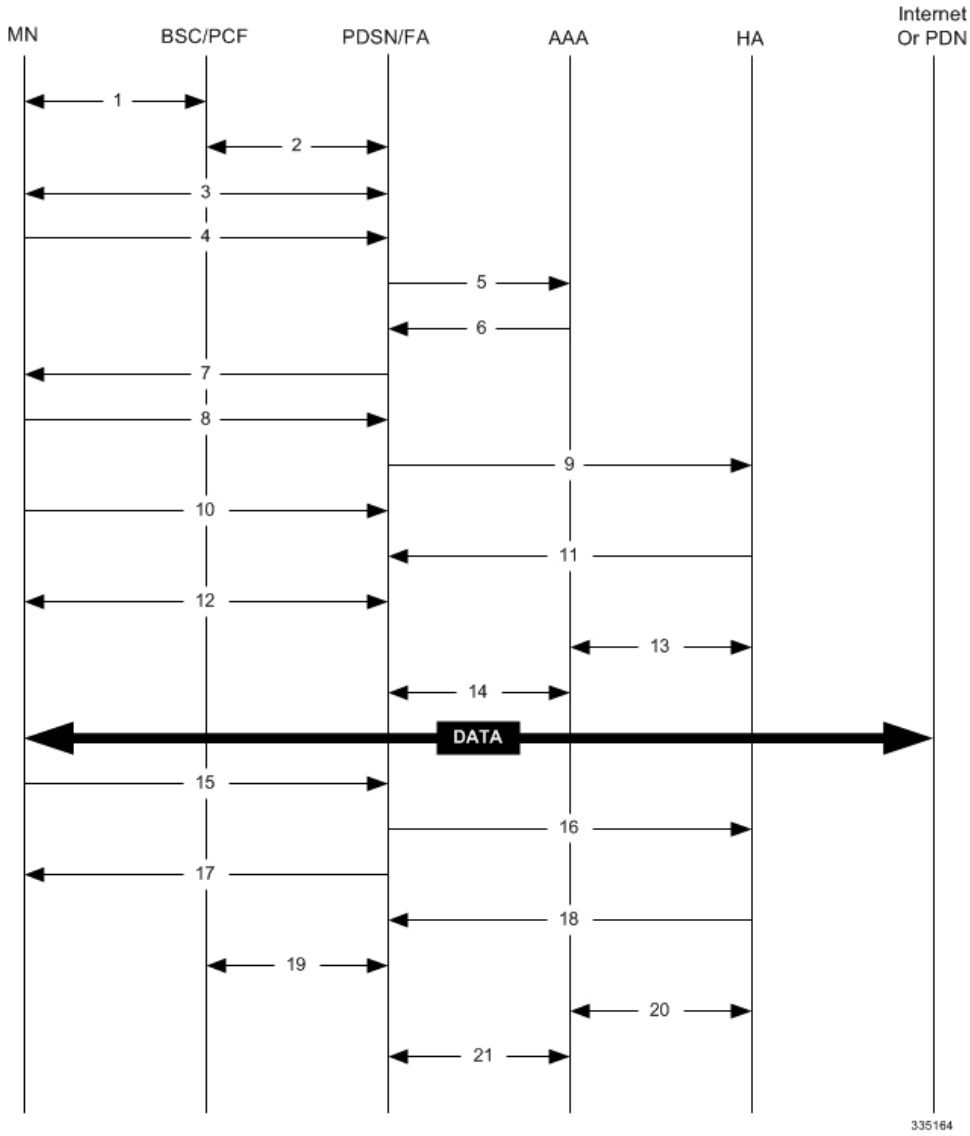


Table 106: HA Assigned IP Address Proxy Mobile IP Call Flow Description

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/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.

Step	Description
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP addr of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fi such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messa
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from o its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding re (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally spec by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network.

The following figure and the text that follows describe a a sample successful Proxy Mobile IP session setup call flow in 3GGP service.

Figure 102: Proxy Mobile IP Call Flow in 3GPP

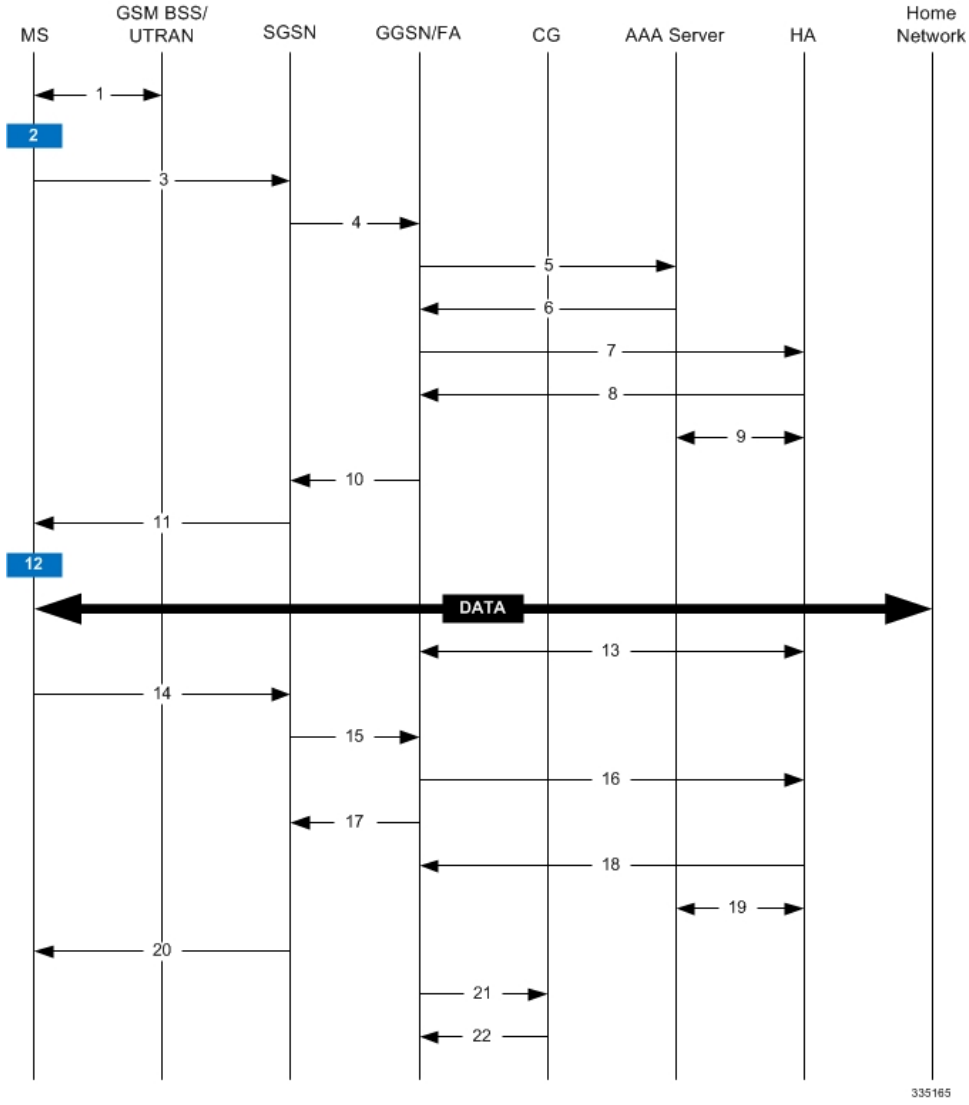


Table 107: Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

Step	Description
2	The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the to place it into PPP mode. The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentica protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), o none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authenticat information. Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Reques message to the MT. The message will either contain a static IP address to use or request that one be dynamical assigned.
3	The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Typ PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.
4	The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN us the GPRS Tunneling Protocol (GTPC, "C" indicates the control signalling aspect of the protocol). The recipien GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The messag consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, a tunnel endpoint identifier (TEID, if the PDP Address was static).
5	The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) creates a new entry in its PDP context list and provides a Charging ID for the session. From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authentic if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact. Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the u profile supersede APN settings. If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored i memory or send a RADIUS Access-Request message to a AAA server.
6	If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Ac message indicating successful authentication and any attributes for handling the subscriber PDP context.
7	If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forward Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the h home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter in (SPI)).
8	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from on its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding rec (MBR) for the subscriber session.
9	The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10	The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or th address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options spec by the GGSN.

Step	Description
11	The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to configuration parameters sent in the initial request.
12	The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. The MS can now send and receive data to or from the PDN until the session is closed or times out. Note th Mobile IP, only one PDP context is supported for the MS.
13	The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA s responses for each request.
14	The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Request message that is received by the SGSN.
15	The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The m includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16	The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Re message to the HA.
17	The GGSN returns a Delete PDP Context Response message to the SGSN.
18	The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19	The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to
20	The SGSN returns a Deactivate PDP Context Accept message to the MS.
21	The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTI (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send p CDRs while the PDP context is active.
22	For each accounting message received from the GGSN, the CG responds with an acknowledgement.

How Proxy Mobile IP Works in WiMAX Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and ASN GW/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.

Figure 103: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

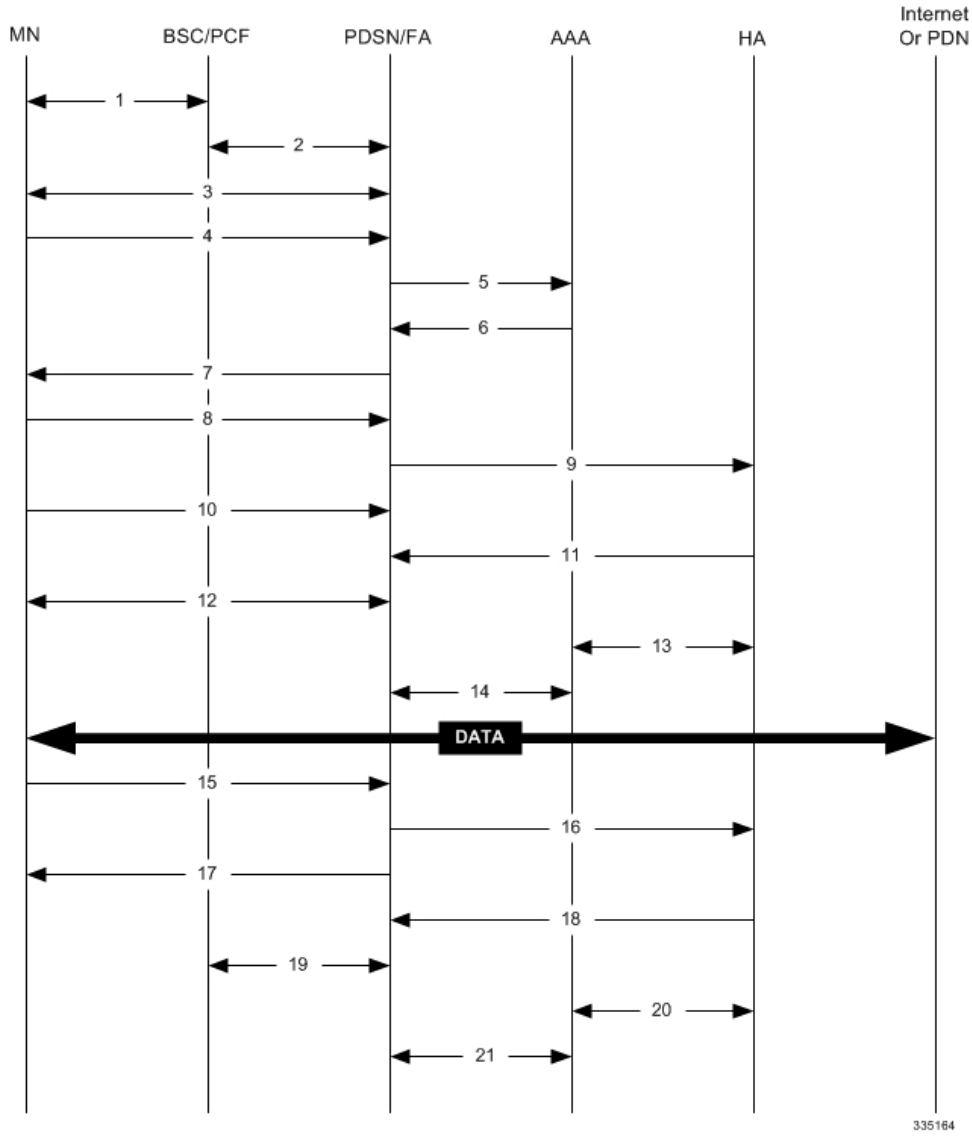


Table 108: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.

Step	Description
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the Home Address (IP address) and the IP address of the HA to use.
7	The ASN GW/FA sends a EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN G with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includ such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request m
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address orig specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully estal the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end subscriber session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interfac
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 104: HA Assigned IP Address Proxy Mobile IP Call Flow

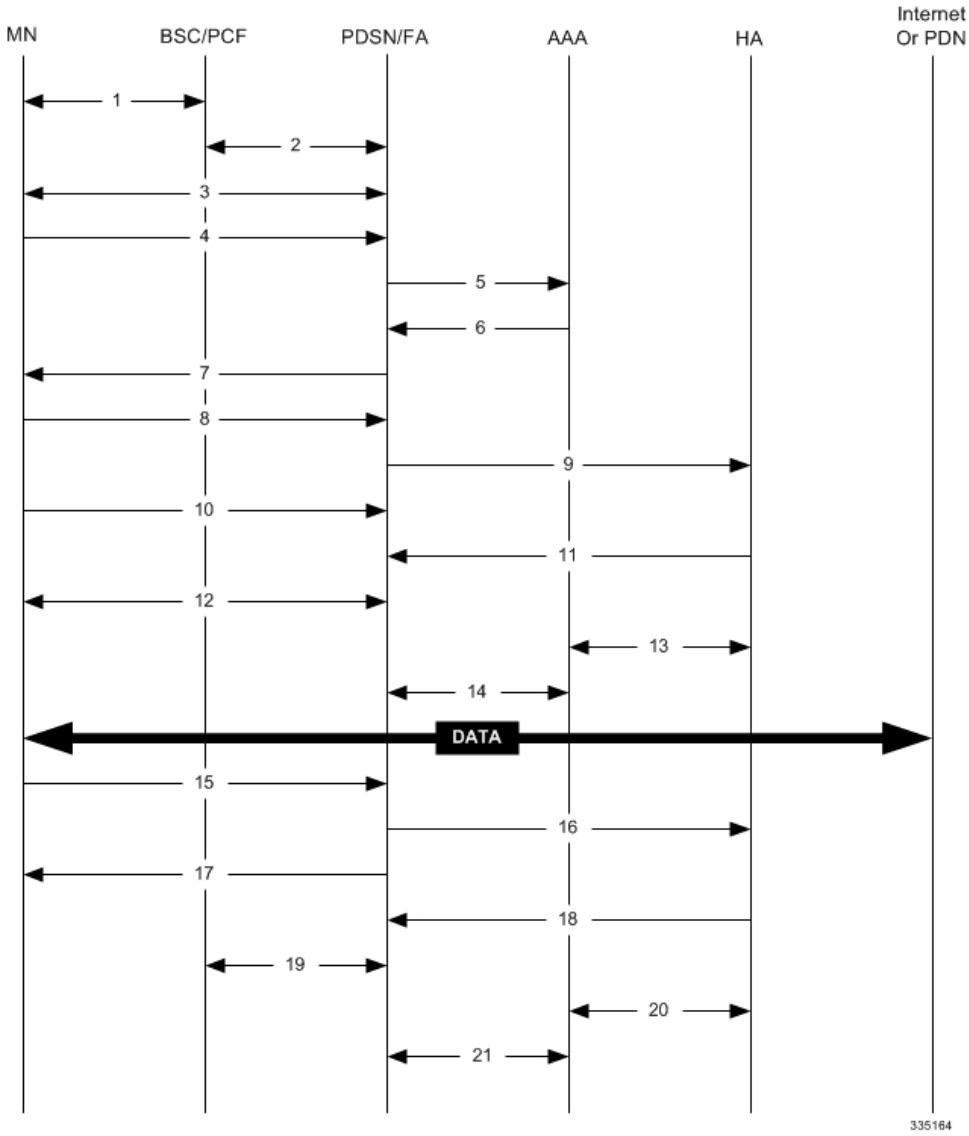


Table 109: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.

Step	Description
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP of the HA to use.
7	The ASN GW/FA sends an EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN G with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includ such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request m
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address fro its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address orig specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully estal the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end subscriber session.
16	The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interfac
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers.

Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool.The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.

Figure 105: Proxy-MIP Call Setup using CHAP Authentication

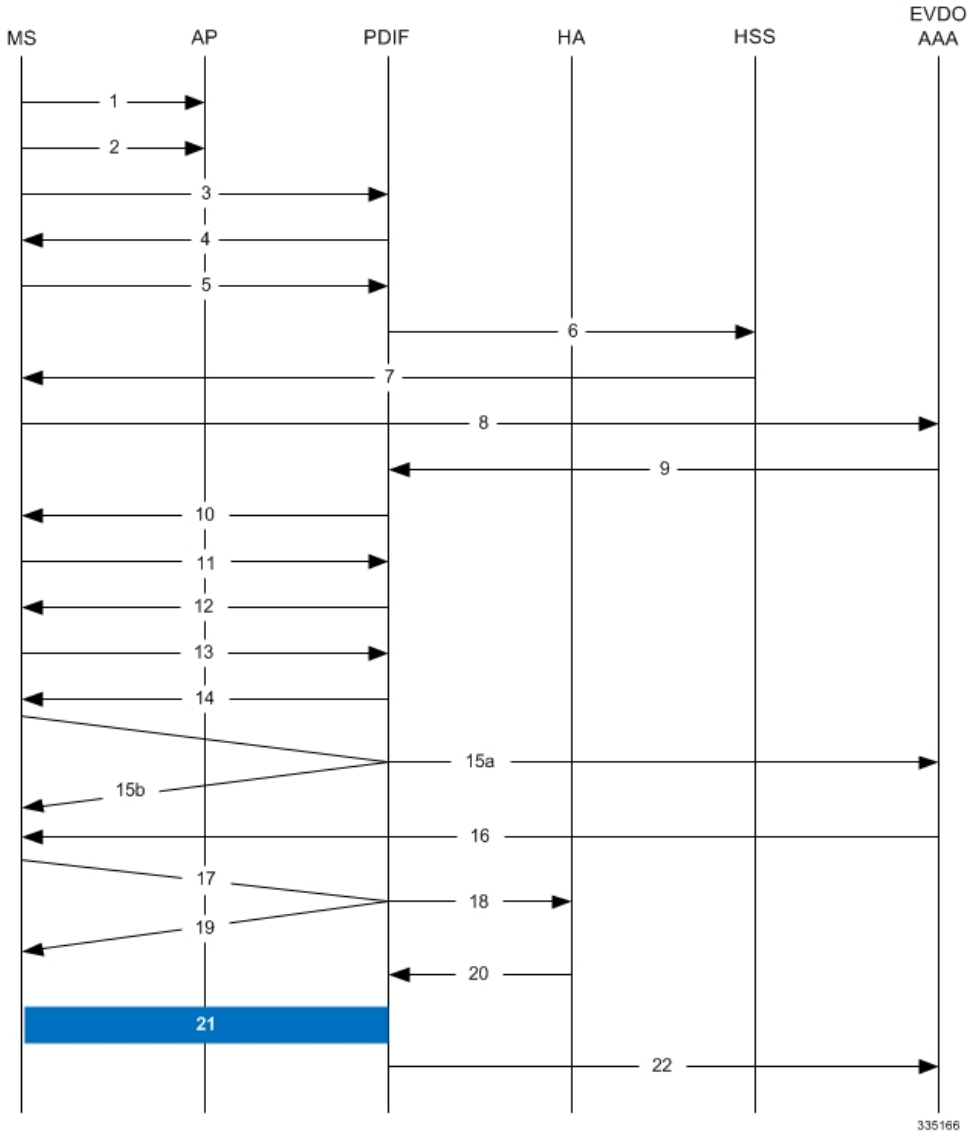


Table 110: Proxy-MIP Call Setup using CHAP Authentication

Step	Description
1	On connecting to WiFi network, MS first send DNS query to get PDIF IP address
2	MS receives PDIF address from DNS
3	MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.

Step	Description
4	PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP ad in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDI service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Respo PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.
5	On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload w contains the NAI, SA, TSi, TSr, CP (requesting IP address and DNS address) payloads. MS will not inclu AUTH payload to indicate that it will use EAP methods.
6	On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA se are selected based on domain profile, default subscriber template or default domain configurations. PDIF incl Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details ar explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Re from MS.
7	PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Pay AVP contents and sends IKE_ AUTH Response back to MS in the EAP payload. PDIF allows IDr and CE configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is config to do so.
8	MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AU Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challe received from MS.
9	The AAA server sends the DEA back to the PDIF with Result-Code AVP as "success." The EAP-Payload message also contains the EAP result code with "success." The DEA also contains the IMSI for the user, w is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.
10	PDIF sends the IKE_AUTH Response back to MS with the EAP payload.
11	MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed fro keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS No payload also.

Step	Description
12	PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH paylo computed from the MSK. PDIF does not assign any IP address for the MS pending second authenticati will the PDIF include any configuration payloads. a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 se sending INFORMATIONAL (Delete) Request.b. If ANOTHER_AUTH_FOLLOWS Notify payload is present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. H if **proxy-mip-required** is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ PDIF receives the Proxy-MIP RRP, it takes the Home Address (and DNS addresses if any) and sends t IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. I case, IKEv2 setup will finish at this stage and IPSec tunnel gets established with a Tunnel Inner Addres
13	MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include th This NAI may be completely different from the NAI used in the first authentication.
14	On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second auther methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP metho be either EAP-Passthru or EAP-Terminated. a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload in challenge.b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP- MS processes the IKE_AUTH Response: • If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the ch compute the response and send IKE_AUTH Request with EAP payload including Challenge and R • If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the M legacy-Nak with EAP-GTC.
15(a)	PDIF receives the new IKE_AUTH Request from MS. If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.).
15(b)	If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_A Response with EAP-GTC.
16	PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.
17	PDIF receives the final IKE_AUTH Request with AUTH payload.
18	PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Ag **proxy-mip-required** is enabled. The HA address may be received from the RADIUS server in the Acces (Step 16) or may be locally configured. PDIF may also remember the HA address from the first auther received in the final DEA message.
19	If **proxy-mip-required** is disabled, PDIF assigns the IP address from the local pool.
20	PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.
21	PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by in the CP payload with the IP address and optionally the DNS addresses. This completes the setup.

Step	Description
22	PDIF sends a RADIUS Accounting start message.

Important For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.

Figure 106: Proxy-MIP Call Setup using PAP Authentication

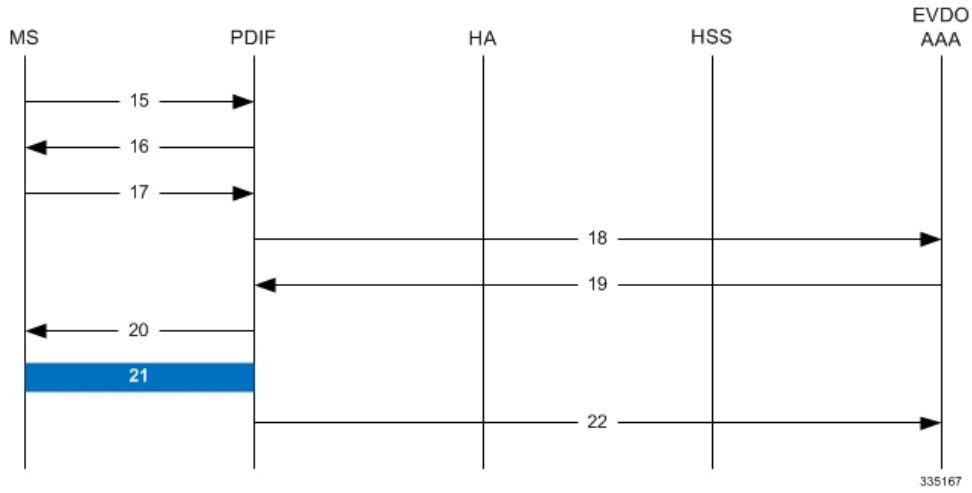


Table 111: Proxy-MIP Call Setup using PAP Authentication

Step	Description
15	MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.
16	PDIF then initiates EAP-GTC procedure, and requests a password from MS.
17	MS includes an authentication password in the EAP payload to PDIF.
18	Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Na attribute and PAP-password.
19	Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may inc Framed-IP-Address attribute.
20	The attribute content in the Access Accept message is encoded as EAP payload with EAP success when P sends the IKE_AUTH Response to the MS.
21	The MS and PDIF now have a secure IPSec tunnel for communication.
22	Pdif sends an Accounting START message.

Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:

Important Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip allow
 proxy-mip max-retransmissions <integer>
 proxy-mip retransmission-timeout <seconds>
 proxy-mip renew-percent-time percentage
 fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number
 { encrypted secret enc_secret | secret secret } [ description string ][
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | replay-protection {
timestamp | nonce } | timestamp-tolerance tolerance ]
authentication mn-ha allow-noauth
 end
```

Notes:

- The **proxy-mip max-retransmissions** command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- **proxy-mip retransmission-timeout** configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.

- **proxy-mip renew-percent-time** configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of **600** seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after **300** seconds have passed.

- Use the **fa-ha-spi remote-address**command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the *Command Line Interface Reference* for the full command syntax.



Important Note that FA-HA SPIs **must** be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the **authentication mn-ha allow-noauth** command to configure the FA service to allow communications from the HA without authenticating the HA.

Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- 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*.

Proceed to the optional Configuring Proxy MIP HA Failover, on page 1094 to configure Proxy MIP HA Failover support or skip to the *Configuring HA Services* to configure HA service support for Proxy Mobile IP.

Configuring Proxy MIP HA Failover

Use this example to configure Proxy Mobile IP HA Failover:



Important This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:

```
configure
 context <context_name>
```

```
fa-service <fa_service_name>
proxy-mip ha-failover [ max-attempts <max_attempts> |
num-attempts-before-switching <num_attempts> | timeout <seconds> ]
```

Notes:

- 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 Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

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.

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

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.

RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

Table 112: Required RADIUS Attributes for Proxy Mobile IP

Attribute	Description	Values
SN-Subscriber- Permission OR SN1-Subscriber-Permission	Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute **must** be set to Simple IP.	• None (0) • Simple IP (0x01) • Mobile IP (0x02) • Home Agent Termina Mobile IP (0x04)

Attribute	Description	Values
SN-Proxy-MIP OR SN1-Proxy-MIP	Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute **must** be enabled to support Proxy Mobile IP.	• Disabled - do not perform compulsory Proxy-MIP (• Enabled - perform compul Proxy-MIP (1)
SN-Simultaneous-SIP-MIP OR SN1-Simultaneous-SIP-MIP	Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services. **Note** Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will **not** allow simultaneous Simple IP and Mobile IP sessions for the MN.	• Disabled (0) • Enabled (1)
SN-PDSN-Handoff-Req-IP-Addr OR SN1-PDSN-Handoff-Req-IP-Addr	Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.	• Disabled - do not reject (• Enabled - reject (1)
3GPP2-MIP-HA-Address	This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.	IPv4 Address

Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

```
configure
 context <context_name>
 subscriber name <subscriber_name>
 permission pdsn-simple-ip
 proxy-mip allow
 inter-pdsn-handoff require ip-address
 mobile-ip home-agent <ha_address>
 <optional> mobile-ip home-agent <ha_address> alternate
 ip context-name <context_name>
 end
```

Verify that your settings for the subscriber(s) just configured are correct.

```
show subscribers configuration username <subscriber_name>
```

Notes:

- Configure the system to enforce the MN\'s use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the **inter-pdsn-handoff require ip-address** command.
- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the **mobile-ip home-agent** *ha_address* alternate command to specify the secondary, or alternate HA.
- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- 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 Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

```
configure
 context <context-name>
 subscriber name <subscriber_name>
 proxy-mip require
```

Note

subscriber_name is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

```
configure
 context <context_name>
 ip context-name <context_name>
 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 APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.



Important This is an optional configuration. In addition, attributes returned from the subscriber's profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

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

```
[local]host_name
```

Procedure

Step 1 Enter the 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 system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.The following prompt appears:

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

Step 3 Enter the configuration mode for the desired APN by entering the following command:

apn <*apn_name*>

apn_name is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).The following prompt appears:

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

Step 4 Enable proxy Mobile IP for the APN by entering the following command:

proxy-mip required

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

Step 5 *Optional.* GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:

proxy-mip null-username static-homeaddr

This command will enables the accepting of MIP Registration Request without NAI extensions in this APN.

Step 6 Return to the root prompt by entering the following command:

end

The following prompt appears:

```
[local]host_name
```

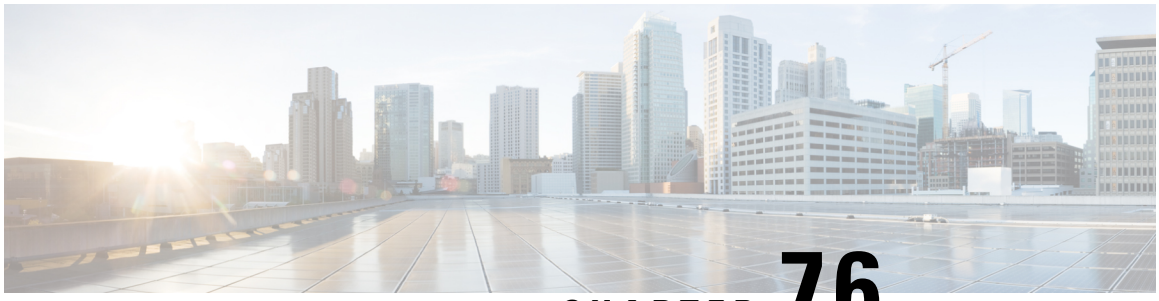
Step 7 Repeat *step 1* through *step 6* as needed to configure additional APNs.

Step 8 Verify that your APNs were configured properly by entering the following command:

show apn { all | name <*apn_name*> }

The output is a detailed listing of configured APN parameter settings.

Step 9 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*.



CHAPTER 76

Sessmgr Restart While Processing Secondary RAT Usage CDR Records

- Feature Summary and Revision History, on page 1099
- Feature Changes, on page 1100
- Command Changes, on page 1100

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• P-GW Administration Guide • Command Line Interface Reference

Revision History

Revision Details	Release
In this release, a new CLI command *limit-secondary-rat-usage* is introduced to limit the RAT usage report in CDR.	21.23
In this release, a new CLI command *limit-secondary-rat-usage* is introduced to limit the RAT usage report in CDR.	21.21.3

Revision Details	Release
First Introduced	21.19.7

Feature Changes

Previous Behavior: Session Manager (SessMgr) is restarted while Charging Data Record (CDR) process is triggered. The restart occurs when the buffer reaches 64K bytes with different stacks.

New Behavior: In thisStarOS 21.21.3 release and StarOS 21.23 release, the SessMgr restart can be avoided by limiting the number of Secondary Radio Access Technology (RAT) usage reports in CDR to a maximum of 32 records. A new CLI command limit-secondary-rat-usage is introduced to limit the Secondary RAT usage report in CDR.



Note By default, limit-secondary-rat-usage is disabled. This CLI is not applicable for CUSTOM38 dictionary.

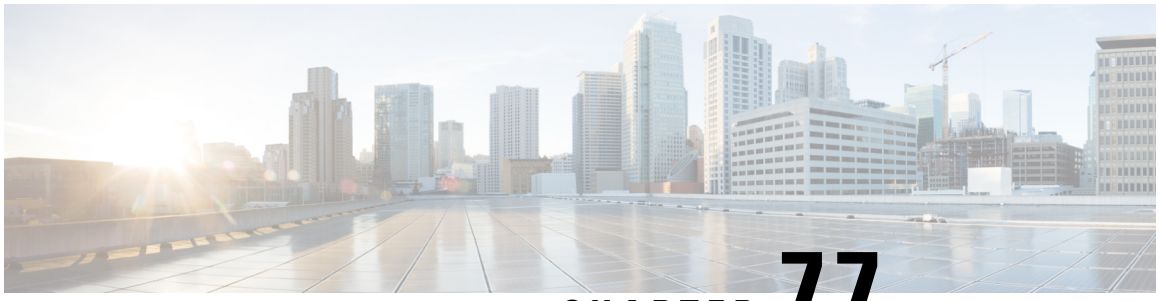
Command Changes

Use the following CLI configuration to limit the Secondary RAT Usage in CDR.

```
configure
   context context_name
   gtpp group group_name
      [no] limit-secondary-rat-usage
      end
```

NOTES:

- **limit-secondary-rat-usage**: Enables limiting the number of Secondary RAT Usage reports in CDR.
- **no**: Disables limiting the number of Secondary RAT Usage reports in CDR.



CHAPTER 77

APN, QCI, and ARP-based DSCP Mapping for WPS Sessions

- Feature Summary and Revision History, on page 1101
- Feature Description, on page 1102
- How it Works, on page 1104
- Configuring IMS Authorization Service for WPS, on page 1108
- Configuring DSCP Mapping, on page 1109
- Monitoring and Troubleshooting, on page 1112

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

The APN, QCI and ARP-based DSCP Mapping for WPS Sessions feature enables P-GW and S-GW to support DSCP marking based on APN, QCI and ARP functionality for Wireless Priority Service subscribers.

Prioritization of Control Plane Traffic: WPS user's control plane traffic is prioritized over other subscribers between different Network Functions in the LTE Core.

Priority Levels: P1, P2, and P3 are the three priority levels available for WPS users:

- P1 and P2 users are identified in HSS/PCRF and GW uses their priority (APN, QCI, and ARP) during default and dedicated bearer creation, modification, update, or deletion.
- P1 and P2 WPS users are always treated as High Priority.
- DSCP markings for prioritized user's control plane IP packets is marked with DSCP=47 while all other users control packets IP packets is marked with DSCP=32.
- Non-WPS users and P3 WPS users (for example, with QCI=5 and ARP PL =5) are given high priority dynamically based on a call being placed. Example: WPS-P1 user calling non-WPS user.
- For the LTE Core, the indication of higher priority for a user comes over Rx based on the presence of MPS-Identifier-AVP and value of Service-Info-Status-AVP in the Rx-AAR. PCRF takes appropriate actions and then propagates appropriate QCI, ARP values over to P-GW on Gx session.

Diameter Interfaces:

- P-GW, Policy Change Rule Function (PCRF), and Diameter Routing Agent (DRA) uses the configuration of Diameter interfaces such as Gx and Rx interfaces to support policy and charging control for subscribers.

Non-Diameter Interfaces: P-GW and S-GW uses non-diameter interfaces such as S5, S8, S11, or S1U with its peer respectively.

Characteristics of Low and High Priority Channels for Diameter based Interfaces

Low Priority channels are used for non-WPS user sessions and High Priority channels are used for WPS user sessions. These channels are identified by different Differentiated Services Code Point (DSCP) markings. The peer connections towards DRA for PGW (Gx) isshown in the figure.

Figure 107: High-Level Overview of Low and High Priority Channels over Gx Interface

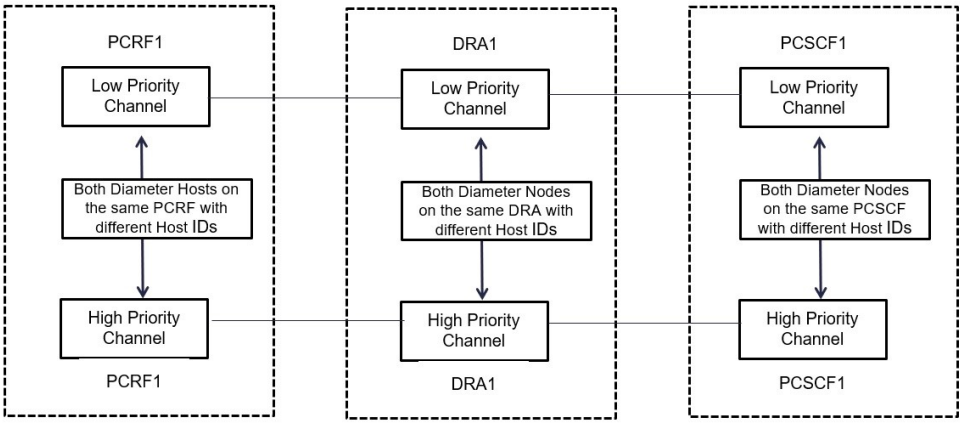


Table 113: Low and High Priority Channels on Gx Interface

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	Gx	Equal to 32	32 **Note** This channel is for non-WPS diameter messages but may carry WPS diameter messages in error scenarios, for example when all the Red Peers are down.	Not Modified Examples: 0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1
High Priority	Gx	Equal to 47	47	Specific to High Priority Examples: 0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

Characteristics of Low Priority and High Priority Channels for S11, S5, or S8 interfaces

The S5 and S11 interfaces are GTPv2 based (which uses UDP as the transport protocol), Low and High Priority channels have the following characteristics.

Table 114: Low and High Priority Channels on Other Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	S11 or S5 or S8	32	—	—
High Priority	S11 or S5 or S8	47	—	—

How it Works

The following is a high-level overview of how this feature works.

The P-GW/S-GW selects either High Priority or Low Priority channels based on the wps profile. The following table describes the DSCP marking rules based on the configured APN name, QCI values, and ARP PL in the default or any of the dedicated bearer of a session. WPS session detection is based on the configured APN name, QCI and ARP PL values in the default or dedicated bearer of a session. The S5, S8 and S11 interface contain IP packets marked with DSCP=47 IP based on APN, QCI, and ARP PL parameters as shown in the table. Other IP packets are marked with DSCP=32.

Table 115: WPS Message Prioritization based on APN, QCI, and ARP Priority Level

APN Name	QCI	ARP PL	DSCP
APN-x/APN-y/*	66,69	*	47
APN-x/APN-y/*	*	1,2	47
APN-x/APN-y/*	8	3	47
APN-x/APN-y/*	9	5	47
APN-x/APN-y/*	2	4	47

The following table explains the process of dynamic transport selection based on transaction or Origin Host:

Table 116: Procedure

Process	Description
Identifying WPS and Non-WPS users	• Use the CLI command **priority-select** at diameter end point to enable or disable WPS users. This CLI command is at policy-control configuration in IMS-authorization service. • P-GW receives Create session request with every WPS session is tagged with the APN name, QCI, and ARP PL values. • P-GW verifies whether that APN name, QCI, and ARP PL value is matching the WPS. • Session Manager checks whether the received ARP PL value matches the WPS session or not. • If the above criteria of matching WPS session and enabling of priority select is met then, the user is called as WPS user. Else, the user is called as Normal user.
Prioritizing Session	At Policy Change Rule Function (PCRF) you can define two priority levels such as Low Priority session for non-WPS users and high priority session for WPS users. • **Always-On WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belongs to WPS users are always treated as high priority. • **On-Demand WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to Non-WPS users can be uplifted to higher priority (lower ARP PL value) dynamically. The most common example of this is when a WPS user makes a WPS call (that is initiated by dialing a call starting with *272) to non-WPS user. These types of sessions are called On-Demand WPS sessions. • Control plane Gx messages belonging to high priority sessions shall use High Priority channels. • Control plane Gx messages belonging to non-high priority sessions shall use low priority channels.

Process	Description
Differentiating paths between normal users and WPS users	On Gx interface, different connections are made to form the second path at the CLI level: • P-GW creates two sets of DRA peer connections. One set for higher priority and other for normal priority messages. • P-GW sends CCR-Initial and CCR-Update Gx messages on specific pair of connections based on type of session (WPS session or non WPS session). • After the peer is configured with priority-select flag, all CCR messages for WPS session is initiated over High Priority peer. if P-GW identifies the users as a WPS user it will bind to the high priority peer with DSCP marking as 47. However, non WPS subscriber's Diameter message is initiated over Low Priority peer and the DSCP is set to 32. **Note** If the DSCP configuration for peer is not specified, then global dscp value configured under diameter endpoint is used. If global dscp value under diameter endpoint is not configured, then dscp value "0" is used. The following actions are performed before triggering CCR-I message with respect to WPS users: • Selection of High Priority peer. • If an existing AVP string is configured in peer configuration, Origin Host ID is appended with a string. If string is not configured, default **-wps** string is appended to Origin Host ID. • DRA/PCRF responds with CCA-I over high priority channel upon reception of the CCR-I. The subsequent messages follow the high priority channel.

Call Flow

The key call flow for this feature include transitioning from non-WPS to WPS Session and PCRF initiated Bearer Deletion.

If CSR (Creation Session Request) has one bearer and ARP PL, QCI does not match with ARP PL, QCI defined in WPS profile for corresponding APN, the Session is treated as Non-WPS Session. All Gx messages follow low priority channel to PCRF. However, if any dedicated bearer triggered by Mobile has ARP PL, QCI matched with ARP PL, QCI in WPS profile for corresponding APN , low priority session is transitioned to WPS session.



Note "Green peer" is "Low priority channel". "Red peer" is "High priority channel"

Figure 108: Transitioning from Non-WPS to WPS Session and Vice Versa

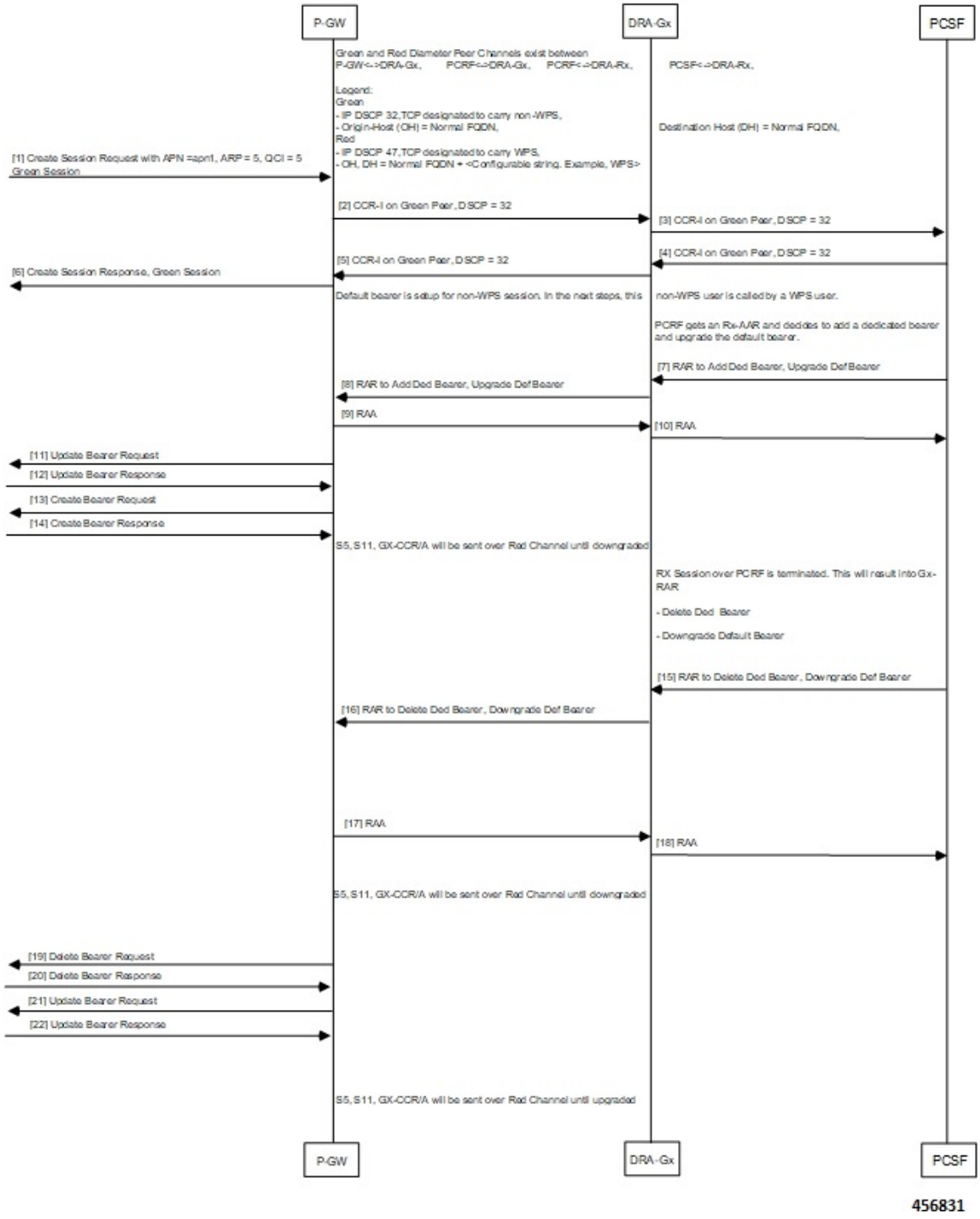


Table 117: Procedure

Step	Description
1 through 6	Low Priority channels are used for a non-WPS session.
7 through 14	P-GW receives dedicated bearer with APN, ARP PL, QCI matched with ARP PL in WPS APN profile, the following operations are performed, and CCR-U is sent to DRA/PCRF. • Non-WPS session is transitioned to WPS session. CLP is updated as WPS session. • P-GW Identifies high priority peer. • Appends the String "-wps" or configured origin-host-suffix string to Origin host ID. The subsequent outgoing messages on Gx, S5, S11, or S8 will follow the high priority channel until the session is downgraded again.
15 through 22	P-GW receives RAR with QCI or ARP PL that are not defined in WPS APN profile, the session is downgraded from WPS session to non-WPS.

Configuring IMS Authorization Service for WPS

Use the following sample configuration 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 priority-select
            diameter dictionary dictionary
            no event-report-indication
            custom-reauth-trigger  qos-change default-bearer-qos-change
ue-ip-addr-allocate resource-modification-request  ue-ip-addr-release
apn-ambr-mod-failure default-bearer-qos-mod-failure
            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  ] ] priority-host [ -noconfirm
]
            exit
         exit
```

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.

- 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.
- **priority-select**: Enables Wireless Priority Services (WPS) for subscribers. This is a mandatory parameter to define peer as Red peer.



Note **priority-select** keyword is used under IMSA as well as under 'diameter endpoint' configuration. Both must be enabled for current feature to work.

- **priority-host**: Configures host as red host. If priority-host keyword configured in a row, both primary and secondary peers are treated as red host .



Note To remove this keyword, configure **no-priority-host**.

Configuring DSCP Mapping

This section describes how to configure the DSCP mapping:

- Configuring a WPS APN Profile.
- Associating an WPS profile with P-GW and S-GW service
- Enabling Gx Prioritization for WPS Sessions
- Differentiating Low Priority and High Priority Peers

Configuring WPS APN Profile

Use the following commands to configure WPS APN profile, which is used to identify a bearer or session as an WPS bearer or session.

```
configure
     wps-apn-profile  wps_apn_name
     [ no ] wps-apn-row row_number qci qci_value earp arp_pl_value dscp dscp_value
end
```

NOTES:

- **wps-apn-profile** *wps_apn_name*: Configures WPS profile for an APN. This APN name is used for wps session detection. **wps-apn-profile all** is used when this WPS APN Profile is to be applied for all APNs.



Important Different **wps-apn-profile** must be defined for different APNs.

- **wps-apn-row**: This configuration is used for marking a bearer/PDN as an WPS. QCI and eARP PL are used for wps session detection. You can configure maximum of 16 rows and an integer value from 1 to16.

  For the **qci and earp**, **all** is the wild card match.

- **dscp**: This configuration is used at S-GW or P-GW, to mark various outgoing GTP-C and Gx messages associated with an WPS PDN with configured DSCP marking. The dscp value is an integer between 1..63.

Associating WPS APN Profiles with P-GW and S-GW Services

This section describes how to associate a WPS APN profile with P-GW and S-GW services.

```
configure
   context  context_name
      [ no ] pgw-service service_name
         [ no ] associate wps-apn
         end
```

Notes:

- **no**: Disables WPS APN profile association with P-GW service.
- **associate wps-apn**: Associates WPS APN profile with P-GW service.

```
configure
   context context_name
      [ no ] sgw-service  service_name
         [ no ] associate wps-apn
         end
```

Notes:

- **no**: Disables WPS APN profile association with S-GW service.
- **associate wps-apn**: Associates WPS APN profile with S-GW service.

Enabling Gx Prioritization for WPS Sessions

This section describes how to enable Gx prioritization levels for WPS sessions

```
configure
   context context_name
      [ no ]ims-auth-service service_name
         [ no ] policy control
             [ no ] diameter origin endpoint  endpoint_name  priority-select
             [ no ] diameter session-prioritization
            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  ] ]  priority-host [ -noconfirm
]
        end
```

Notes:

- **priority-select**: Enables Wireless Priority Services (WPS) for the selected IMS authorization service.

Note The **priority-select** keyword is mandatory for WPS feature.

- **no diameter session-prioritization**: Enables or disables Gx signalling prioritization for WPS sessions:
  - By default, the **diameter session-prioritization** CLI command is disabled and Gx messages does not get prioritized based on WPS value.
  - If previously configured, use the **no diameter session-prioritization** CLI command to set the default behavior
  - The **diameter session-prioritization** CLI takes effect when Gx, along with WPS APN profile, is enabled in the configuration.
  - The **diameter session-prioritization**configuration attaches DRMP-0 AVP to Diameter Messages going over the High Priority channel. DRA/PCRF takes appropriate actions based on DRMP-0, incase of fallback from High Priority to Low Priority channel takes place on P-GW to DRA or DRA to PCRF Gx links.

Note Diameter session-prioritization is an existing CLI and it is not mandatory for configuring WPS feature.

- **priority-host**: Configures host as red host. If priority-host keyword configured in a row, both primary and secondary peers are treated as red host.

Differentiating Low Priority and High Priority Peers

This section describes how to differentiate between low and priority peers. Priority-endpoint configuration under policy-control ensures WPS feature is only applicable to IMS auth service under policy control area. It is applicable for Gx interface

```
configure
   context context_name
      [ no ] diameter endpoint pgw-gx
        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 ] priority-select dscp dscp_value origin-host-suffix
suffix_name
          end
```

NOTES:

- **priority-select**: Defines peer as high priority wps peer. It is optional to configure to both parameters. Following conditions apply during peer configuration:
  - If **priority-select** is not configured, peer will not be treated as high priority **WPS** peer.

- If no DSCP at peer is configured, endpoint level DSCP is filled in IP packets towards DRA/PCRF. Otherwise, configured DSCP is filled in IP packet.
- If Priority-select is set and **origin-host-suffix** is configured in peer, configured string is added to Origin Host ID. Otherwise, default "-wps" string is added to origin host id (for example, pgw-gx-wps).
- **dscp**: DSCP can also be configured on low priority peer. The dscp value is a integer between 1..63.

Monitoring and Troubleshooting

This section describes troubleshooting information, show commands and Outputs, IMSA level statistics, eGTPC statistics, and Bulk statistics.

Show Commands and Outputs

show ims-authorization policy-control statistics

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics

Field	Description
DPCA WPS Session Stats	
Total Current Sessions	The total number of DPCA WPS session currently running on this system
Switched from Priority Chnl	Indicates the total subscribers moved from Wireless Priority to Normal
Switched to Priority Chnl	Indicates the total subscribers moved from Normal to Wireless Priority
DPCA WPS Message Stats	
Priority Channel Indicates message statistics for WPS session, which is sent or received on high priority channel.	
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
Total CCA	Total Credit Control Answer (CCA) messages sent in response to CCRs.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.

Field	Description
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message.
CCA-Update Dropped	Total number of CCA-U messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end sessions.
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end sessions but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages, which are dropped due to S-GW restoration, DPCA is off ,or not present, or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization..
RAA	Total number of Re-Auth-Requests(RARs) answered with Re-Auth-Answer (RAA) message.

Field	Description
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.
Non-Priority Channel	**Indicates message statistics for WPS session, which is supposed to be sent/received on Priority channel but sent/received on Non-priority channel**
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages which are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message
CCA-Update Dropped	Total number of CCA-U messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end session/s..

Field	Description
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end session/s but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization.
RAA	Total number of Re-Auth-Requests (RARs) answered with Re-Auth-Answer (RAA) message.
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.

show diameter peers full all

Use this CLI command to view peer details.

Counters	Description
Priority Channel	Indicates peer is high priority or not. The options are: • Yes: Indicates peer is WPS. • No: Indicates peer is non-WPS.

show wps-apn-profile{all | name wps_apn_profile_name}

View a particular or all WPS APN profile(s) configured with its associated attributes.

show pgw-service { name <name> | all }

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn profile** associated with P-GW service or not. The options are Yes and No.

You can view similar output field information for the **show sgw-service { name <name> | all }** command.

show pgw-service { name_*name* | all }

The output of this command is modified to reflect the WPS APN profile associated with the P-GW service.

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn** profile associated with pgw service or not. The options are **Yes** and **No**.

show sgw-service { name_*name* | all }

The output of this command is modified to reflect the WPS APN profile associated with the S-GW service.

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn** profile associated with sgw service or not. The options are **Yes** and **No**.

show subscribers pgw-only full all

The output of this command is modified to reflect whether the session is WPS or not.

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show sgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show subscribers sgw-only full all

The output of this command is modified to reflect whether the session is WPS or not

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show subscribers saegw-only full all

The output of this command is modified to reflect whether the session is WPS or not.

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show pgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show sgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show saegw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	

Field	Description
Colocated PDNs	Displays the WPS PDN statistics information for collapsed PDNs.
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN PGW-Anchor WPS PDNs. Displays the WPS PDN statistics information for P-GW-Anchor PDNs.
PGW-Anchor WPS PDNs: Displays the WPS PDN statistics information for PGW-Anchor PDNs.	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN PGW-Anchor WPS PDNs. Displays the WPS PDN statistics information for P-GW-Anchor PDNs.
SGW-Anchor WPS PDNs: Displays the WPS PDN statistics information for SGW-Anchor PDNs.	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show egtpc statistics interface pgw-ingress interface-type S5/S8

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S5/S8 interface of P-GW Ingress.

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by P-GW when it receives Create session request message on S5/S8 interface that makes session as WPS.

Counter	Description
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Create session response message on the S5/S8 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by P-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer request message on the S5/S8 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Update Bearer response message on the S5/S8 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by P-GW when it receives Create session request message on S5/S8 interface that makes a session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Create session response message on the S5/S8 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer request message on the S5/S8 interface.
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Update Bearer response message on the S5/S8 interface.

show egtpc statistics interface sgw-egress interface-type S5/S8

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S5/S8 interface of S-GW Egress.

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S5/S8 interface that makes session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S5/S8 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by S-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S5/S8 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S5/S8 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S5/S8 interface that makes a session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S5/S8 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S5/S8 interface.

Counter	Description
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S5/S8 interface.

show egtpc statistics interface sgw-ingress interface-type s11

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S11 interface of S-GW Ingress

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on the S11 interface that makes session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S11 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S11 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by S-GW when it transmits Modify Bearer response message on the S11 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S11 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S11 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S11 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S11 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S11 interface that makes a session as WPS.

Counter	Description
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S11 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S11 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Modify Bearer response message on the S11 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S11 interface.
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S11 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S11 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S11 interface.

clear egtpc

The following CLI commands are modified to clear WPS statistics at interface level and eGTP-C service level:

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**: Clears interface statistics along with WPS statistics for all eGTP-C services of P-GW Ingress type and S5/S8 interface.
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s11 | sgw-s5s8]** : Clears interface statistics along with WPS statistics for all eGTP-C services of S-GW Ingress type and S11 interface/S-GW Egress type and S5/S8 interface.
- **clear egtpc statistics egtp-service pgw_egtpc_service_name interface [s5s8]** : Clears interface statistics along with WPS statistics for all P-GW eGTP-C services and S5/S8 interface.
- **clear egtpc statistics egtp-service sgw_egptc_service_name interface [s11 | sgw-s5s8]** : Clears interface statistics along with WPS statistics for all S-GW eGTP-C services and S11 or S5/S8 interface.

Bulk Statistics

This section provides information on the bulk statistics in support of the QCI and ARP based DSCP mapping feature.

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users.

Counters	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca-imsa-total-sessions-switched-from-priority-channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca-imsa-total-sessions-switched-to-priority-channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.

PGW Schema

The following bulk statistics are included in the P-GW Schema.

Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of P-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of P-GW PDNs that were either released or degrades to a non-WPS PDN.

SGW Schema

The following bulk statistics are included in the S-GW Schema.

Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of S-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of S-GW PDNs that were either released or degrades to a non-WPS PDN.

SAEGW Schema

The following bulk statistics are added in the SAEGW schema to support Bulk Statistics Variables.

Counters	Description
pgw-anchor-pdns-wps-cumulative-activated	Shows the total number of P-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
pgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of P-GW anchored PDNs that were either released or degrades to a non-WPS PDNs.
saegw-colocated-pdns-wps-cumulative-activated	Shows the total number of SAE-GW collapsed PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
saegw-colocated-pdns-wps-cumulative-deactivated	Shows the total number of SAE-GW collapsed PDNs that were either released or degrades to a non-WPS PDN.

Counters	Description
sgw-anchor-pdns-wps-cumulative-activated	Shows the total number of S-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of S-GW anchored PDNs that were either released or degrades to a non-WPS PDN.

eGTP-C Schema

The following new bulk statistics variables are added to the eGTP-C schema in support of this feature. These statistics are only for the current bulkstat intervals.

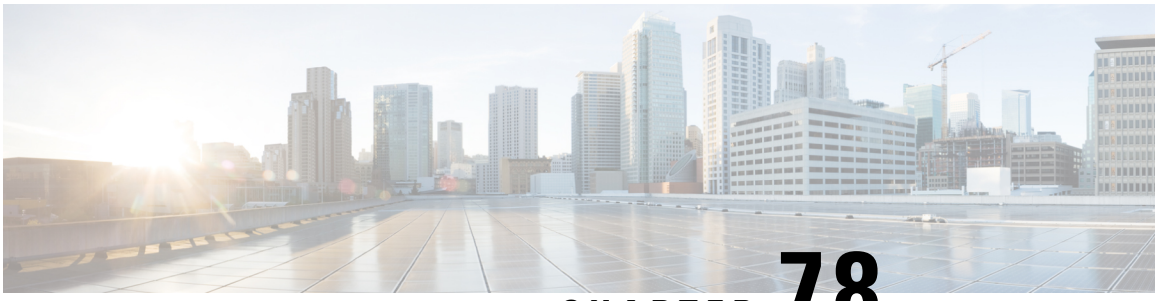
Counters	Description
s11-tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the s11 interface.
s11-tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the s11 interface.
s11-tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the s11 interface s11.
s11-tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the s11 interface .
tun-sent-cresessreq-wps	Shows the total number of tunnel create session request messages sent by the system for WPS subscriber on the s5/s8 interface .
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the s5/s8 interface.
tun-sent-updbearerresp-wps	Shows the total number of tunnel update bearer response messages sent by the system for WPS subscriber on the s5/s8 interface .

P-GW eGTP-C S5/S8 Schema

The following bulk statistics are added to the P-GW eGTP-C S5/S8 schema in support of this feature. These statistics are only for the current bulkstat intervals.

Counters	Description
tun-recv-cresessreq-wps	Shows the total number of tunnel create session request messages received by the system for WPS subscriber on the S5/S8 interface.

Counters	Description
tun-sent-cresessresp-wps	Shows the total number of tunnel create session response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the S5/S8 interface.
tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the S5/S8 interface
tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the S5/S8 interface.



CHAPTER 78

Retrieve MDN from S6b

- Feature Changes, on page 1127
- Command Changes, on page 1128
- Performance Indicator Changes, on page 1128

Feature Changes

As per the current implementation, during an initial attach, P-GW selects Mobile Directory Number (MDN) or Mobile Station International Subscriber Directory Number (MSISDN) from the S6b interface. Later, when the call is handed off from P-GW to other services like eHRPD/trusted WiFi/untrusted WiFi or the handoff is done from these services to the P-GW, then the MDN/MSISDN is picked from the create session (CS) request and the S6b authorized MDN/MSISDN is lost. As a result, different values of MDN/MSISDN are sent in the Rf records. Since, typically, operators use MDN to charge subscribers, this results in revenue loss.

This feature retains the MDN/MSISDN value from the S6b interface or the CS request, during the initial attach and even during handoff between P-GW and eHRPD/ trusted WiFi/untrusted WiFi. The MDN/MSISDN value does not change in the call lifetime. As a result, all Rf records of a session have the same MDN/MSISDN values.

A new keyword **retain-mdn** has been added to the CLI command **authorize-with-hss**. This CLI command keyword, when configured, retains the MDN/MSISDN value. If the CLI command keyword is not configured, the MDN/MSISDN value is not received from the S6b interface. In this case, the MDN/MSISDN value received in the CS request is used.

Important This feature is not applicable to GnGp handoff.

Old Behavior: MSISDN value was overwritten during handoffs between P-GW and services like eHRPD/trusted/untrusted WiFi.

New Behavior: MSISDN value is retained during the lifetime of call, including handoffs between P-GW and services like eHRPD/trusted/untrusted WiFi.

Command Changes

retain-mdn

This CLI command keyword has been added to retain the MDN/MSISDN value from the S6b interface or Create Session Request.

If the CLI command is disabled in between the handoff procedure, MDN/MSISDN value is not retained. For example, if the following CLI command is configured and the MDN/MSISDN value is authorized by S6b, then the same value is used for the call. However, if the CLI command is disabled before the handoff, the MDN/MSISDN value received in Create Session Request is used. This value might be different from the one received from the S6b interface during initial attach.

If the CLI command is not configured, the MDN/MSISDN value is not received from the S6b interface. In this case, the MDN/MSISDN value received in the create session (CS) request is used.

```
configure
     context context_name
       pgw-service service_name
          authorize-with-hss retain-mdn
          { no | default } authorize-with-hss
          end
```

Notes:

- **no:** Disables S6b authorization after the initial attach or handoff.
- **default:** Sets default configuration for **authorize-with-hss** which does not enforce the MDN after handoffs if retrieved from S6b during initial attach.
- **authorize-with-hss:**Enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface.
- **retain-mdn:** Enables MSISDN/MDN value to be retained as negotiated during the call setup (S6b retrieved MDN or CS Request MDN), for the lifetime of call (including handoffs).

Performance Indicator Changes

show pgw-service all

This command displays the following output:

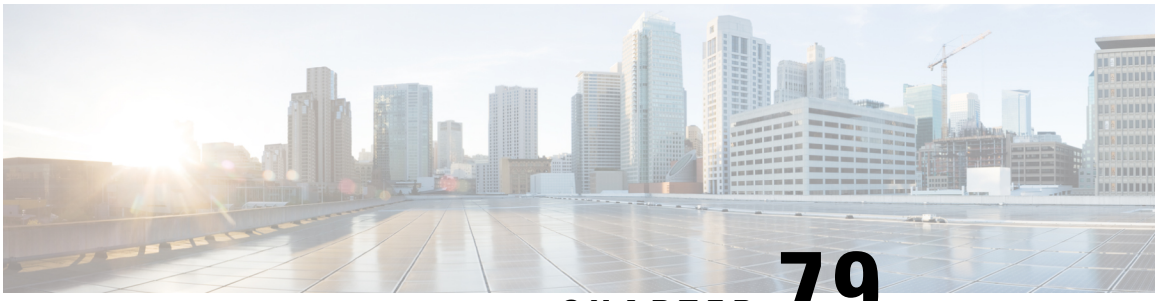
```
S6b IPv6 Reporting:     Disabled
Retain MDN :     Enabled
```

show pgw-service name *<service_name>*

This command displays the following output:

```
S6b IPv6 Reporting:     Disabled
Retain MDN :        Enabled
```

show pgw-service name <service_name>



CHAPTER 79

Revised Marking for Subscriber Traffic

- Feature Summary and Revision History, on page 1131
- Feature Description, on page 1132
- How It Works, on page 1132
- Configuring Revised Marking for Subscriber Traffic, on page 1133
- Configuring 802.1p and MPLS EXP Marking for User Data Traffic, on page 1134
- Monitoring and Troubleshooting Revised Marking for Subscriber Traffic, on page 1137

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	• Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. This feature is fully qualified in this release.	21.20.2

Revision Details	Release
In this release P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20

Feature Description

802.1p/MPLS EXP marking helps in providing QoS treatment by prioritizing traffic at L2 level.

Currently, data traffic for different access types, such as GGSN, eHRPD, P-GW, and S-GW, refer to the QCI-QoS table and configure the appropriate 802.1p or MPLS-EXP (L2 QoS) markings based on the internal-qos value associated with particular row. However, the usage of internal-qos from the QCI-QoS table is not configurable and uses the default values. In addition, L2 QoS (802.1p/MPLS EXP) marking is not supported in GGSN, SAEGW, and GTPv1/eHRPD calls on P-GW.

With this feature, you can:

- Configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls.
- Mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. A new CLI command has been introduced to support service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Limitations

- This feature does not control the behavior of the control packets. The control packets (GTP-C) continue to get L2 marked based on DSCP derived L2 marking.
- This feature is not supported on standalone GGSN. It is supported on GnGp-GGSN node.

How It Works

You can configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. You can also mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Behavior Changes for Different Services

This section describes behavior of this feature for different services. Please see the *Command Changes* section for more information on the CLI command options and its behavior:

GGSN/P-GW GTPv1 Calls:

Previous Behavior: Earlier, the traffic was not marked for data path. This was default behavior for GGSN.

New Behavior: A new CLI command has been introduced to mark the traffic based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked. When the feature is not enabled, traffic is not marked.

P-GW GTPv2, S-GW, SAEGW Calls:

Previous Behavior: The QCI-QoS mapping feature used internal-QoS for L2 marking, which in turn uses QCI-Derived marking for data traffic. This was the default behavior for P-GW, S-GW, and SAEGW calls.

New Behavior: With this feature, the traffic is marked based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked and the default behavior is executed. When the feature is not enabled, traffic is not marked.

Configuring Revised Marking for Subscriber Traffic

By default, the traffic data path is supported with GGSN.. The internal priority can be configured in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. Subscriber traffic can also be marked with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Configuring Internal Priority

To configure internal priority in the QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls, use the following service specific configuration. This command in the GGSN service configuration overrides the behavior of QCI-QOS-mapping for data packets only.

```
configure
     context context_name
        ggsn-service service_name
           internal-qos data { dscp-derived | none | qci-derived }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           end
```

Notes:

- **no:** Disables the specified functionality.
- **default:** Disables the functionality.

- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.
- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show** *service-type* **{ all | name** *service_name* **}**

Please see the *Monitoring and Troubleshooting Revised Marking for Subscriber Traffic* section for the command output.

Configuring 802.1p and MPLS EXP Marking for User Data Traffic

This section describes how to configure the 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. Configuring the feature consists of the following tasks:

1. Configure ip-dscp-iphb-mapping.
2. Configure L2-mapping
3. Configure qci-qos-mapping.
4. Associate the l2-mapping in Egress context.
5. Associate the l2-mapping in Igress context.
6. Associate internal-qos data in P-GW and S-GW service

Configure ip-dscp-iphb-mapping

Use the following example to access *QOS Profile Configuration Mode* and configure ip-dscp-iphb-mapping.

```
configure
  qos ip-dscp-iphb-mapping dscp Value  internal-priority cos  value
  end
```

Notes:

- *qos ip-dscp-iphb-mapping dscp* : Creates a QOS profile.
- **dscp** : Specify dscp mapping with Hexadecimal value between 0x0 and 0x3F.
- **internal-priority cos** : Define the Class of Service (cos) value between 0x0 and 0x7.

Configure L2-mapping

Use the following example to access *QOS L2 Mapping Configuration Mode* and configure L2 mapping.

```
configure
  qos l2-mapping-table name  { name map_table_name | system-default }
    internal-priority cos class_of_service_value color color_value [ 802.1p-value
 802.1p_value ] [ mpls-tc mpls_tc_value ]
      end
```

Notes:

- **qos l2-mapping-table name** : Maps qos from internal qos to l2 values.
- **internal-priority cos** : Maps internal QoS priority with Class of Service (COS) values.
  - *class_of_service_value*: Specify a Hexadecimal number between 0x0 and 0x7.
  - **802.1p-value** : Maps to a 802.1p value and *.802.1p_value* must be a Hexadecimal number between 0x0 and 0xF.
  - **mpls-tc** *mpls_tc_value*: Maps to an MPLS traffic class. *mpls_tc_value* must be a Hexadecimal number between 0x0 and 0x7.

Configure qci-qos

Use the following commands to configure qci-qos mapping.

```
Configure
  qci-qos-mapping  name
    qci  num [ arp-priority-level arp_value ] [ downlink [ encaps-header
 { copy-inner | dscp-marking  dscp-marking-value } ] [ internal-qos
priority  priority ] [ user-datagram dscp-marking  dscp-marking-value  ]
 ]  [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking
dscp-marking-value } ] [ internal-qos priority  priority ]  [ user-datagram
 dscp-marking  dscp-marking-value  ] ]
     end
```

Notes:

- **qci-qos-mapping** : Maps internal QoS priority with Class of Service (CoS) value.
- **quci num**: Specifies the non-standard, operator-defined QCI value to be enabled.
- **arp-priority-level** : Specifies the address retention priority (ARP) priority level.
- **downlink**: Configures parameters for downlink traffic.
- **encaps-header { copy-inner | dscp-marking** *dscp-marking-value}*: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
  - **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
  - **dscp-marking** *dscp-marking-value*: Specifies that the DSCP marking is to be defined by this keyword.

dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

- **uplink**: Configures parameters for uplink traffic.
- **internal-qos priority** *priority* : Sets the internal QoS. These get resolved in L2 values.
- **user-datagram dscp-marking** *dscp-marking-value*: Specifies that the IP DSCP marking is to be defined by this keyword.*dscp-marking-value* is expressed as a hexadecimal number from 0x00 through 0x3F.

Associate L2-mapping table

Use the following commands to associate L2 mapping table in egress context and ingress context.

```
configure
   contextegress context_name | ingress context_name
   associate l2-mapping-table { name table_name
   exit
   context ingress context_name
   associate l2-mapping-table { name table_name
   end
```

- **associate l2-mapping-table**: Maps qos from internal qos to l2 values.
- **{ name** *table_name* : Specifies the name of table to map qos from internal qos to l2 values. *table_name* must be a alphanumeric string of size 1 to 80.

Associate internal-qos-data in a P-GW and S-GW Service

Use the following commands to associate internal-qos-data in a P-GW and S-GW service.

```
configure
     context context_name
       pgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          exit
        sgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          end
```

Notes:

- **no:** : Disables the specified functionality.
- **default** : Disables the functionality.
- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.

- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Monitoring and Troubleshooting Revised Marking for Subscriber Traffic

The following section describes commands available to monitor Revised Marking for Subscriber Traffic.

Internal Priority Show Commands

The following section describes commands available to monitor Internal Priority.

show configuration

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
internal-qos data none
```

- When **internal-qos data** is configured as **qci-derived**:

```
internal-qos data qci-derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
internal-qos data dscp-ds-derived
```

- When **internal-qos data** is **not configured**:

```
no internal-qos data
```

show *service-type* { all | name *service_name* }

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:         None
```

- When **internal-qos data** is configured as **qci-derived**:

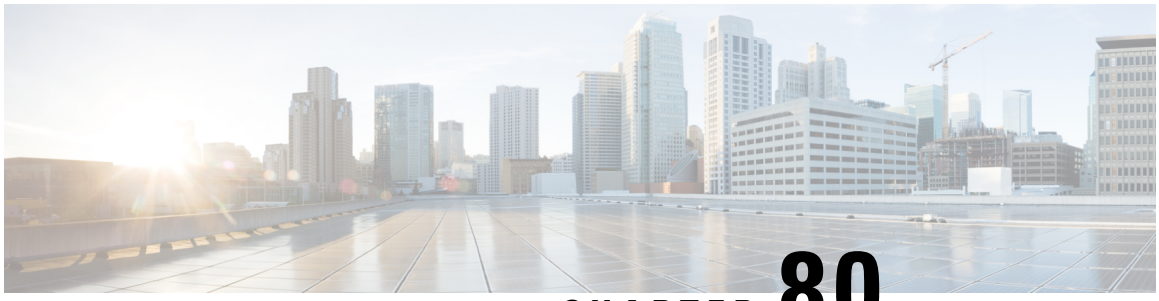
```
Internal QOS Application:   Enabled
Internal QOS Policy:        QCI Derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
 Internal QOS Application:    Enabled
 Internal QOS Policy:         DSCP Derived
```

- When **internal-qos data** is **not configured**:

```
        Internal QOS Application:     Backward-compatible
```



CHAPTER 80

Rf Interface Support

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

Rf interface support is available on the Cisco system for the following products:

- Gateway GPRS Support Node (GGSN)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)

Important The Rf interface is not supported on the S-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.

This chapter includes the following topics:

- Introduction, on page 1139
- Feature Summary and Revision History, on page 1142
- Features and Terminology, on page 1143
- How it Works, on page 1156
- Configuring Rf Interface Support, on page 1158

Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/eHRPD offline charging is based on 3GPP TS 32.299 V8.6.0, 3GPP TS 32.251 V8.5.0 and other 3GPP specifications. The Rf interface specification for IP Multimedia Subsystem (IMS) offline charging is based on 3GPP TS 32.260 V8.12.0 and 3GPP TS 32.299 V8.13.0.

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows the CTF (Diameter client) to issue offline charging events to a Charging Data Function (CDF) (Diameter server). The charging events can either be one-time events or may be session-based.

The system provides a Diameter Offline Charging Application that can be used by deployed applications to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on chassis to act as CTF to a configured CDF.

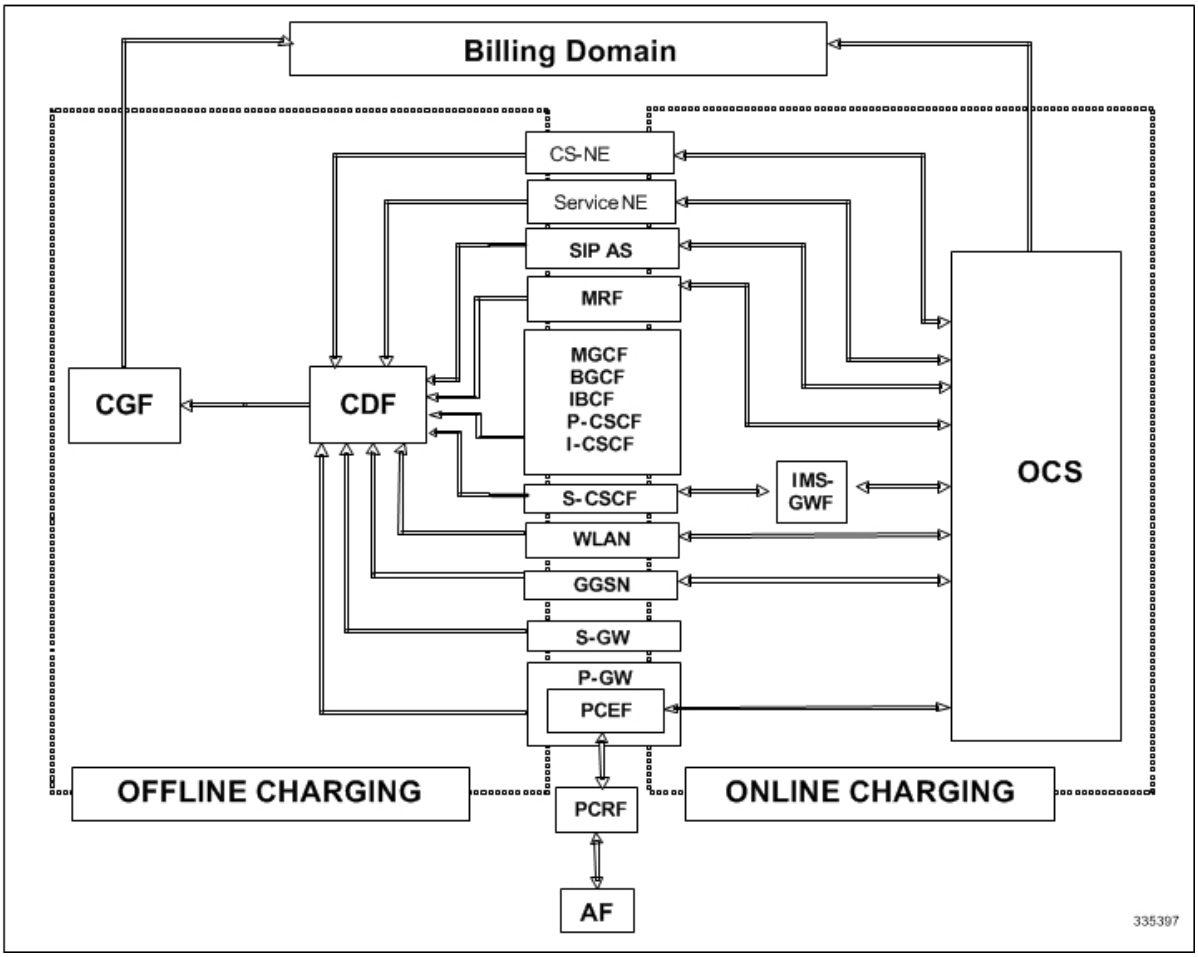
In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

The CCF with the CDF and Charging Gateway Function (CGF) will be implemented as part of the core network application. The CDF function collects and aggregates Rf messages from the various CTFs and creates CDRs. The CGF collects CDRs from the CDFs and generates charging data record files for the data mediation/billing system for billing.

Offline Charging Architecture

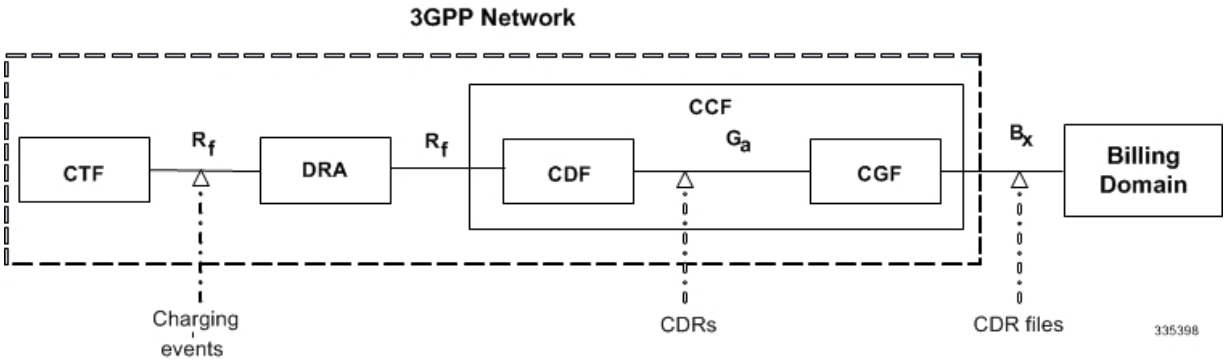
The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).

Figure 109: Charging Architecture



The following figure shows the Rf interface between CTF and CDF.

Figure 110: Logical Offline Charging Architecture



The Rf offline charging architecture mainly consists of three network elements CCF, CTF and Diameter Dynamic Routing Agent (DRA).

Charging Collection Function

The CCF implements the CDF and CGF. The CCF will serve as the Diameter Server for the Rf interface. All network elements supporting the CTF function should establish a Diameter based Rf Interface over TCP connections to the DRA. The DRA function will establish Rf Interface connection over TCP connections to the CCF.

The CCF is primarily responsible for receipt of all accounting information over the defined interface and the generation of CDR (aka UDRs and FDRs) records that are in local storage. This data is then transferred to the billing system using other interfaces. The CCF is also responsible for ensuring that the format of such CDRs is consistent with the billing system requirements. The CDF function within the CCF generates and CGF transfers the CDRs to the billing system.

The CDF function in the CCF is responsible for collecting the charging information and passing it on to the appropriate CGF via the GTP' based interface per 3GPP standards. The CGF passes CDR files to billing mediation via SCP.

Charging Trigger Function

The CTF will generate CDR records and passes it onto CCF. When a P-GW service is configured as CTF, then it will generate Flow Data Record (FDR) information as indicated via the PCRF. The P-GW generates Rf messages on a per PDN session basis. There are no per UE or per bearer charging messages generated by the P-GW.

The service data flows within IP-CAN bearer data traffic is categorized based on a combination of multiple key fields (Rating Group, Rating Group and Service -Identifier). Each Service-Data-Container captures single bi-directional flow or a group of single bidirectional flows as defined by Rating Group or Rating Group and Service-Identifier.

Dynamic Routing Agent

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a CTF to the CCF.

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one

Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

License Requirements

The Rf 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

Rf 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 (Release9)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• 5G Non Standalone Solution Guide • AAA Interface Administration and Reference • Command Line Interface Reference • MME Administration Guide • Statistics and Counters Reference

Revision History

Revision Details	Release
The StarOS 21.22 is enhanced, where an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW.	21.22

Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in 3GPP TS 32.240.

Basic Principles

The Diameter client and server must implement the basic functionality of Diameter accounting, as defined by the RFC 3588 Diameter Base Protocol.

For offline charging, the CTF implements the accounting state machine as described in RFC 3588. The CDF server implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588, i.e. there is no order in which the server expects to receive the accounting information.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the following ACR event types:

Table 118: Rf ACR Event Types

Request	Description
START	Starts an accounting session
INTERIM	Updates an accounting session
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.

Important The ACR Event Type "EVENT" is supported in Rf CDRs only in the case of IMS specific Rf implementation.

The following table describes all possible ACRs that might be sent from the IMS nodes i.e. a P-CSCF and S-CSCF.

Table 119: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE
	ISUP:ANM (applicable for the MGCF)
ACR [Interim]	SIP 200 OK acknowledging a SIP
	RE-INVITE or SIP UPDATE [e.g. change in media components]
	Expiration of AVP [Acct-Interim-Interval]
	SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE
ACR [Stop]	SIP BYE message (both normal and abnormal session termination cases)
	ISUP:REL (applicable for the MGCF)
ACR [Event]	SIP 200 OK acknowledging non-session related SIP messages, which are: • SIP NOTIFY • SIP MESSAGE • SIP REGISTER • SIP SUBSCRIBE • SIP PUBLISH
	SIP 200 OK acknowledging an initial SIP INVITE
	SIP 202 Accepted acknowledging a SIP REFER or any other method
	SIP Final Response 2xx (except SIP 200 OK)
	SIP Final/Redirection Response 3xx
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
	SIP CANCEL, indicating abortion of a SIP session set-up

Event Based Charging

In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

In this scenario, CTF asks the CDF to store event related charging data.

Session Based Charging

Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

In this scenario, CTF asks the CDF to store session related charging data.

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.

In order for the application to be compliant with the specification, state machines should be implemented at some level within the implementation.

Diameter Base supports the following Rf message commands that can be used within the application.

Table 120: Diameter Rf Messages

Command Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

There are a series of other Diameter messages exchanged 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.
- 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 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 considered 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. 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.

Timer Expiry Behavior

Upon establishing the Diameter connection, an accounting interim timer (AII) is used to indicate the expiration of a Diameter accounting session, and is configurable at the CTF. The CTF indicates the timer value in the ACR-Start, in the Acct-Interim-Interval AVP. The CDF responds with its own AII value (through the DRA), which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. An instance of the AII timer is started in the CCF at the beginning of the accounting session, reset on the receipt of an ACR-Interim and stopped on the receipt of the ACR-Stop. After expiration of the AII timer, ACR INTERIM message will be generated and the timer will be reset and the accounting session will be continued.

Rf Interface Failures/Error Conditions

The current architecture allows for primary and secondary connections or Active-Active connections for each network element with the CDF elements.

DRA/CCF Connection Failure

When the connection towards one of the primary/Active DRAs in CCF becomes unavailable, the CTF picks the Secondary/Active IP address and begins to use that as a Primary.

If no DRA (and/or the CCF) is reachable, the network element must buffer the generated accounting data in non-volatile memory. Once the DRA connection is up, all accounting messages must be pulled by the CDF through offline file transfer.

No Reply from CCF

In case the CTF/DRA does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the CTF/DRA sends the ACRs to the secondary/alternate DRA/CCF.

Detection of Message Duplication

The Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in RFC 3588.

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

CCF Detected Failure

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behavior of the CCF is operator configurable.

Rf-Gy Synchronization Enhancements

Both Rf (OFCS) and Gy (OCS) interfaces are used for reporting subscriber usage and billing. Since each interface independently updates the subscriber usage, there are potential scenarios where the reported information is not identical. Apart from Quota enforcement, OCS is utilized for Real Time Reporting (RTR), which provides a way to the user to track the current usage and also get notifications when a certain threshold is hit.

In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

When time/volume quota on the Gy interface gets exhausted, Gy triggers "Service Data Volume Limit" and "Service Data Time Limit". Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI command " **trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } }**" the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions. If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

The CLI configuration options are provided in policy accounting configuration to control the various Rf messages (ACRs) triggered for sync on this feature.

This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

Once a CCR-U was sent out over Gy interface, the containers are closed only after receiving CCA-U successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

For more information on the command associated with this feature, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

A common timer based approach is implemented for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing. Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.

Cessation of Rf Records When UE is IDLE

The P-GW is not generating Rf records when the UE was identified to be in IDLE state and not sending any data. New CLI configuration command "**session idle-mode suppress-interim**" is provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and no data is transferred.

That is, this CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

For more information on the command, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

QoS Change Scenarios

QOS_CHANGE Trigger in Rf Records During eHRPD-LTE Handoff

The SDC in the generated Rf record does not include QOS_CHANGE trigger during handoff from eHRPD to LTE.

QoS Change for Default Bearer

For a change in the QoS of default bearer, NR SDV containers will not be seen unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e. the default bearer.

Diameter Rf Duplicate Record Generation

This section describes the overview and implementation of Rf Duplicate Record Generation feature.

This section discusses the following topics for this feature:

- Feature Description, on page 1148
- Configuring Rf Duplicate Record Generation, on page 1150
- Monitoring and Troubleshooting the Rf Duplicate Record Generation, on page 1152

Feature Description

This feature is introduced to support creation and communication of duplicate Rf records to secondary AAA group servers configured for the Rf interface.

To achieve this functionality, the following configurations must be enabled –

- **aaa group** CLI command under APN to configure a maximum of 2 AAA groups - primary and secondary AAA groups, or two different endpoints for Rf Diameter accounting servers
- **diameter accounting duplicate-record** under AAA group to allow Rf duplicate record creation

The **diameter accounting duplicate-record** is a new CLI command introduced in this release for duplicating the Rf START, INTERIM and STOP accounting records.

Important This is a license-controlled CLI command. For more information, contact your Cisco account representative.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.

Important The failed duplicate records will neither be written to HDD nor added to the archival list.

There is no change in the current behavior with the primary AAA group messages. The primary AAA group is independent of the secondary AAA group, and it has multiple Rf servers configured. When the Rf servers do not respond even after multiple retries as per the applicable configuration, the Rf records are archived and stored in HDD. This behavior continues as is irrespective of the configuration of secondary aaa-group.

Secondary aaa group has a very similar configuration as the primary aaa group except that the new CLI command **diameter accounting duplicate-record** is additionally included to configure the secondary aaa-group. It is also important to note that different Diameter endpoints and a separate set of Rf servers should be provisioned for both primary and secondary AAA groups.

If all the configured servers are down, the request message will be discarded without writing it in HDD or archiving at aaamgr.

The original and duplicate Rf messages use two different aaa-groups and two different Diameter endpoints. Hence, the values for Session-ID AVP will be different. Based on the configuration of primary and secondary endpoints the values for Origin-Host, Origin-Realm, Destination-Realm, and Destination-Host AVPs may be different. Also based on the configuration under policy accounting for inclusion of virtual/gn apn name for secondary group Called-Station-ID AVP might change. All other AVPs will have the same values as with the primary aaa group Rf message.

Also, note that the values such as Acct-Interim-Interval (AII) interval received in ACA from secondary group of AAA servers will be ignored.

Relationships to Other Features

This feature can be used in conjunction with Virtual APN Truncation feature to achieve the desired results.

The Virtual APN Truncation feature is new in release 21. For more information on this feature, see the administration guide for the product you are deploying.

Limitations

The following are the limitations of this feature:

- Only one secondary AAA group can be configured per APN.
- If all the Rf peers under secondary aaa group are down and duplicate Start Record is not sent, then the duplicate Interim and Stop records will also not be sent to any of the secondary aaa group servers even though they arrived later. However if the servers are up and duplicate Start record was sent but the server

did not respond, duplicate Start will be dropped after all the retries. In this case, the duplicate Interim and Stop records may be sent out to the server.

- In cases when duplicate Start record was sent, but during duplicate Interim/Stop record generation peers were not responding/down, after all retries duplicate Interim and Stop records will be dropped and will not be written to HDD.
- Minimal impact to memory and CPU is expected due to the duplicate record generation for every primary Rf record.

Configuring Rf Duplicate Record Generation

The following section provides the configuration commands to enable the Rf duplicate record generation.

Configuring Secondary AAA Group

Use the following configuration commands to configure the secondary AAA group for receiving the duplicate Rf records.

```
configure
   context context_name
      apn apn_name
         aaa group group_name
         aaa secondary-group group_name
         exit
```

Notes:

- **aaa group** *group_name*: Specifies the AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.
- **secondary group** *group_name*: Specifies the secondary AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

Configuring Duplication of Rf Records

Use the following configuration commands to configure the system to create a secondary feed of Rf records and send them to the secondary AAA group.

```
configure
   context context_name
      aaa group group_name
         diameter accounting duplicate-record
         exit
```

Notes:

- **duplicate-record**: Sends duplicate Rf records to configured secondary AAA group. This keyword is license dependent. For more information, contact your Cisco account representative.
- The default configuration is **no diameter accounting duplicate-record**. By default, this feature is disabled.
- The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

Verifying the Rf Duplicate Record Generation Configuration

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

show configuration

show aaa group all

- or -

show aaa group *group_name*

group_name must be the name of the AAA group specified during the configuration.

This command displays all the configurations that are enabled within the specified AAA group.

The following is a sample configuration of this feature.

```
configure
   context source
      apn domainname.com
         associate accounting-policy policy_accounting_name
         aaa group group1
         aaa secondary-group group2
         exit
      aaa group group1
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint1
         diameter accounting server rf_server1 priority 1
         diameter accounting server rf_server2 priority 2
         exit
      aaa group group2
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint2
         diameter accounting duplicate-record
         diameter accounting server rf_server3 priority 3
         diameter accounting server rf_server4 priority 4
         exit
      diameter endpoint rf-endpoint1
         use-proxy
         origin host rf-endpoint1.carrier.com address 192.50.50.3
         no watchdog-timeout
         response-timeout 20
         connection retry-timeout 5
         peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
         peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
         exit
      diameter endpoint rf-endpoint2
         use-proxy
         origin host rf-endpoint2.carrier.com address 192.50.50.2
         no watchdog-timeout
         response-timeout 20
         connection retry-timeout 5
         peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
         peer rf_server4 realm domainname.com address 192.50.50.5 port 4893
end
```

Notes:

- The **diameter accounting duplicate-record** CLI is license specific. So, the corresponding license must be enabled for the CLI command to be configured.
- Both primary and secondary aaa groups are preferred to have different accounting endpoint names.

Monitoring and Troubleshooting the Rf Duplicate Record Generation

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

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration** or **show aaa group all** CLI command. If not enabled, configure the diameter accounting duplicate-record CLI command and check if it works.
- Collect the output of **show diameter aaa statistics** command and analyze the debug statistics. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.

show diameter aaa-statistics

The following statistics are added to the output of this show command for duplicate Rf records which were dropped because of the failure in sending the Accounting records instead of adding them to HDD or archival list.

- Duplicate Accounting Records Stats
  - ACR-Start Dropped
  - ACR-Interim Dropped
  - ACR-Stop Dropped

These statistics are maintained per aaamgr instance level. For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

These statistics can also be collected per group basis/server basis for duplicate records i.e. through **show diameter aaa-statistics group** <*group_name*> and **show diameter aaa-statistics server** <*server_name*> CLI commands.

Truncation of Virtual APN for Rf Records

This feature enables the truncation of Virtual APN (VAPN) returned by S6b server to be sent to Gx, Gy and Rf interfaces.

Feature Description

Currently there is no way to quickly turn on the Rf accounting to the Data Streaming Service (DSS) server per Virtual APN (S6b-VAPN) without reaching all nodes in the network and provision the Virtual APN on each of them. This feature is implemented to truncate the virtual APN name returned by S6b server with the configured standard delimiters. In this way a single configuration per node can be utilized for all enterprises based on a virtual APN. This approach will significantly reduce the size and time to provision new enterprises with the requested feature.

To achieve this functionality, a configuration is added per APN to enable truncation of S6b-VAPN and also to configure the delimiter(s) where the APN name is to be truncated. Standard delimiters like (.) and (-) are used since APN name supports only these two characters apart from the alphanumeric ones.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

AAA manager performs the truncation of the Virtual APN name based on the APN configuration and provides the correct APN profile for the truncated APN name. If the truncation is successful, the full virtual APN name will be sent to Gx, Gy and Rf interfaces.

Accounting records are required to support real-time usage notification and device management functionality. So, the **apn-name-to-be-included** CLI command is extended to enable actual APN (Gn-APN) or virtual APN (S6b returned virtual APN) name to be included in Called-Station-ID AVP in the secondary Rf accounting records (secondary server group) under policy accounting configuration. Currently, policy accounting configuration supports sending the Gn-APN/S6b-VAPN in Called-Station-ID for primary Rf server. With this CLI command, this functionality is extended for the secondary Rf server.

A new AAA attribute “Secondary-Called-Station-ID” is added to support sending Gn/Virtual APN name in the Called-Station-ID AVP for duplicate Rf records sent to secondary group Rf server.

Configuring Virtual APN Truncation for Rf Records

The following section provides the configuration commands to enable the Virtual APN Truncation feature for Rf records.

Configuring Gn-APN/VAPN for Rf Accounting

Use the following configuration commands to configure the actual APN or Virtual APN (VAPN) for Rf accounting.

```
configure
  context context_name
    policy accounting policy_name
      apn-name-to-be-included { gn | virtual } [ secondary-group { gn |
 virtual } ]
      end
```

Notes:

- **apn-name-to-be-included**: Configures the APN name to be included in the Rf messages for primary server group.
- **secondary-group { gn | virtual }**: Configures the APN name to be included in the Rf messages for secondary server group.
- **gn**: Configures the Gn APN name to be included in the Rf messages.
- **virtual**: Configures the virtual APN name to be included in the Rf messages.
- By default, the apn name to be included in Called-Station-ID AVP is Gn-APN for both primary and secondary Rf server groups.
- If the secondary group configuration is not available, the default behavior is to have Gn APN for secondary Rf group duplicate records.

Configuring Truncation of Virtual APN

Use the following configuration commands to configure the gateway to truncate the APN name returned from S6b interface.

```
configure
   context context_name
      apn apn_name
        virtual-apn { gcdr apn-name-to-be-included { gn | virtual } |
truncate-s6b-vapn delimiter { dot [ hyphen ] | hyphen [ dot ] } }
        end
```

Notes:

- For information on the existing keywords, see the *Command Line Interface Reference* guide.
- **truncate-s6b-vapn**: Allows truncation of virtual APN received from S6b at the configured delimiter character.
- **delimiter { dot [hyphen] | hyphen [dot] }**: Configures the delimiter for truncation of virtual APN received from S6b. If the CLI command is configured, the S6b returned virtual APN will be truncated at the configured delimiter.
  - **dot**: Configures the delimiter to dot (.) for truncation of S6b-VAPN
  - **hyphen**: Configures the delimiter to hyphen (-) for truncation of S6b-VAPN
- Both dot and hyphen delimiters can be configured in the same line or a new line.
- **no virtual-apn truncate-s6b-vapn**: Disables the truncation of virtual APN name. If both delimiters should be disabled at once, use the **no virtual-apn truncate-s6b-vapn** CLI command.

  If a particular delimiter needs to disabled, it should be done explicitly. For example, if the dot delimiter should be disabled, use the **no virtual-apn truncate-s6b-vapn delimiter dot** CLI command.
- By default this feature will be disabled and no delimiter will be configured.
- This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message.
- If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

Verifying the Virtual APN Truncation Configuration

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

```
show configuration apn apn_name
```

apn_name must be the name of the APN specified during the feature configuration.

This command displays all the configurations that are enabled within the specified APN name. The following is a sample output of this show command.

```
[local]st40# show configuration apn intershat
configure
   context ingress
      apn intershat
         pdp-type ipv4 ipv6
         bearer-control-mode mixed
```

```
virtual-apn truncate-s6b-vapn delimiter hyphen
end
```

Monitoring and Troubleshooting the Virtual APN Truncation

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

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration apn** *apn_name* CLI command. If not enabled, configure the **virtual-apn truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] } }** CLI command and check if it works.
- Collect the output of **show apn statistics** CLI command and analyze the debug statistics. For further assistance, contact Cisco account representative.



Important For P-GW, GGSN and SAEGW services, if the truncation of S6b returned virtual APN name fails and the virtual APN name is not configured, the call will be rejected with ‘unknown-apn-name’ cause.

show apn statistics

This show command uses the existing APN statistics to populate the truncated virtual APN name, if this feature is enabled.

show subscribers ggsn-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers pgw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers saegw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

Accounting Record Stop Location Report

Previous Behavior: When P-GW or S-GW sends new User Location Information (ULI) message in an ACR stop message to Offline Charging System (OFCS) through the Rf interface, the reported location at the end of sessions was not aligning with the expected location reporting. The location used in the Accounting Stop Record (ACR Stop) was inconsistent and during location reporting it caused an `ACR stop` interim messages rather than the location before the ACR was sent

New Behavior: In the StarOS 21.22 and later releases, an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW when Delete Session Request is received with a New ULI.

How it Works

This section describes how offline charging for subscribers works with Rf interface support in GPRS/eHRPD/LTE/IMS networks.

The following figure and table explain the transactions that are required on the Diameter Rf interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

Figure 111: Rf Call Flow for Event Based Charging

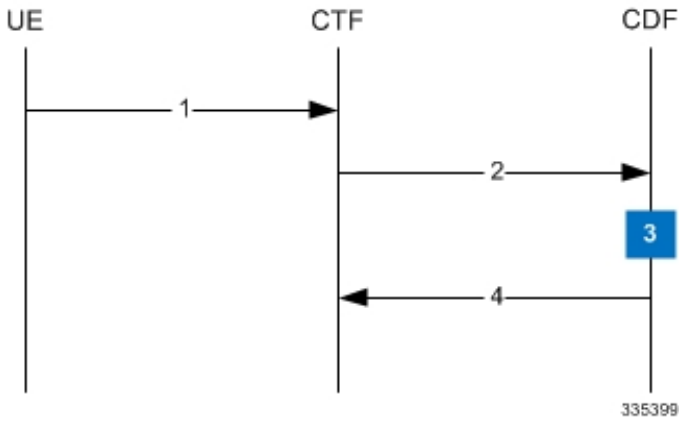


Table 121: Rf Call Flow Description for Event Based Charging

Step	Description
1	The network element (CTF) receives indication that service has been used/delivered.
2	The CTF (acting as Diameter client) sends Accounting-Request (ACR) with Accounting-Record-Type AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as Diameter server).
3	The CDF receives the relevant service charging parameters and processes accounting request.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.

The following figure and table explain the simple Rf call flow for session based charging.

Figure 112: Rf Call Flow for Session Based Charging

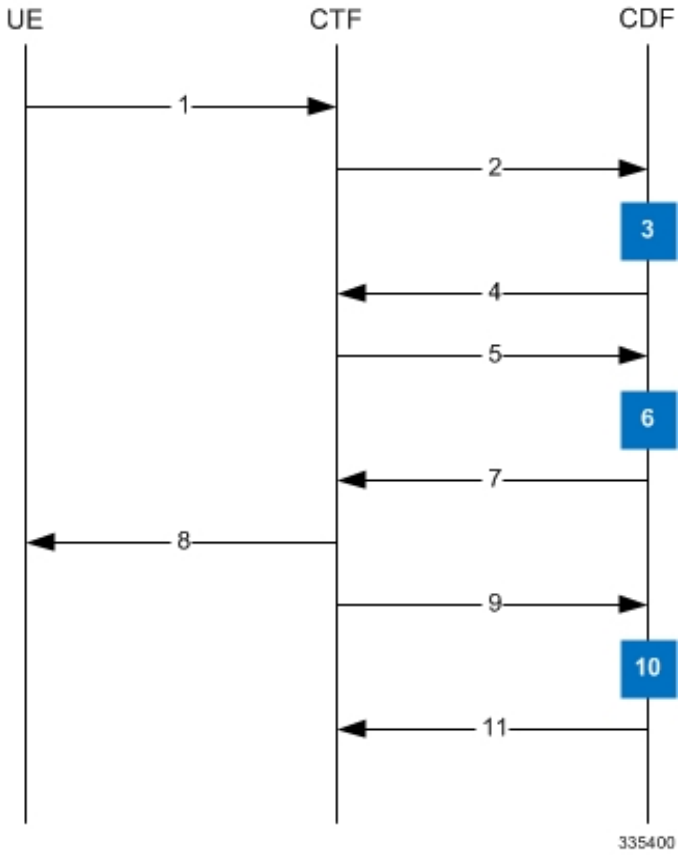


Table 122: Rf Call Flow Description for Session Based Charging

Step	Description
1	The CTF receives a service request. The service request may be initiated either by the user or the other network element.
2	In order to start accounting session, the CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to START_RECORD to the CDF.
3	The session is initiated and the CDF opens a CDR for the current session.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.
5	When either AII elapses or charging condition changes are recognized at CTF, the CTF sends an Accounting-Request (ACR) with Accounting-Record-Type AVP set to INTERIM_RECORD to the CDF.
6	The CDF updates the CDR in question.
7	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.

Step	Description
8	The service is terminated.
9	The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.
10	The CDF updates the CDR accordingly and closes the CDR.
11	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.

Configuring Rf Interface Support

To configure Rf interface support:

1. Configure the core network service as described in this Administration Guide.
2. Enable Active Charging Service (ACS) and create ACS as described in the *Enhanced Charging Services Administration Guide*.

Important The procedures in this section assume that you have installed and configured your chassis including the ECS installation and configuration as described in the *Enhanced Charging Services Administration Guide*.

3. Enable Rf accounting in ACS as described in Enabling Rf Interface in Active Charging Service, on page 1159.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN / P-GW Rf Interface Support, on page 1159
   - Configuring P-CSCF/S-CSCF Rf Interface Support, on page 1166

Important In StarOS versions 19 and later, the Rf interface is not supported on the S-GW.

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.

Enabling Rf Interface in Active Charging Service

To enable the billing record generation and Rf accounting, use the following configuration:

```
configure
   active-charging service <service_name>
      rulebase <rulebase_name>
         billing-records rf
         active-charging rf { rating-group-override | service-id-override
 }
         end
```

Notes:

- Prior to creating the Active Charging Service (ACS), the **require active-charging** command should be configured to enable ACS functionality.
- The **billing-records rf** command configures Rf record type of billing to be performed for subscriber sessions. Rf accounting is applicable only for dynamic and predefined ACS rules.

  For more information on the rules and its configuration, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- The **active-charging rf** command is used to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

  For more information on this command, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring GGSN / P-GW Rf Interface Support

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

```
configure
   context <context_name>
      apn <apn_name>
         associate accounting-policy <policy_name>
         exit
      policy accounting <policy_name>
         accounting-event-trigger { cgi-sai-change | ecgi-change |
flow-information-change | interim-timeout | location-change | rai-change
 | tai-change } action { interim | stop-start }
         accounting-keys qci
accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
         cc profile index { buckets num | interval seconds | sdf-interval
seconds | sdf-volume { downlink octets { uplink octets } | total octets |
uplink octets { downlink octets } }  | serving-nodes num | tariff time1 min
hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets
 } | total octets | uplink octets { downlink octets } } }
         max-containers { containers | fill-buffer }
         end
```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting levels/policies/modes/event triggers, refer to the *Accounting Policy Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- Depending on the triggers configured, the containers will either be cached or released. In the case of GGSN/P-GW, the containers will be cached when the event trigger is one of the following:
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
  - SERVING_NODE_CHANGE
  - SERVICE_IDLE
  - SERVICE_DATA_VOLUME_LIMIT
  - SERVICE_DATA_TIME_LIMIT
  - IP_FLOW_TERMINATION
  - TARIFF_CHANGE

  If the event trigger is one of the following, the containers will be released:
  - VOLUME_LIMIT
  - TIME_LIMIT
  - RAT_CHANGE
  - TIMEZONE_CHANGE
  - PLMN_CHANGE



Important Currently, SDF and flow level accounting are supported in P-GW.

The following assumptions guide the behavior of P-GW, GGSN and CCF for Change-Condition triggers:

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 123: P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/e-HRPD/GGSN

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Normal Release	YES	NO	YES	Normal Release	Normal Release	When PDN/IP session closed, C-C in both le will have Normal Release.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Normal Release	YES	NO	NO	N/A	Normal Release	Flow is closed, SD is populated and c container is added record. The contai this change condit will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
Stop	Abnormal Release	YES	NO	YES	Abnormal Release	Abnormal Release	When PDN/IP ses closed, C-C in bot will have Abnorm Release.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Abnormal Release	YES	NO	NO	N/A	Abnormal Release	Flow is closed, SD is populated and c container is added record. The contai this change condit will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	QoS-Change	YES	NO	NO	N/A	QoS-Change	The container for change condition cached by the P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Volume Limit	YES	YES	NO	Volume Limit	Volume Limit	For PDN/IP Session Volume Limit. The Volume Limit is configured as part of t Charging profile and t Charging-Characterist AVP will carry this charging profile that w passed on from the HSS/AAA to P-GW/GGSN through various interfaces. Th charging profile will b provisioned in the HS
Interim	Time Limit	YES	YES	NO	Time Limit	Time Limit	For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging-Characterist AVP will carry this charging profile that w passed on from the HSS/AAA to P-GW/GGSN through various interfaces. Th charging profile will b provisioned in the HS
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Serving Node Change	YES	NO	NO	N/A	Serving Node Change	The container for this change condition will cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.
Interim	Serving Node PLMN Change	YES	YES	NO	Serving Node PLMN Change	Serving Node PLMN Change	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	User Location Change	YES	NO	NO	N/A	User Location Change	This is BSID Char eHRPD. The conta for this change con will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
Interim	RAT Change	YES	YES	NO	RAT Change	RAT Change	
Interim	UE Timezone Change	YES	YES	NO	UE Timezone change	UE Timezone change	This is not applica eHRPD.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Tariff Time Change	YES	NO	NO	N/A	Tariff Time Change	Triggered when Ta Time changes. Tar Time Change requ online charging si change. The implementation of Change Condition dependent on implementation of Online Charging u
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Idled Out	YES	NO	NO	N/A	Service Idled Out	Flow Idled out. Th container for this c condition will be c by the P-GW/GGS the container will ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Volume Limit	YES	NO	NO	N/A	Service Data Volume Limit	Volume Limit reached for a specific flow. Th container for this char condition will be cach by the P-GW/GGSN a the container will be i ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Time Limit	YES	NO	NO	N/A	Service Data Time Limit	Time Limit reached fo a specific flow. The container for this char condition will be cach by the P-GW/GGSN a the container will be i ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Max Number of Changes in Charging Conditions	YES	YES	NO	YES	YES, Will include SDC that correponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volunme Limt, Service Data Time Limit)	This ACR[Interim triggered at the ins when the Max Nu of changes in char conditions takes p Max Change Cond is applicable for QoS-Change, Service-Idled Out change, Flow Nor Release, Flow Abr Release, Service D Volume Limit, Ser Data Time Limit, Timer ACR Interi Service Node Char only. The Max Nu of Changes in Cha Conditions is set a Example assuming flow in the PDN Se [1] Max Number o Changes in Charg Conditions set at P-GW/GGSN = 2. Change Condition takes place. No AC Interim is sent. P-GW/GGSN stor SDC. [3] Change Condition 2 takes An ACR Interim i Now Max Numbe Changes in Charg conditions is popu in the PS-Informa Service-Data-Con (1 for each change condition) are pop in the ACR Interi CCF creates the pa record.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Management Intervention	YES	NO	YES	YES	YES	Management intervent will close the PDN session from P-GW/GGSN.
Interim	-	YES	NO	NO	N/A	N/A	This is included here indicate that an ACR[Interim] due to timer will contain one more populated SDC/ for a/all flow/s, but Change-Condition AV will NOT be populate

Configuring P-CSCF/S-CSCF Rf Interface Support

To configure P-CSCF/S-CSCF Rf interface support, use the following configuration:

```
configure
   context vpn
      aaa group default
         diameter authentication dictionary aaa-custom8
         diameter accounting dictionary aaa-custom2
         diameter accounting endpoint <endpoint_name>
         diameter accounting server <server_name> priority <priority>
         exit
      diameter endpoint <endpoint_name>
         origin realm <realm_name>
         use-proxy
         origin host <host_name> address <ip_address>
         peer <peer_name> address <ip_address>
         exit
      end
```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference*.

Gathering Statistics

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

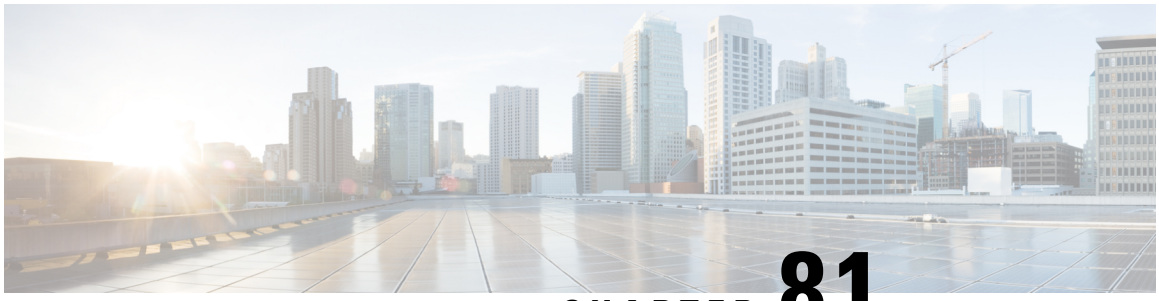
In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for Diameter Rf accounting sessions	**show diameter aaa-statistics**

The following is a sample output of the **show diameter aaa-statistics** command:

```
Authentication  Servers Summary
 ------------------------------
Message Stats :
  Total MA Requests:            0        Total MA Answers:             0
  MAR - Retries:                0        MAA Timeouts:                 0
  MAA - Dropped:                0
  Total SA Requests:            0        Total SA Answers:             0
  SAR - Retries:                0        SAA Timeouts:                 0
  SAA - Dropped:                0
  Total UA Requests:            0        Total UA Answers:             0
  UAR - Retries:                0        UAA Timeouts:                 0
  UAA - Dropped:                0
  Total LI Requests:            0        Total LI Answers:             0
  LIR - Retries:                0        LIA Timeouts:                 0
  LIA - Dropped:                0
  Total RT Requests:            0        Total RT Answers:             0
  RTR - Rejected:               0
  Total PP Requests:            0        Total PP Answers:             0
  PPR - Rejected:               0
  Total DE Requests:            0        Total DE Answers:             0
  DEA - Accept:                 0        DEA - Reject:                 0
  DER - Retries:                0        DEA Timeouts:                 0
  DEA - Dropped:                0
  Total AA Requests:            0        Total AA Answers:             0
  AAR - Retries:                0        AAA Timeouts:                 0
  AAA - Dropped:                0
  ASR:                          0        ASA:                          0
  RAR:                          0        RAA:                          0
  STR:                          0        STA:                          0
  STR - Retries:                0
Message Error Stats:
  Diameter Protocol Errs:       0        Bad Answers:                  0
  Unknown Session Reqs:         0        Bad Requests:                 0
  Request Timeouts:             0        Parse Errors:                 0
  Request Retries:              0
Session Stats:
  Total Sessions:               0        Freed Sessions:               0
  Session Timeouts:             0        Active Sessions:              0
STR Termination Cause Stats:
  Diameter Logout:              0        Service Not Provided:         0
  Bad Answer:                   0        Administrative:               0
  Link Broken:                  0        Auth Expired:                 0
  User Moved:                   0        Session Timeout:              0
  User Request:                 0        Lost Carrier                  0
  Lost Service:                 0        Idle Timeout                  0
  NAS Session Timeout:          0        Admin Reset                   0
  Admin Reboot:                 0        Port Error:                   0
  NAS Error:                    0        NAS Request:                  0
  NAS Reboot:                   0        Port Unneeded:                0
  Port Preempted:               0        Port Suspended:               0
  Service Unavailable:          0        Callback:                     0
  User Error:                   0        Host Request:                 0
 Accounting Servers Summary
 --------------------------
Message Stats :
  Total AC Requests:            0         Total AC Answers:            0
```

```
  ACR-Start:                    0       ACA-Start:                    0
  ACR-Start  Retries :          0       ACA-Start  Timeouts:          0
  ACR-Interim:                  0       ACA-Interim:                  0
  ACR-Interim  Retries :        0       ACA-Interim  Timeouts:        0
  ACR-Event:                    0       ACA-Event:                    0
  ACR-Stop :                    0       ACA-Stop:                     0
  ACR-Stop  Retries :           0       ACA-Stop  Timeouts:           0
  ACA-Dropped :                 0
AC Message Error Stats:
  Diameter Protocol Errs:       0       Bad Answers:                  0
  Unknown Session Reqs:         0       Bad Requests:                 0
  Request Timeouts:             0       Parse Errors:                 0
  Request Retries:              0
```



CHAPTER 81

Routing Behind the Mobile Station on an APN

The routing behind the Mobile Station(MS) feature enables the routing of packets to IPv4 addresses that do not belong to the PDN Session (the MS), but exist behind it. The network address of the destination can be different than the Mobile Station address.

This chapter includes the following topics:

- Feature Description, on page 1169
- How It Works, on page 1169
- Configuring Routing Behind the Mobile Station, on page 1170
- Monitoring and Troubleshooting the Routing Behind the Mobile Station, on page 1174

Feature Description

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message. Framed-Route can work at a context level or VRF level. VRFs can be on per enterprise and each can have its own set of framed-routes. In such configuration, framed routes will be installed in VRF's dedicated for respective enterprise. Association of Framed-Route with VRF will be done based on subscriber IP pool.

Mobile Router enables a router to create a PDN Session which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the "mobile router." If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN session.

How It Works

Routing Behind the Mobile Station on an APN

The following rules apply:

- AAA interface of GGSN/P-GW supports receiving "Framed Route AVP" in Radius Access-Accept Message from the Radius Server.
- AAA interface of GGSN/P-GW supports maximum 16 "Framed Route AVP" in Radius Access-Accept Message

- GGSN/P-GW does not accept framed route with destination address as 0.0.0.0 and/or netmask as 0.0.0.0.
- GGSN/P-GW does not accept framed route where gateway address in the route is not matching with the address that would be assigned to Mobile station.
- GGSN/P-GW ignores duplicate framed routes.
- GGSN/P-GW supports controlling enabling/disabling of this feature through CLI in APN Configuration.
- GGSN/P-GW supports controlling number of framed-routes to be installed through this feature.
- GGSN/P-GW supports controlling number of hosts (addresses) supported behind the mobile station per route.
- The routing behind an MS is supported only for IPv4 PDP contexts.
- Packets routed behind the MS share the same 3GPP QoS settings of the MS.

Configuring Routing Behind the Mobile Station

The routing behind the MS feature enables the routing of packets to IPv4 addresses that do not belong to the PDN Session (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- The Framed-Route (attribute 22) as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the profile of a user and contain at least one route, and up to 16 routes for each MS that is to use the routing behind the MS feature.

  When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the RADIUS authentication and authorization phase of the PDN Session creation. If routing behind the MS has not been enabled using the network-behind-mobile command in access-point configuration mode, the GGSN ignores the Framed-Route attribute.

  When the MS session is no longer active, the routes are deleted.
- Static routes are not configured. The configuration of the routing behind the mobile station feature (Framed Route, attribute 22) and static routes at the same time is not supported.

Configuration Overview

To enable routing behind a Mobile Station perform the following steps:

Procedure

Step 1 Create an APN Profile. Refer to Creating an APN Profile, on page 1171.

Step 2 Enable or disable a Network behind Mobile Station for APN. Refer to Enabling Routing Behind the Mobile Station, on page 1171.

Creating an APN Profile

Use the following example to create an APN profile on the P-GW/SAEGW/S-GW:

```
config
   context context_name
      apn apn_name
      end
```

Notes:

- The apn name must be an alphanumeric string from 1 to 64 characters in length.
- Once you have created an APN profile, you will enter the Access Point Profile Configuration Mode.

Enabling Routing Behind the Mobile Station

To enable routing behind an MS, use the following steps command in access-point configuration mode:

```
config
   network-behind-mobile { max-addresses-behind-mobile max_addrs |
max-subnets max_subnets }
   { default | no } network-behind-mobile
 end
```

Notes:

- **default**

  Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

- **no**

  Disables the network behind mobile station functionality on the APN.

- **max-addresses-behind-mobile** *max_addrs*

  Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

- **max-subnets** *max_subnets*

  Specifies the maximum number of subnets that can be enabled for a call in the APN.

  max_subnets must be an integer from1 through 16.

  Default: 10

Verifying the Routing Behind the Mobile Station

To verify the routing behind the mobile station configuration, use the following show commands.

1.
```
Router show ip route vrf vpn_am2
"*" indicates the Best or Used route.  S indicates Stale.
Destination         Nexthop          Protocol   Prec Cost Interface
*17.18.19.20/32      10.7.104.2       bgp        20   0    bgp_neighbour
(nhlfe-ix:3)
*17.18.19.21/32      0.0.0.0          connected  0    0    vpn_am2lb1
*40.40.41.0/24       0.0.0.0          connected  0    0
```

```
*41.40.41.0/24       0.0.0.0          connected  0    0
*42.40.41.0/24       0.0.0.0          connected  0    0
*43.40.41.0/24       0.0.0.0          connected  0    0
*44.40.41.0/24       0.0.0.0          connected  0    0
*45.40.41.0/24       0.0.0.0          connected  0    0
*46.40.41.0/24       0.0.0.0          connected  0    0
*47.40.41.0/24       0.0.0.0          connected  0    0
*48.40.41.0/24       0.0.0.0          connected  0    0
*49.40.41.0/24       0.0.0.0          connected  0    0
*106.106.0.0/16      0.0.0.0          connected  0    0    pool pool_test_3
Total route count : 13
Unique route count: 13
Connected: 12 BGP: 1
```

2. `show subscribers pgw-only full all`

```
Username: starent
  Subscriber Type : Visitor
  Status          : Online/Active
  State           : Connected
  Connect Time    : Mon Oct 12 12:23:52 2015
  Auto Delete     : No
  Idle time       : 00h00m50s
  MS TimeZone     : n/a                  Daylight Saving Time: n/a
  Access Type: gtp-pdn-type-ipv4         Network Type: IP
  Access Tech: eUTRAN                    pgw-service-name: PGW21
  Callid: 0db5d3a3                       IMSI: 123456789012345
  Protocol Username: starent             MSISDN: 9326737733
  Interface Type: S5S8GTP                Low Access Priority: N/A
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
  Access Peer Profile: default
  Acct-session-id (C1): 141414650F55554B
  ThreeGPP2-correlation-id (C2): 17767C4D / 6SKDhW-2
  Card/Cpu: 12/0                         Sessmgr Instance: 47
  Bearer Type: Default                   Bearer-Id: 5
  Bearer State: Active
  IP allocation type: local pool
  IPv6 allocation type: N/A
  IP address: 209.165.200.225
  Framed Routes:                                  Framed Routes Source: RADIUS
    40.40.41.0      255.255.255.0   106.106.0.5
    41.40.41.0      255.255.255.0   106.106.0.5
    43.40.41.0      255.255.255.0   106.106.0.5
    44.40.41.0      255.255.255.0   106.106.0.5
    45.40.41.0      255.255.255.0   106.106.0.5
    46.40.41.0      255.255.255.0   106.106.0.5
    47.40.41.0      255.255.255.0   106.106.0.5
    48.40.41.0      255.255.255.0   106.106.0.5
    49.40.41.0      255.255.255.0   106.106.0.5
    42.40.41.0      255.255.255.0   106.106.0.5
  ULI:
   TAI-ID:
    MCC: 214  MNC: 365
    TAC: 0x6789
   ECGI-ID:
  MCC: 214 MNC: 365
    ECI: 0x1234567
  Accounting mode: None                  APN Selection Mode: Sent by MS
  MEI: 1122334455667788                  Serving Nw: MCC=123, MNC=765
  charging id: 257250635                    charging chars: normal
  Source context: EPC2                   Destination context: ISP1
 S5/S8/S2b/S2a-APN: cisco.com
  SGi-APN:   cisco.com
  APN-OI:    n/a
```

```
  Restoration priority level: n/a
  traffic flow template: none
 IMS Auth Service : IMSGx
  active input ipv4 acl: IPV4ACL         active output ipv4 acl: IPV4ACL
active input ipv6 acl:                  active output ipv6 acl:
ECS Rulebase: cisco
Bearer QoS:
QCI: 5
ARP: 0x04
PCI: 0 (Enabled)
PL : 1
PVI: 0 (Enabled)
MBR Uplink(bps): 0                     MBR Downlink(bps): 0
GBR Uplink(bps): 0                     GBR Downlink(bps): 0
PCRF Authorized Bearer QoS:
QCI: n/a
ARP: n/a
PCI: n/a
PL: n/a
PVI: n/a
MBR uplink (bps): n/a                      MBR downlink (bps): n/a
GBR uplink (bps): n/a                      GBR downlink (bps): n/a
Downlink APN AMBR: n/a                   Uplink APN AMBR: n/a
P-CSCF Address Information:
Primary IPv6  :   n/a
  Secondary IPv6:   n/a
Tertiary IPv6 :   n/a
 Primary IPv4  :   n/a
  Secondary IPv4:   n/a
   Tertiary IPv4 :   n/a
Access Point MAC Address:  N/A
  pgw c-teid: [0x8000002f] 2147483695    pgw u-teid: [0x8000002f] 2147483695
  sgw c-teid: [0x50010001] 1342242817    sgw u-teid: [0x60010001] 1610678273
  ePDG c-teid: N/A                       ePDG u-teid: N/A
  cgw c-teid: N/A                        cgw u-teid: N/A
  pgw c-addr: 2002::2:101                pgw u-addr: 209.165.200.232    2002::2:101
  sgw c-addr: 2002::2:61                 sgw u-addr: 2002::2:61
  ePDG c-addr: N/A                       ePDG u-addr: N/A
  cgw c-addr: N/A                        cgw u-addr: N/A
  Downlink APN AMBR:   16534000 bps    Uplink APN AMBR:   16534000 bps
Mediation context: None                Mediation no early PDUs: Disabled
  Mediation No Interims: Disabled        Mediation Delay PBA: Disabled
  input pkts: 0                                output pkts: 0
  input bytes: 0                               output bytes: 0
  input bytes dropped: 0                       output bytes dropped: 0
  input pkts dropped: 0                        output pkts dropped: 0
  input pkts dropped due to lorc    : 0          output pkts dropped due to lorc    :
0
  input bytes dropped due to lorc   : 0
  in packet dropped suspended state: 0           out packet dropped suspended state: 0

 in bytes dropped suspended state: 0            out bytes dropped suspended state: 0
  in packet dropped overcharge protection: 0      out packet dropped overcharge
protection: 0
  in bytes dropped overcharge protection: 0      out bytes dropped overcharge protection:
 0
  in packet dropped sgw restoration state: 0      out packet dropped sgw restoration
state: 0
  in bytes dropped sgw restoration state: 0       out bytes dropped sgw restoration
state: 0
 pk rate from user(bps): 0                      pk rate to user(bps): 0
  ave rate from user(bps): 0                     ave rate to user(bps): 0
  sust rate from user(bps): 0                    sust rate to user(bps): 0
  pk rate from user(pps): 0                      pk rate to user(pps): 0
```

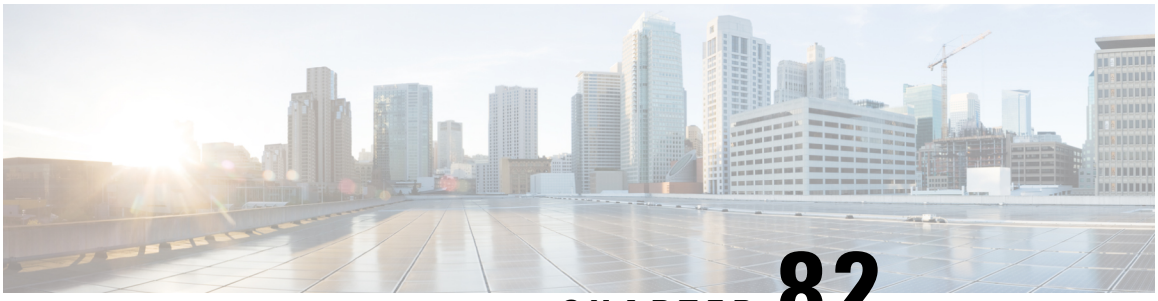
```
  ave rate from user(pps): 0                    ave rate to user(pps): 0
  sust rate from user(pps): 0                   sust rate to user(pps): 0
  link online/active percent: 65
  ipv4 bad hdr: 0                               ipv4 ttl exceeded: 0
  ipv4 fragments sent: 0                        ipv4 could not fragment: 0
  ipv4 input acl drop: 0                        ipv4 output acl drop: 0
  ipv4 bad length trim: 0
 ipv4 input mcast drop: 0                      ipv4 input bcast drop: 0
  ipv6 input acl drop: 0                        ipv6 output acl drop: 0
  ipv4 input css down drop: 0                   ipv4 output css down drop: 0
  ipv4 input css down drop: 0                   ipv4 output css down drop: 0
  ipv4 output xoff pkts drop: 0                 ipv4 output xoff bytes drop: 0
  ipv6 output xoff pkts drop: 0                 ipv6 output xoff bytes drop: 0
  ipv6 input ehrpd-access drop: 0               ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0                  output pkts dropped (0 mbr): 0
  ip source violations: 0                       ipv4 output no-flow drop: 0
  ipv6 egress filtered: 0
  ipv4 proxy-dns redirect: 0                    ipv4 proxy-dns pass-thru: 0
  ipv4 proxy-dns drop: 0
  ipv4 proxy-dns redirect tcp connection: 0
  ipv6 bad hdr: 0                               ipv6 bad length trim: 0
  ip source violations no acct: 0
  ip source violations ignored: 0
  dormancy total: 0                             handoff total: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Input Pkts Drop: 0                   APN AMBR Output Pkts Drop: 0
  APN AMBR Input Bytes Drop: 0                  APN AMBR Output Bytes Drop: 0
```

Monitoring and Troubleshooting the Routing Behind the Mobile Station

Routing Behind the Mobile Station Show Command(s) and/or Outputs

show apn name <apn_name>

```
...
proxy-mip: Disabled
proxy-mipv6: Disabled
proxy-mip null-username static home address: Disabled
Network Behind Mobile Station: Enabled
Maximum subnets behind Mobile station: 10
Maximum Addresses Behind Mobile Station:  16777214
Tunnel peer load-balancing : random
L3-to-L2 tunnel address-policy no-alloc-validate
tunnel address-policy alloc-validate
NPU QoS Traffic Priority: Derive from packet DSCP
```



CHAPTER 82

Routing Based on Realm Name S6B

- Summary Data, on page 1175
- Overview of Routing Based on Realm P-GW, on page 1176
- How it Works, on page 1176
- Enabling Realm for S6b Interface, on page 1176

Summary Data

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Table 124: Revision History

Revision Details	Release
First introduced	21.19

Overview of Routing Based on Realm P-GW

Currently, not all diameter applications have an option to have configurable ‘Destination-Realm’ name on initial diameter messages going out of P-GW. As a result, DRAs whenever P-GW is connected to diameter application servers through DRA must look inside those messages, make a routing decision to route it to the correct application server and then overwrite the destination-realm received from client node before sending out to the application server node. However, this generates some level of increased processing and load on the DRA.

This feature provides the facility to fill the ‘Destination-realm’ value from a configurable value to allow DRAs to act in ‘transparent’ mode thus reducing the load on them. It also allows DRAs to use more sophisticated load balancing mechanisms based on ‘Destination-realm’.

Part of this feature was developed for MME (S6a and S13 interfaces). For P-GW, the facility is already present with ‘host-select’ and ‘peer-select’ commands on Gx and Gy interfaces but S6b interface does not have any such facility. This feature fills that gap.

How it Works

Under this feature, ‘Destination-Realm’ AVP in AAR message towards DRA contains the value configured under ‘realm’ as described in the next section. This allows DRAs to act in transparent mode. 'Destination-Realm' AVP is also set to the configured value in further messages for that session, for example, STR.

Enabling Realm for S6b Interface

Use the following configuration to associate the diameter authentication server with a realm name:

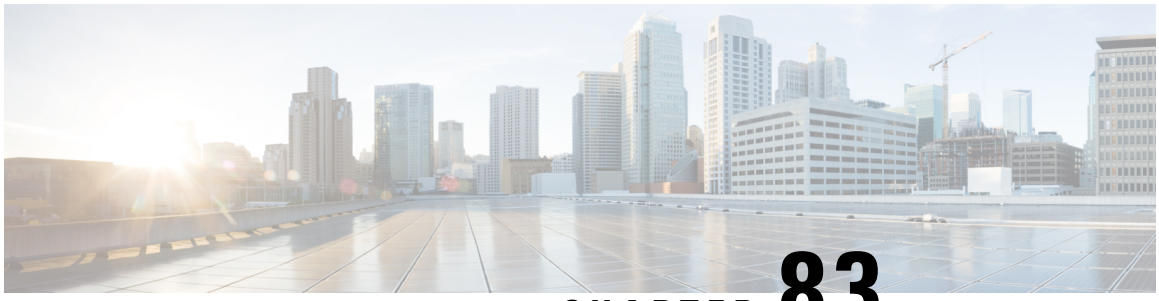
```
configure
   context context_name
     aaa group group_name
     diameter authentication server  diameter_host_name priority priority_value
 realm realm_name
    end
```

Note If the 'realm' attribute is configured, then there must be a 'route-entry' with the same 'realm_name'. This is described in the example given below:

Example

```
aaa group s6b
 diameter authentication endpoint s6b
 diameter authentication server dra1.dra.mnc123.mcc456.3gppnetwork.org priority 10 realm
xyz.org

...

diameter endpoint s6b
      origin realm abc.com
      use-proxy
```

```
      origin host SPRC01.s6b address 10.239.144.69
      watchdog-timeout 6
      device-watchdog-request max-retries 3
      response-timeout 5
      cea-timeout 3
      reconnect-timeout 30
      connection retry-timeout 10
      peer dra1.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
address 10.1.1.1
      peer dra2.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
address 10.1.1.2
      route-entry realm xyz.org peer dra1.dra.mnc123.mcc456.3gppnetwork.org
```



CHAPTER 83

S6b Interface Enhancement

- Feature Summary and Revision History, on page 1179
- Feature Description, on page 1179

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic IP addresses through AVPs.	21.22

Feature Description

In the StarOS 21.22 and later releases, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic IP addresses through the following AVPs:

- **Class AVP**

- **User-Name AVP**
- **Origination-Time-Stamp AVP**

Class AVP: The following enhancement is supported:

During the initial PDN connection request, PGW/GGSN receives the CLASS AVP, if available, in the AA Answer message from 3GPP AAA. Then, P-GW/GGSN sends Answer to 3GPP AAA. While sending AA_request message to 3GPP AA, P-GW/GGSN drops the CLASS AVP. PGW/GGSN has the option to initiate re-authorization. However, if P-GW/GGSN has previously received the CLASS AVP from 3GPP AAA, it includes Class AVP in subsequent session termination requests but not re-authorization requests. It results in removal of Class AVP from all messages except AA Answer and Session-Termination messages (STR and STA messages).

If Auth-Session-State is negotiated as STATE_MAINTAINED, then on session termination, P-GW initiates a Session-Termination-Request {Session-Id, Origin-Host, Origin-Realm, Destination-Realm, Auth-Application-Id=(16777999), Destination-Host, Termination-Cause, User-Name } to the 3GPP AAA.



Note The Class AVP can only be removed from the instances wherever `aaa-custom15` dictionary is used.

User-Name AVP: The following enhancement is supported.

When P-GW/GGSN sends subsequent session termination (STR) requests to 3GPP AAA, it includes the mandatory parameter, **User-Name AVP**.



Note During backward compatibility, 3GPP AAA accepts STR without **User-Name AVP**.

Ensure that the User-Name doesn't include prefix.

For Example:

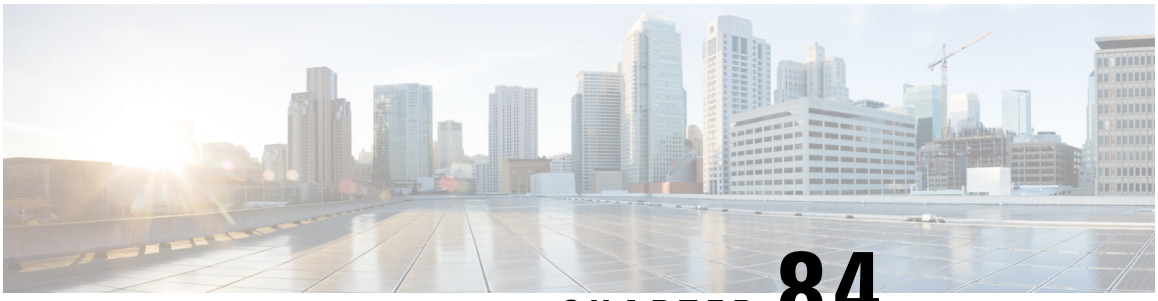
```
<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
```

Origination-Time-Stamp AVP: The following enhancement is supported.

The **Origination-TimeStamp AVP** is replaced with the 3GPP standard Origination-Time-Stamp AVP.

Maximum-Wait-Time AVP: The following enhancement is supported.

The **Max-Wait-Time AVP** is replaced with 3GPP standard Maximum-Wait-Time AVP **Maximum-Wait-Time AVP**.



CHAPTER 84

Handling Uneven Resource Distribution Notifications on Session Managers

- Feature Summary and Revision History, on page 1181
- Feature Description, on page 1182
- Configuring Threshold Levels and SNMP Traps, on page 1182
- Monitoring and Troubleshooting, on page 1183

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • GGSN • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The SNMP traps and alarms support uneven distribution of resources on session managers across the system. The active session manager task calculates the threshold of resource usage. The supported SNMP trap and alarm configures the monitoring threshold difference between the number of calls among the session managers.

This feature supports the following functions:

1. Raise alarms and traps

   The alarm will be raised when the load difference between the most loaded and least loaded session manager is greater than the configured threshold. The session manger load is calculated by the number of sessions.

2. Clear alarms and traps

   The alarm will be cleared when the load difference between the most loaded and least loaded session manager is lesser than the configured threshold. The session manger load is calculated by the number of sessions.



Note The threshold calculations does not consider the standby session manager instances.

Configuring Threshold Levels and SNMP Traps

Configuring Threshold Levels

Use the following configuration to configure threshold levels for session manager:

```
configure
   [ no ] threshold sess-uneven-dist threshold_percentage [ clear
clear_threshold_percentage [ sess-min-sessmgr-cnt number_of_sessmgr_with_least_calls
 [ sess-active number_of_min_active_session_system_wide ]]]
   [ no ] threshold monitoring sess-uneven-dist
   threshold poll sess-uneven-dist interval interval_range
   default threshold sess-uneven-dist
   end
```

NOTES:

- **threshold**: Configures a specific threshold-based alarm.
- **sess-uneven-dist** *threshold_percentage*: The number of threshold indicates the percentage difference of established session between the most loaded session manager and the least loaded session manager. The default value for threshold is 50%.
- **clear** *clear_threshold_percentage*: Clears the configured alarm threshold. The default value for threshold is 50%.

- **sess-min-sessmgr-cnt** *number_of_sessmgr_with_least_calls*: Configures the number of count of session managers with minimum number of calls to be monitored for calculating uneven session distribution.
- **sess-active** *number_of_min_active_session_system_wide*: Configures the active sessions after which uneven call distribution threshold will be monitored. The default value is 10000.
- **monitoring sess-uneven-dist**: Enables or disables thresholds alerting for a group of thresholds. The number of threshold indicates the percentage difference of established session between the most loaded session manager and the least loaded session manager.
- **poll sess-uneven-dist interval** *interval range*: Configures the threshold polling interval. The value is rounded up to the closest multiple of 30 seconds. The default value is 900.
- **default**: Sets or restores the default value assigned for the specified parameter.

Configuring SNMP Traps

Use the following configuration to configure SNMP traps for session managers and uneven resource distribution:

```
configure
   snmp trap [ enable | suppress ] { sessionUnevenDistribution |
sessionUnevenDistributionclear }
   end
```

NOTES:

- **sessionUnevenDistribution**: Configures the threshold for detection of uneven call distribution on session manager.
- **sessionUnevenDistributionclear**: Clears the threshold detection of uneven call distribution on session manager.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature using show commands and bulk statistics.

Show Commands and Outputs

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

show threshold

The output of this command displays the following fields:

```
show threshold

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
```

```
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:32:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist              SYSTEM

Non-default poll intervals:
        place-holder                            0Sec
        sess-uneven-dist                      120Sec

No outstanding alarm
```

show threshold all

The output of this command displays the following fields:

```
show threshold all

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:34:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist              SYSTEM

Non-default poll intervals:
        place-holder                            0Sec
        sess-uneven-dist                      120Sec

No outstanding alarm
```

show threshold default

The output of this command displays the following fields:

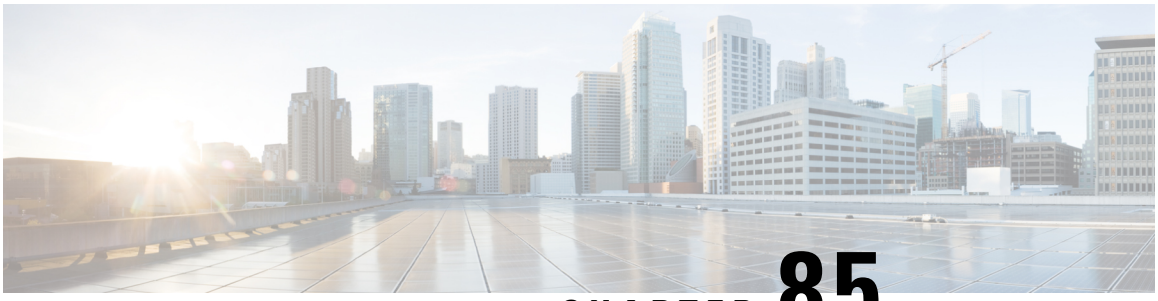
```
show threshold default
Default Thresholds:
```

```
sess-uneven-dist                      15Min     Notify Above     50%
```

show snmp trap statistics

The output of this command displays the following fields:

```
show snmp trap statistics
SNMP Notification Statistics:
  Total number of notifications   : 118
  Last notification sent          : Tuesday August 10 17:31:56 IST 2021
  Notification sending is         : enabled
  Notifications have never been disabled
  Notifications have never been cleared
  Notifications in current period : 2
  Notifications in previous period: 0
  Notification monitor period     : 300 seconds

Trap Name                          #Gen #Disc  Disable Last Generated
---------------------------------- ----- -----  ------- --------------------

SessionUnevenDistribution             1     0       0  2021:08:10:13:36:00
SessionUnevenDistributionClear        1     0       0  2021:08:10:15:12:00

Total number of notifications Disabled  : 92
```



CHAPTER 85

Secondary RAT Usage Report in CDR Records

- Feature Summary and Revision History, on page 1187
- Feature Description, on page 1188
- Configuring Secondary RAT Usage Report through GTPP, on page 1191
- Monitoring and Troubleshooting, on page 1194

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW • S-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GTPP Interface Administration and Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
P-GW and S-GW supports secondary RAT usage reports and CDRs processing through GTPP Group Configuration CLIs.	• 21.26 • 21.23.14
P-GW and S-GW supports secondary RAT usage reports and CDRs processing through GTPP Group Configuration CLIs.	21.20.31
First Introduced.	21.22.n7

Feature Description

Reporting issues pertaining to 5G **RANSecondaryRATUsageReport** occur due to lack of:

- Control in identifying whether the **RANSecondaryRATUsageReport** must be processed in CDRs or not. This allows the S-GW, P-GW, and SAEGW to either include these reports in the SGW-CDR or PGW- CDR or to simply ignore them.
- Number of available reports inside a CDR, if the control is active.
- Control in identifying whether Zero-volume reports must make it inside the CDR or not.

This results in billing loss of data. To overcome these reporting issues, you can trigger CLI controls using GTPP group configuration to:

- Allow the S-GW, P-GW, and SAEGW to either include the RANSecondary RAT Usage reports in the SGW-CDR or PGW-CDR or to simply ignore them.
- Identify the number of secondary RAT usage reports available inside the SGW-CDR or the PGW- CDR.

Note This limit must be in accordance with the system capability and ensure to consider the File-Format of the CDRs. If the configured limit exceeds, the system closes the SGW-CDR or PGW-CDR with the appropriate change-condition. For example, **max-change-condition** CDR is reused for further reports.

- Add or ignore Zero-volume reports inside the CDR.
- The CLI **gtpp limit-secondary-rat-usage** or hardcoded limit will be removed and the CLI **gtpp limit-secondary-rat-usage** is reused to control the number of records within the range 1-100.
- Provides logging when the CDR size reaches the maximum size. Through PGW-CDR counter, you can monitor the number of occurrences when the CDR exceeds its size limit.

Behavior Matrix

The following table explains the new behavior of P-GW and S-GW for this feature.

CLI	P-GW New Behavior	S-GW New Behavior
gtpp attribute secondary-rat-usage By default, this CLI command is enabled in gtpp group.	P-GW sends secondary RAT usage records in CDR including zero volume records.	S-GW sends secondary RAT usage records in CDR including zero volume records.
[no] gtpp attribute secondary-rat-usage	P-GW does not send secondary RAT usage records in CDR.	S-GW does not send secondary RAT usage records in CDR.
gtpp suppress-secondary-rat-usage zero-volume By default, this CLI command is disabled in gtpp group.	P-GW does not include and send zero volume secondary RAT records in CDR. P-GW sends only secondary RAT records with non-zero volumes.	S-GW does not include and send zero volume secondary RAT records in CDR. S-GW sends only secondary RAT records with non-zero volumes.
[no] gtpp suppress-secondary-rat-usage zero-volume	P-GW sends secondary RAT usage records including zero volume records in CDR.	S-GW sends secondary RAT usage records including zero volume records in CDR.
gtpp limit-secondary-rat-usage *range_1–100*. If not configured, the default value is 32. By default, this CLI command is enabled in gtpp group. **Example: gtpp limit-secondary-rat-usage 32** **Note** This CLI is the modification of the existing CLI command **gtpp limit-secondary-rat-usage** with range between 1– 100.	P-GW generates CDR immediately when total received secondary RAT records exceeds 32 and reported cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 32. **Example**: If P-GW receives 100 RAT records between two triggers, P-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.	S-GW generates CDR immediately when total received secondary RAT records exceeds 32 and the reported cause value is *maximum change condition*. S-GW generates multiple CDRs if the total received secondary RAT records are multiples of 32. **Example**: If S-GW receives 100 RAT records between two triggers, S-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.
Example:gtpp limit-secondary-rat-usage 40	P-GW generates CDR immediately when total received secondary RAT records exceeds 40 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 40. **Example**: If P-GW receives 100 RAT records between two triggers, it will generate 2 CDRs and will keep remaining 20 RAT records for the next CDR trigger.	If the configured value is greater than 32 and sends 32 secondary RAT records in every CDR, Ignores **gtpp limit-secondary-rat-usage 40** CLI command.

CLI	P-GW New Behavior	S-GW New Behavior
Example:gtpp limit-secondary-rat-usage 20	P-GW generates CDR immediately when total received secondary RAT records exceed 20 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 20. **Example:** If P-GW receives 100 RAT records between two triggers, P-GW generates 2 CDRs and will store the remaining 20 RAT records for the next CDR trigger.	S-GW generates CDR immediately when the total received secondary RAT records exceeds 20 and cause value is *maximum change condition*. S-GW generates multiple CDRs if total received secondary RAT records are in multiples of 20. **Example**: If S-GW receives 100 RAT records between two triggers, it will generate 5 CDRs.
[no] gtpp limit-secondary-rat-usage	Generates CDR immediately when the total received secondary RAT records exceed 255 and cause value is *maximum change condition*. Generates multiple CDRs if the total received secondary RAT records are multiples of 255. **Example**: If 1000 RAT records between two triggers are received, then 3 CDRs are generated. The remaining 235 RAT records are stored for the next CDR trigger.	Ignores the **[no] gtpp limit-secondary-rat-usage** CLI and sends 32 secondary RAT records in every CDR. Behavior is similar to the **gtpp limit-secondary-rat-usage** *32* CLI implementation. Counter and debug logs are not required as it will never exceed the CDR size of 64k.
	Service-specific unit limit is sent in the **serviceConditionChange** file.	Record Closure

Relationship to Other Features

- Sessmgr Restart While Processing Secondary RAT Usage CDR Records in the *P-GW Administration Guide*.
- Secondary RAT Usage IE during GnGp handover, S-GW, and P-GW support of Secondary RAT Data Usage Report in Gz CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.
- P-GW support of Secondary RAT Data Usage Report in Rf CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.

Limitations

This feature has the following limitations:

- S-GW allows a maximum number of 16 secondary RAT records per bearer during session recovery and checkpointing.
- P-GW allows a maximum number of 142 secondary RAT records across all bearers during session recovery and checkpointing.
- Anything beyond these numbers gets lost during session recovery.

Configuring Secondary RAT Usage Report through GTPP

Use the following GTPP configurations to close Secondary RAT Usage CDR records before exceeding a buffer size.

Enabling or Disabling the Secondary RAT Usage Report

Use the following configuration to enable or disable secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute secondary-rat-usage
      default gtpp attribute secondary-rat-usage
      no gtpp attribute secondary-rat-usage
      end
```

NOTES:

- **gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records.
- **default gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records by default.
- **no gtpp attribute secondary-rat-usage**: Does not send the optional attribute Secondary RAT usage records.

Controlling the Maximum Number of Entries

When the Secondary RAT usage record reaches the maximum configured value within a CDR, the CDR closure cause occurs and uses **maxChangeCond**. The **gtpp limit-secondary-RAT-usage** CLI command controls the maximum number of Secondary RAT usage record entries in the P-GW and S-GW CDRs. If the limit is configured with a value more than 32, the partial CDRs get generated with a maximum of 32 for S-GW CDR.



Note The existing behaviour of S-GW has a limit of 32 Secondary RAT Usage records.

The following table explains the behavior of Secondary RAT records and CDR, and the maximum limit.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
1	P-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 secondary RAT records.
					Remaining 15 secondary RAT records sent in the next trigger.
	S-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 Secondary RAT records.
					Remaining 15 Secondary RAT records sent in the next trigger.
2	P-GW	32	32	35	Partial CDR is generated with 32 Secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.
	S-GW	32	32	35	Partial CDR is generated with 32 secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
3	P-GW	Greater than 32 Example: 100	100	100	Partial CDR is generated with 100 secondary RAT records.
	S-GW	Greater than 32 Example: 100	32	100	Three partial CDRs are generated with 32 secondary RAT records each.
					Remaining 4 secondary RAT records sent in the next trigger.
4	P-GW	Not configured	255	1000	Three partial CDRs are generated with 255 secondary RAT records each.
					Remaining reported Secondary RAT records become a part of CDR in the next trigger.
	S-GW	Not configured	32	1000	No partial CDR is generated.
					32 Secondary RAT records become part of the CDR in the next trigger.

Use the following configuration to control the maximum number of entries.

```
configure
  context context_name
    gtpp group group_name
      gtpp limit-secondary-rat-usage usage_limit
      default gtpp limit-secondary-rat-usage
```

```
no gtpp limit-secondary-rat-usage
end
```

NOTES:

- **gtpp limit-secondary-rat-usage** *usage_limit*: Enter a maximum number of secondary RAT reports. *usage_limit* must be an integer in the range of 1-100. The recommended value for S-GW CDR is 32.

  For example, if the limit is set to 10, then the CDR is generated once the configured value is reached.

- **default gtpp limit-secondary-rat-usage**: Specifies a default value of 32.
- **no gtpp limit-secondary-rat-usage**: Disables the CDR generation with limited number of secondary RAT usage information.

Suppressing Zero-Volume Secondary RAT Usage Report

Use the following configuration to suppress zero-volume Secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp suppress-secondary-rat-usage zero-volume
      default gtpp suppress-secondary-rat-usage zero-volume
      no gtpp suppress-secondary-rat-usage zero-volume
      end
```

NOTES:

- **gtpp suppress-secondary-rat-usage zero-volume**: Suppresses either Secondary RAT records or zero volume Secondary RAT records.
- **default gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume secondary RAT usage records.
- **no gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume Secondary RAT usage records.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show config

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Specify this option to include the Secondary RAT reports field in the CDR.
gtpp suppress-secondary-rat-usage zero-volume	Enables the exclusion of the zero volume Secondary RAT reports in the CDR.
gtpp limit-secondary-rat-usage	Enables limiting the number of Secondary RAT Usage reports in CDR with the configured value.

show config verbose

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Displays the Secondary RAT usage records.
gtpp suppress-secondary-rat-usage zero-volume	Displays only Secondary RAT records that is having non-zero volumes from P-GW and S-GW.
gtpp limit-secondary-rat-usage	If total received Secondary RAT records are multiples of 10, displays multiple CDR generated by P-GW and S-GW. The reported cause value will be the maximum change condition.
no gtpp limit-secondary-rat-usage	Displays Secondary RAT records for unconfigured cause.

show gtpp group

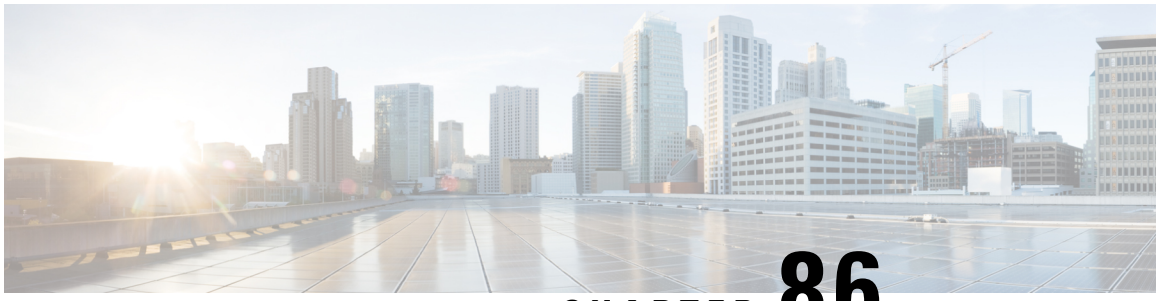
The output of this CLI command displays the following parameters.

Field	Description
Secondary RAT records present	Specifies whether the Secondary RAT record is present or not. The available options are: • no • yes
Limit-secondary-rat-usage	Specifies a limit for Secondary RAT usage report.

show gtpp statistics group

The output of this CLI command displays the following parameter.

Field	Description
Total PGW-CDR exceed size limit	Displays the total number of CDRs that exceeded size limit in P-GW.



CHAPTER 86

Separation of 2G, 3G, and 4G Bulkstatistics

This chapter describes the following topics:

- Feature Summary and Revision History, on page 1197
- Feature Description, on page 1198
- Configuring RAT types in Stats Profile, on page 1198
- Monitoring and Troubleshooting, on page 1199

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.5

Feature Description

Important In this release, this feature is not fully qualified and is available only for testing purpose. For more information, please contact your Cisco Account representative.

This feature separates bulkstats by RAT type (2G, 3G, and 4G). This helps KPI monitoring and reporting per RAT type. Per APN per RAT type statistics is integrated with the existing stats-profile implementation. A new CLI command **rat-type** is added to the **stats-profile** configuration mode to configure the RAT-types in stats-profile.

Configuring RAT types in Stats Profile

A new CLI command **rat-type** has been added to the **stats-profile** configuration mode. This CLI command integrates per APN per RAT type statistics with the existing stats-profile implementation. To gather RAT level statistics, you must configure RAT type under the stats-profile for which RAT level statistics are required. Once that is done, associate stats-profile in APN for which APN per RAT level statistics is required. Only after this association, the stats are collected. Per APN per RAT level statistics are lost if stats-profile association is removed from APN and/or rat type option is removed from stats-profile.

To enable per APN per RAT types statistics collection, execute the following command:

```
configure
    stats-profile <stats_profile_name>
       [no] rat-type { [geran | utran | eutran]* }
       end
```

NOTES:

- **no:** Disables statistics collection based on RAT type.
- **stats-profile:** Configures statistics profile to collect packet drop counters and/or ARP level statistics.
- **rat-type:** Configures collection of RAT level statistics.
- **geran:** Configures collection of statistics for RAT Type GERAN.
- **utran:** Configures collection of statistics for RAT Type UTRAN.
- **eutran:** Configures collection of statistics for RAT Type EUTRAN.

Sample Configuration

Sample configuration to enable stats collection based on rat type:

```
config
   stats-profile stats-info
      rat-type eutran utran
      rat-type utran geran
      end
```

Sample configuration to disable stats collection based on rat type:

```
config
   stats-profile stats-info
      no rat-type eutran utran
      end
```

Monitoring and Troubleshooting

This section provides information on the show commands available to support the 2G/3G/4G bulkstat separation.

Show Commands and Outputs

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

show apn statistics all

The output of the above command is modified to display the following new field depending on whether the CLI command is enabled or disabled:

- Data Statistics:
  - RAT Type statistics for uplink and downlink bytes:
    - GERAN
      - Uplnk DataBytes
      - Dnlnk DataBytes
    - UTRAN
      - Uplnk DataBytes
      - Dnlnk DataBytes
    - EUTRAN
      - Uplnk DataBytes
      - Dnlnk DataBytes
- IP address allocation statistics
  - RAT Type statistics for dynamic address allocation for PDN types IPv4, IPv6, IPv4v6:
    - GERAN Dynamic address allocated:
      - IPv4
      - IPv6
      - IPv4v6
    - UTRAN Dynamic address allocated:

- IPv4
- IPv6
- IPv4v6

show gtpc statistics

The output of the above command is modified to display the following new fields. These fields do not have any dependency on stats-profile configuration. The gtpc stats will increase irrespective of the stats profile configured with rat type.

- Total CPC Req GERAN
- Total CPC Req UTRAN

show stats profile all

The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

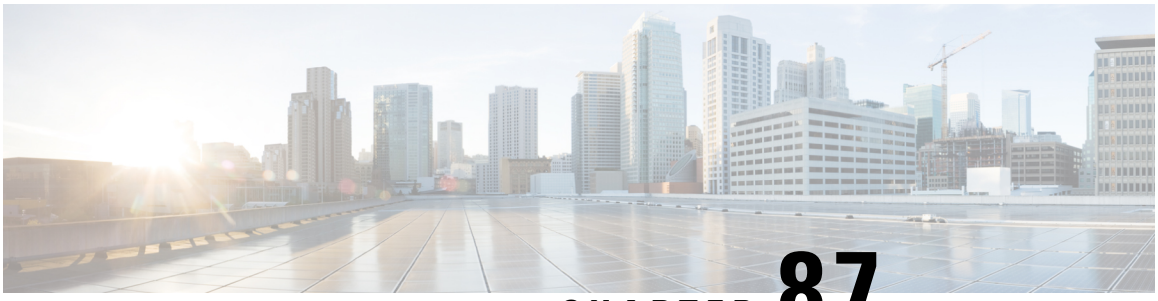
- rat-type geran utran eutran

Bulk Statistics

The following bulk statistics are added in the APN schema to support the 2G, 3G, 4G bulkstats separation feature:

Bulk Statistics	Description
att-pdp-ctxt-geran	Indicates the total number of CPC requests received per APN for a call with a RAT type of GERAN.
att-pdp-ctxt-utran	Indicates the total number of CPC requests received per APN for a call with a RAT type of UTRAN.
dyn-ipv4-success-geran	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GERAN RAT type.
dyn-ipv4-success-utran	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a UTRAN RAT type.
dyn-ipv6-success-geran	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GERAN RAT type.
dyn-ipv6-success-utran	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a UTRAN RAT type.

Bulk Statistics	Description
dyn-ipv4v6-success-geran	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GERAN RAT type.
dyn-ipv4v6-success-utran	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a UTRAN RAT type.
uplnk-bytes-geran	Indicates the total number of bytes sent from the APN for a GERAN RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-geran	Indicates the total number of bytes received for a GERAN RAT type on the Gi interface for the APN.
uplnk-bytes-utran	Indicates the total number of bytes sent from the APN for a UTRAN RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-utran	Indicates the total number of bytes received for a UTRAN RAT type on the Gi interface for the APN.
uplnk-bytes-eutran	Indicates the total number of bytes sent from the APN for a EUTRAN RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-eutran	Indicates the total number of bytes received for a EUTRAN RAT type on the Gi interface for the APN.



CHAPTER 87

Separation of 2G 3G 4G WLAN Bulkstatistics

- Feature Summary and Revision History, on page 1203
- Feature Description, on page 1204
- **Configuring RAT types in Stats Profile**, on page 1204
- Monitoring and Troubleshooting, on page 1205

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
In this release, separation of 2G 3G 4G WLAN Bulk Statistics is introduced	21.23
First introduced.	21.5

Feature Description

Some of the contractual Key Performance Indicators (KPIs) are monitored by operations that require reporting per Radio Access Technology (RAT) type (2G, 3G, 4G). A few of the bulkstat counters implemented currently do not separate the RAT type. To enable and disable per APN RAT types statistics, the newly introduced RAT types are"gtpv2-s2a" and "gtpv2-s2b".These types provide RAT separation (2G, 3G, 4G, WLAN).

This separation enables the operations team to report the usage by RAT type separately, as well as enhance the troubleshooting tools used to detect any network issues.

Configuring RAT types in Stats Profile

The configuration command gtpv2-s2a and gtpv2-s2b has been added to the stats-profile configuration mode. It integrates the per APN per RAT type (2G, 3G, 4G, gtpv2-s2a, gtpv2-s2b) statistics with the existing stats-profile implementation.

To enable per APN per RAT types statistics collection, execute the following command:

```
configure
  stats-profile stats_profile_name
    [ no ]  rat-type { gtpv2-s2a | gtpv2-s2b }
  end
```

After the association of stats-profile with APN, the statistics are collected for and this requires APN per RAT level statistics.

Per APN per RAT level statistics are lost if stats-profile association is removed from APN and RAT type option is removed from stats-profile.

To assoicate stats-profile with APN , execute the following command:

```
configure
  context context_name
    apn apn_name
      stats-profile stats_profile_name
  end
```

NOTES:

- **stats-profile** : Configures statistics profile to collect packet drop counters and/or ARP level stats.
- **rat-type** Configures collection of RAT level statistics.
- **gtpv2-s2a** Configures collection of statistics for RAT Type WLAN S2A.
- **gtpv2-s2b** Configures collection of statistics for RAT Type WLAN S2B.

Monitoring and Troubleshooting

This section provides information on the show commands and bulk statistics available to support the 2G, 3G, 4G, WLAN bulkstat separation.

Show Command and Output

show stats-profile all

The output of this command displays the collection of statistics for RAT Type gtpv2-S2A and gtpv2-S2B as follows:

- stats profile name
- RAT Type
- gtpv2-s2a
- gtpv2-s2b

show apn statistics all

The output of this command displays the statistics of dynamic address allocation, uplink and downlink of gtpv2-s2a and gtpv2-s2b as follows:

- Data Statistics
  - gtpv2-s2a
    - Uplnk Bytes
    - Dnlnk Bytes
  - gtpv2-s2b
    - Uplnk Bytes
    - Dnlnk Bytes
- RAT Type Statistics
  - gtpv2-s2a
    - Ipv4
    - Ipv6
    - Ipv4v6
  - gtpv2-s2b
    - Ipv4
    - Ipv6

- Ipv4v6

show gtpc statistics

The output of this command displays the statictics of updated pdp context transmission and reception of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted

Note The above Accepted counter is for GERAN UPC RX.

  - UTRAN UPC RX
  - Accepted

Note The above Accepted counter is for UTRAN UPC RX.

  - GERAN UPC TX
  - Accepted

Note The above Accepted counter is for GERAN UPC TX.

  - UTRAN UPC TX
  - Accepted

Note The above Accepted counter is for UTRAN UPC TX.

show gtpc statistics apn <apn_name> verbose

The output of this command displays the statistics of RAT type create pdp context statistics of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted

- Total UTRAN Accepted
- GERAN UPC RX
- Accepted

Note The above Accepted counter is for GERAN UPC RX.

- UTRAN UPC RX
- Accepted

Note The above Accepted counter is for UTRAN UPC RX.

- GERAN UPC TX
- Accepted

Note The above Accepted counter is for GERAN UPC TX.

- UTRAN UPC TX
- Accepted

Note The above Accepted counter is for UTRAN UPC TX.

- GERAN PDP Context Denied
  - No Resources
  - Memory
  - All Dyn Addr Occupied
  - User Auth Failed
  - Unknown Missing/APN
  - System Failure
  - Service Not Supported
  - No APN Subscription
- UTRAN PDP Context Denied
  - No Resources
  - Memory

- All Dyn Addr Occupied
- User Auth Failed
- Unknown Missing/APN
- System Failure
- Service Not Supported
- No APN Subscription

show gtpc statistics apn <apn_name>

The output of this command displays the statictics of updated pdp context transmission and reception of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted

Note The above Accepted counter is for GERAN UPC RX.

  - UTRAN UPC RX
  - Accepted

Note The above Accepted counter is for UTRAN UPC RX.

  - GERAN UPC TX
  - Accepted

Note The above Accepted counter is for GERAN UPC TX.

  - UTRAN UPC TX
  - Accepted

Note The above Accepted counter is for UTRAN UPC TX.

Bulk Statistics

APN Schema

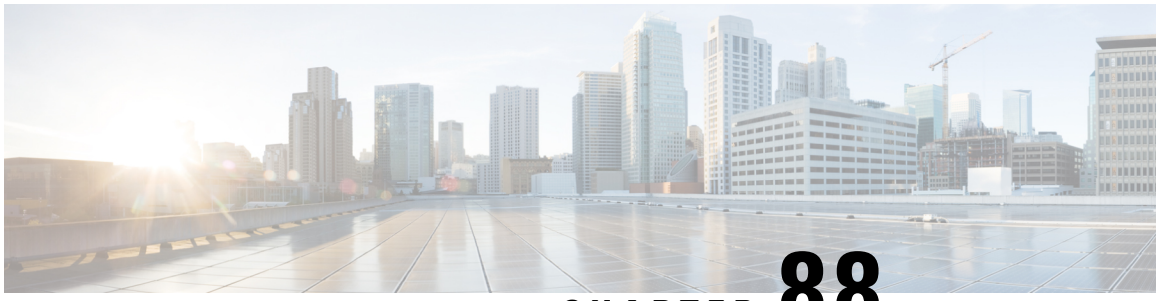
The following bulk statistics are added in the APN schema to support the 2G, 3G, 4G, WLAN bulkstats separation feature:

Bulk Statistics	Description
uplnk-bytes-gtpv2-s2a	Indicates the total number of bytes sent from the APN for a GTPV2 based S2A RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2a	Indicates the total number of bytes received for a GTPV2 based S2A RAT type on the Gi interface for the APN.
uplnk-bytes-gtpv2-s2b	Indicates the total number of bytes sent from the APN for a GTPV2 based S2B RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2b	Indicates the total number of bytes received for a GTPV2 based S2B RAT type on the Gi interface for the APN.
dyn-ipv4-success-eutran	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv4-success-gtpv2-s2a	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4-success-gtpv2-s2b	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv6-success-eutran	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv6-success-gtpv2-s2a	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type
dyn-ipv6-success-gtpv2-s2b	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv4v6-success-eutran	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.

dyn-ipv4v6-success-gtpv2-s2a	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4v6-success-gtpv2-s2b	The total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
upc-rx-geran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a GERAN RAT type per APN.
upc-tx-geran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a GERAN RAT type per APN.
upc-rx-accept-geran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.
upc-tx-accept-geran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.
upc-rx-utran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a UTRAN RAT type per APN.
upc-tx-utran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a UTRAN RAT type per APN.
upc-rx-accept-utran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
upc-tx-accept-utran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-accept-geran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted)for a GERAN RAT type per APN.

cpc-accept-utran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-nomem-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a GERAN RAT type per APN.
cpc-nomem-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a UTRAN RAT type per APN.
cpc-noresource-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a GERAN RAT type per APN.
cpc-noresource-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a UTRAN RAT type per APN.
cpc-srv-not-supp-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a GERAN RAT type per APN.
cpc-srv-not-supp-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a UTRAN RAT type per APN.
cpc-sys-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a GERAN RAT type per APN.
cpc-sys-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a UTRAN RAT type per APN.
cpc-auth-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a GERAN RAT type per APN.

cpc-auth-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a UTRAN RAT type per APN.
cpc-no-apn-subscription-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a GERAN RAT type per APN because there was no apn subscription.
cpc-no-apn-subscription-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a UTRAN RAT type per APN because there was no apn subscription.
cpc-missing-apn-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a GERAN RAT type per APN.
cpc-missing-apn-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a UTRAN RAT type per APN.
cpc-addr-occupied-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a GERAN RAT type per APN.
cpc-addr-occupied-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a UTRAN RAT type per APN.



CHAPTER 88

Session Tracing

This chapter provides information on subscriber session trace functionality that allows an operator to trace subscriber activity at various points in the network and at various level of detail. Subscriber session tracing is supported on the following UMTS/EPC GW network elements:

- GGSN
- P-GW
- SAEGW
- S-GW

Important For detailed information for session tracing on the MME, refer to the *MME Administration Guide*.

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 includes a feature description, configuration procedures, monitoring commands, and a session tracing file example.

- Session Tracing Overview, on page 1213
- Configuring Session Trace Functionality, on page 1217
- Monitoring the Session Trace Functionality, on page 1227
- Supported SAEGW Session Trace Configurations, on page 1228
- Session Trace File Example, on page 1231

Session Tracing Overview

Session Trace capability enables an operator to trace subscriber activity at various points in the network and at various levels of detail. The trace can be subscriber initiated (that is, signaling based) or management initiated from the CLI (Command Line Interface) and can be propagated throughout the access cloud via the various signaling interfaces available to the UMTS/EPC network element.

Essentially, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a User Equipment (UE) connects to the access network.

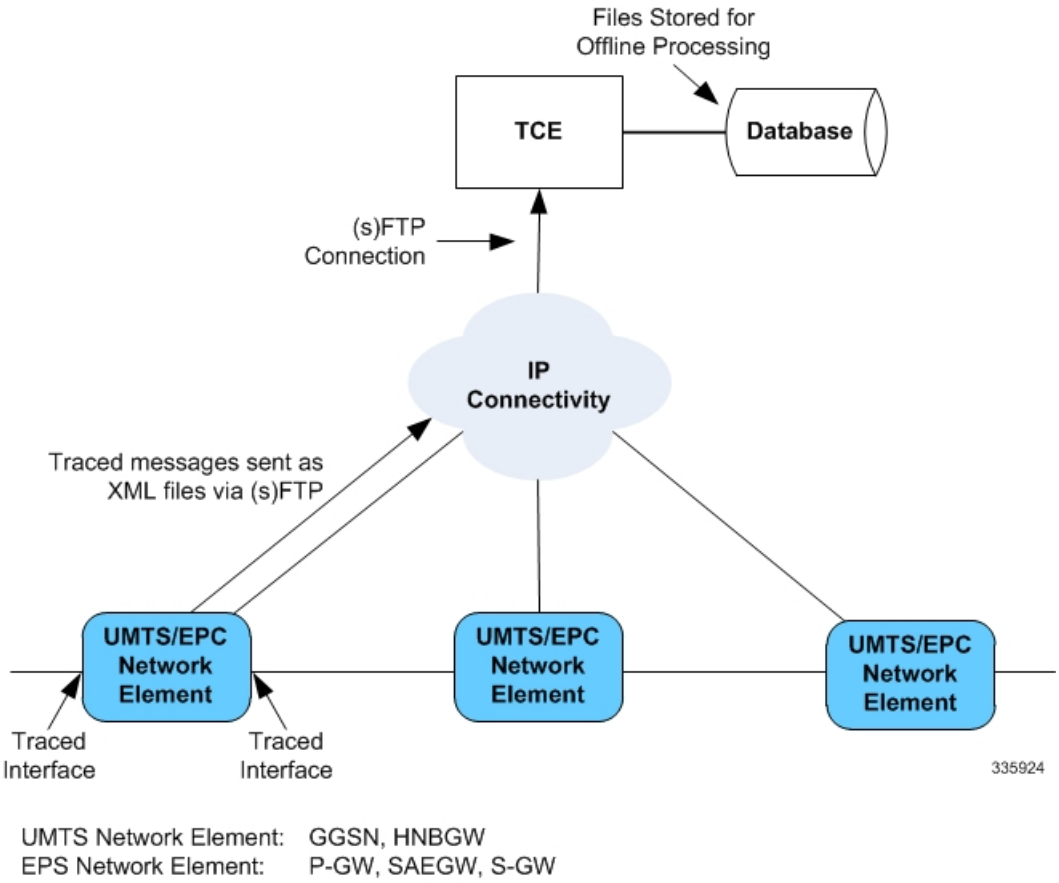
All monitored activity is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a File Transfer Protocol (FTP) or secure FTP (sFTP) connection.

Important Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

Important Only the SFTP option supports for Session Trace function. FTP does not support for the Session Trace function.

As can be seen in the following illustration, of the three Network Elements (NEs) shown, one NE is actively tracing data on one or more interfaces. All data collected is stored as files in an XML format and then transferred to the collection entity using (S)FTP or FTP. Note that IPv4 or IPv6 connectivity is required between the NE and the TCE in order to transfer the files.

Figure 113: Session Tracing Architecture



Session Trace Types

There are three types of session trace functions available.

- **Management Trace:** The operator sends an activation request via the CLI directly to the UMTS/EPC network element where the trace is to be initiated. The network element establishes the trace session and waits for a configured trigger event to start actively tracing. When management-initiated trace activations are executed at the network element, they are never propagated to other NEs whether or not it is involved in the actual recording of the call.
- **Random Trace**: Enables or disables the subscriber session trace functionality based on a the random trace on the UMTS/EPC network element. The trace control and configuration parameters are configured directly in the specified network element through the **random trace** CLI command. There is no propagation of trace parameters in random based trace activation. This NE shall not propagate the received data to any other NEs whether or not it is involved in the actual recording of the call. If enabled, the subscriber selection will be based on random logic all instances of session on the specified UMTS/EPC network element.
- **Signaling Trace**: With a signaling based activation, the trace session is indicated to the UMTS/EPC network element across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active). Signaling based activations are always propagated to neighboring NEs even if the current NE does not participate in the trace (either they not enabled by configuration or not present in the configured trace parameters).

Important Note that the maximum number of unique International Mobile Subscriber Identification (IMSI) numbers or International Mobile Equipment Identification (IMEI) numbers cannot exceed 32; however, each NE can trace all 32 unique IMSI/IMEIs.

Caution Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

Session Trace Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, an (S)FTP connection to the Trace Collection Entity (TCE) is established if one does not already exist. The NE will store up to 2 MB of XML data on its local disk to allow for the (S)FTP connection to be established and the files to be pushed to or pulled from the TCE.

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity waits until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to the maximum being exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

Session Trace Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session

to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Data Collection

Data collection is done inline by each of the NEs. In order to reduce the overhead on a per-control packet basis, a copy of the entire packet is made and stored into an internal database (DB) of packets.

The local internal path for the trace database is **/hd-raid/trace**.

This storage is done regardless of the trace depth. After xx bytes (or xx messages) have been stored or a configurable number of seconds have elapsed, all cached data is encoded in the standard XML format and written out to a file to be forwarded to/pulled from the TCE. If there is no TCE active, the UMTS/EPC network element will continue to cache data and create trace files as long as there is space available before stopping the trace recording session. Once the connection to the TCE becomes active, all cached data will be sent immediately to the TCE.

Data Forwarding

When a session is activated, the IP address of the TCE is supplied in the session activation request. Upon activation and if the push mode is used, a check is made to see if there is already an (S)FTP connection to the TCE. If so, it is used for all traffic associated with this trace session. If not, an (S)FTP connection is made to the TCE using the supplied IP address. Data is buffered locally and trace files generated until the connection is established. Once the connection is established, all previously created trace files are sent to the TCE. Note that the (S)FTP connection is established to the TCE at session activation regardless of whether or not a trace recording session has been triggered. The (S)FTP connection is maintained until the trace session is deactivated.

Note the following:

- If a default TCE IP Address is supplied when the trace capability is configured, a default (S)FTP connection is made to the remote TCE.
- The TCE can be reachable either via IPv4 or IPv6 addressing. The supplied TCE address indicates the version.
- If the push mode is not used, the files are stored on the local hard drive (**/hd-raid/trace**) and must be pulled off by the TCE using FTP or SFTP.

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added for the Session Trace feature:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

Configuring Session Trace Functionality

Configuring Session Trace on the UMTS/EPC network element consists of the following:

1. Enabling Session Tracing, on page 1217
2. Configuring a Session Trace Template for the Management Trace Function, on page 1218
3. Configuring a Management Session Trace, on page 1222
4. Configuring a Signaling Session Trace, on page 1223
5. Configuring a Random Trace, on page 1224

The trace files can be stored locally, or pushed to a Trace Collection Entity (TCE) specified in the various trace commands.



Important Not all combinations of Session Trace configuration types are allowed on the SAEGW. For details on the supported session trace configuration types, refer to Supported SAEGW Session Trace Configurations, on page 1228 in this document.

Enabling Session Tracing

Session Tracing functionality must first be enabled before a specific management, random, or signaling session trace can be configured.

The following commands enable or disable the subscriber session trace functionality based on a specified subscriber device or ID on one or all instances of a session on a specified UMTS/EPC network element.

Use the following example to enable session tracing on the UMTS/EPC network element:

```
config
   session trace network-element { all | ggsn | hnbgw | mme | pgw | saegw
 | sgw } [  file-type <a-type  |  b-type>  ]  tce-mode none | push transport
 ftp | sftp  username  username encrypted password password  path  directory_path
  collection timer  ctimer_value
   end
```

Notes:

- **session trace network-element** : Enables Session Tracing functionality on the specified network element. To enable session tracing for all supported network elements, enter **all**.
- **file-type { a-type | b-type }**: Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. Note that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs. The default is **a-type**.
- **tce-mode** : Specifies that trace files are stored locally and must be pulled by the TCE (**none**) or trace files are pushed to the TCE (**push**). The default is **none**.
- **transport** : Specifies the method by which the trace files are pushed to the TCE (either **ftp** or **sftp**.) The default is **sftp**.

- **username**: Must be specified if the **tce-mode** is **push**.
- **password**: Must be specified if the **tce-mode** is **push**.
- **encrypted**: Specifies that the password used to push files to the TCE server will be encrypted.
- **password**: Specifies the password to use to push files to the TCE server. The user name can be from 1 to 31 alphanumeric characters.
- **collection-timer**: Specifies the amount of time, in seconds, to wait from initial activation/data collection before data is reported to TCE. The default is 10 seconds.
- **retry-timer**: Specifies the amount of time, in seconds, to wait before retrying a file transfer if the previous transfer failed. The default is 60 seconds.

Example:

```
session trace network-element saegw tce-mode push transport sftp path /SessionTrace username
 root encrypted password 5c4a38dc2ff61f72 collection-timer 5
```

Verifying that Session Tracing is Enabled

Use the following example to verify that session tracing functionality is enabled on the UMTS/EPC network element:

show session trace statistics

The output indicates for which NEs session tracing is enabled, and also indicates the configured trace type, where applicable. For example:

```
Network element status:
      MME:      Enabled      Cell-Trace: Disabled
      S-GW:    Enabled
SAEGW Enabled
            PGW:                    Trace-Type: None
            SGW:                    Trace-Type: None
```

Disabling Session Trace Functionality

Use the following example to disable session tracing functionality:

```
config
      no session trace network-element { all | ggsn | hnbgw | mme | pgw
| saegw | sgw }
      end
```

Configuring a Session Trace Template for the Management Trace Function

Operators must create a template for a management trace in Global Configuration Mode. Management traces executed in Exec mode will use the template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

Note that to activate subscriber session traces for specific IMSI/IMEI, the operator will use the Exec mode **session trace subscriber** command specifying a pre-configured template and the IMSI/IMEI, trace reference, and TCE address.

Use the following example to configure a template for use with the **session trace subscriber** command:

```
config
   template-session-trace network-element { ggsn | hnbgw | mme | pgw |
saegw | sgw } template-name template_name
```

Once this command is entered, the user is placed in *Session Trace Template Configuration Mode*. In this mode, the operator selects the interfaces to be traced for the selected network element.

Important The options available in *Session Trace Template Configuration Mode* are dependent on the network element selected in the previous command.

For the **GGSN**, **MME**, **P-GW** and **S-GW**, enter the following command in *Session Trace Template Configuration Mode*:

```
interface interface_name
end
```

For the **SAEGW**, enter the following command in *Session Trace Template Configuration Mode*:

```
{ func-pgw | func-sgw } interface interface_name
end
```

- Notes: The available UMTS/EPC network elements provide various interface options for the session trace template.

GGSN

Available **ggsn** interfaces include:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

HNBGW

Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the iucs interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the iups interface between the HNB-GW and the SGSN.

MME

Available **mme** interfaces include:

- **all**: Specifies that all MME interfaces are to be traced.
- **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.

- **s13**: Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.
- **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

P-GW

Available **pgw** interfaces are:

- **all**: Specifies that all available P-GW interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

SAEGW

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

- Available **func-pgw interface** options are:
  - **all**: Specifies that all available **func-pgw** interfaces are to be traced.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.

- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

- Available **func-sgw interface** options are:
  - **all**: Specifies that all available **func-sgw** interfaces are to be traced.
  - **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
  - **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

S-GW

The available **sgw** interfaces are:

- **all**: Specifies that all available S-GW interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

Verifying the Session Trace Template Configuration

To verify the session trace configuration, enter the following command in Exec Mode.

```
show session trace template network-element { ggsn | hnbgw | mme | pgw |
 saegw | sgw } all
```

The output provides the template name, the NE type, and all interfaces configured for tracing.

Disabling the Session Trace Template Configuration

Use the following example to disable the session trace template configuration:

```
no template-session-trace network-element { ggsn | hnbgw | mme | pgw |
saegw | sgw }
```

Disabling the Session Trace Template Configuration per Network Element and Subscriber

To disable the session trace template per network element and subscriber:

```
no session trace subscriber network-element { ggsn | hnbgw | mme | pgw |
 saegw | sgw } template-name template_name { imsi id | imei id } trace-ref
 trace_ref_value collection-entity ip_address
```

Configuring a Management Session Trace

Session tracing functionality must be enabled before a management trace can be configured. Refer to Enabling Session Tracing, on page 1217 for the procedure.

To configure a management session trace on the UMTS/EPC network element from Exec Mode:

```
session trace subscriber network-element { ggsn | hnbgw | mme | pgw |
saegw | sgw } template-name template_name { imei id | imsi id } { all |
interface } } trace-ref id collection-entity ip_address
```

Notes:

- **template-name**: Specifies the name of the session trace template to use for this session trace. Session trace templates are configured in *Global Configuration Mode* using the **template-session-trace** command. Management traces executed in Exec mode will use the specified template.
- **imsi** *id*: Specifies the International Mobile Subscriber Identification Number for the subscriber.
- **imei** *id*: Specifies the International Mobile Equipment Identification number for the subscriber.
- **trace-ref**: Specifies the Trace Reference for this subscriber management trace. It must be composed of the Mobile Country Code (MCC) + the Mobile Network Code (MNC) + a 3 byte octet string Trace ID. Example: 31001212349.
- **collection-entity**: Specifies the IP address of the Trace Collection Entity (TCE) to which the trace file generated will be sent. The IP address must be in IPv4 format.

Example:

This following is a complete example showing the configuration of a subscriber management trace for all S-GW and P-GW interfaces. It consists of enabling session tracing on the SAEGW, creating the session trace template for all S-GW and P-GW interfaces, and then executing the subscriber management trace for a specific IMSI using the template.

```
config
  session trace network-element saegw
  end
config
  template-session-trace network-element saegw template-name saegw_all
    func-pgw interface all
    func-sgw interface all
    end
session trace subscriber network-element saegw template-name saegw_all imsi
123456789012345 trace-ref 123456789012 collection-entity 209.165.200.225
```

Verifying the Management Trace Configuration

To verify that the management trace configuration for the subscriber is enabled, enter the **show session trace statistics** command from Exec Mode. Verify that the correct NE(s) show their Network element status as **Enabled**. For example:

```
SAEGW Enabled
            PGW:                    Trace-Type: M
            SGW:                    Trace-Type: M
```

Use the following example to verify that specific parameters have been activated for the subscriber management trace:

show session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace-ref *trace_ref_value*

The output fields show the NE Type and the Trace Type configured for each network element. Below is sample output for an SAEGW management trace configuration:

```
NE Type: SAEGW
            PGW:                    Trace-Type:                     M
            SGW:                    Trace-Type:                     M
......
Traced Interfaces:
PGW:
      <P-GW interfaces configured for the trace.>
SGW:
      <S-GW interfaces configured for the trace.>
```

Disabling the Management Trace Configuration

To disable the management trace configuration from Exec Mode:

no session trace subscriber network element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace ref *trace_ref_value*

Configuring a Signaling Session Trace

Session trace functionality must be enabled before a signaling session trace can be configured. Refer to Enabling Session Tracing, on page 1217 for the procedure.

To configure a signaling session trace:

session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw [func-pgw | func-sgw] | sgw }

Notes:

- **func-pgw**Enables tracing of the P-GW signaling under the SAEGW
- **func-sgw**: Enables tracing of the S-GW signaling under the SAEGW
- If neither **func-sgw** or **func-pgw** is specified, then the signaling trace will be performed for all P-GW and S-GW interfaces of the SAEGW.
- **collection-entity**: Specifies the IPv4 or IPv6 address of the Trace Collection Entity (TCE) to which the trace files are sent.

Example:

This example configures a signaling session trace for all S-GW and P-GW interfaces under an SAEGW:

session trace signaling network-element *saegw*

Verifying the Signaling Session Trace Configuration

To verify the signaling session trace configuration:

show session trace statistics

Look for the following fields to verify the signaling trace configuration. For example:

```
Network element status:
......
SAEGW Enabled
          PGW:                    Trace-Type: S
          SGW:                    Trace-Type: S
```

Disabling the Signaling Session Trace

To deactivate signaling trace on the SAEGW:

no session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw [func-pgw | func-sgw] | sgw }

Configuring a Random Trace

Session trace functionality first must be enabled on the UMTS/EPC network element before a random trace can be configured. Refer to Enabling Session Tracing, on page 1217 in this chapter for the procedure.

The following command enables or disables the subscriber session trace functionality based on a random trace on the UMTS/EPC network element. If enabled, the subscriber selection will be based on random logic for all instances of session on a specified network element.

To configure a random session trace:

session trace random *range* **network-element { ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] } interface [all |** *interface* **} collection-entity** *ipv4_address*

Notes:

- **session trace random range**: Enables a random trace for a specified number of subscribers. Valid entries are from 1 to 1000 subscribers.
- **{ ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] }**: Specifies that the random trace is enabled for the selected network element.
- **func-pgw**: Enables random tracing of the P-GW interfaces under the SAEGW.
- **func-sgw**: Enables random tracing of the S-GW interfaces under the SAEGW.
- If neither **func-pgw** or **func-sgw** are specified, random tracing will occur for both the P-GW and S-GW.
- **interface**: Specifies the network interfaces for the random trace. Interfaces available depend on the network element type selected.

GGSN

Available **ggsn** interfaces are:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.

- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

HNBGW

Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the **iucs** interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the **iups** interface between the HNB-GW and the SGSN.

P-GW

Available P-GW interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

SAEGW

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

Available SAEGW **func-pgw interface** options are:

- **all**: Specifies that all **func-pgw** interfaces configured under an SAEGW are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.

- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.

Available SAEGW **func-sgw** interfaces are:

- **all**: Specifies that all available **func-sgw** interfaces under an SAEGW are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

S-GW: Available **sgw** interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

- **collection-entity** specifies the IPv4 address of the Trace Collection Entity (TCE)

Example:

To enable random tracing on a range of 40 SAEGW subscribers on all S-GW interfaces and the s5 interface of the P-GW in the SAEGW, enter the following sample command:

```
session trace random 40 network-element saegw func-pgw interface s5 func-sgw
 interface all collection-entity 209.165.200.225
```

Verifying the Random Trace Configuration

To verify the random session trace configuration:

show session trace statistics

Look for the fields that verify that Random Session Trace has been enabled for the network element. For example:

```
Network element status:
...
SAEGW Enabled
          PGW:                    Trace-Type: R
          SGW:                    Trace-Type: R Configured-Random: 40
```

Disabling the Random Trace for a Specific Network Element

To disable random session tracing for a specific network element:

no session trace random network-element { ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] }

Monitoring the Session Trace Functionality

This section provides information on commands you can use to monitor the session trace functionality

show session trace statistics

This command provides high-level statistics on the current use of the session trace functionality, including:

- Number of current trace sessions
- Number of total trace sessions
- Total sessions activated
- Number of activation failures
- Number of sessions triggered
- Total messages traced
- Number of current TCE connections
- Total number of TCE connections
- Total number of files uploaded to all TCEs

show session trace subscriber network-element trace-ref

This command shows detailed information about a specific trace, based on the trace-ref value of the session and network element type. It includes activation time, IMSI, start time, number of trace messages, and total number of files created. It also lists the interfaces that this session trace is configured to trace.

show session trace trace-summary

This command provides the trace-ref value of all session traces, broken down my network element type.

show session trace tce-summary

This command provides the IP address and index information for all configured TCEs.

show session trace tce-address

This command provides detailed information about a specific TCE, including IP address, start time, and total number of files uploaded.

Supported SAEGW Session Trace Configurations

Different tracing configurations are supported on the SAEGW. The different combinations of session tracing types depend on Call Type, Trace Type, and whether the operator would like to configure a Func-SGW and/or a Func-PGW trace.

Note the following:

- M = Management
- R = Random
- S = Signaling

Table 125: Supported Session Trace Configurations on the SAEGW

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	When M traces are enabled for Func-SGW, Func-PGW and cal type Collapsed botl S-GW control messages (gtpv2) a P-GW control messages shall be traced in 1 SAEGW trace file.
R	R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	S	Collapsed	Yes	Yes	1 SAEGW trace file generated	

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M+S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	When M+S trac enabled for Func-S-GW, Func-P-GW an type collapsed b -SGW control messages (gtpv P-GW control messages shall traced in 2 SAE trace files. One file due to Management an due to Signaling files have the sa contents.
M+R	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	R	Collapsed	No	No	None	Not a valid trac configuration
R	S	Collapsed	No	No	None	Not a valid trac configuration
M	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M	Collapsed	No	Yes	1 SAEGW trace file generated	
M	S	Collapsed	No	Yes	1 SAEGW trace file generated	
S	M	Collapsed	Yes	No	1 SAEGW trace file generated	
M+S	M	Collapsed	Yes	No	2 SAEGW trace files generated	P-GW Trace is generated
M	M+S	Collapsed	No	Yes	2 SAEGW trace files generated, but S-GW trace not generated	S-GW Trace is generated
M+S	S	Collapsed	Yes	Yes	2 SAEGW trace files generated	
S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M+R	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M+R	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M+R	Collapsed	No	Yes	1 SAEGW trace file generated	
M	n/a	Pure S	Yes	No	1 SAEGW trace file generated	Config for func-P-G is not applicable fo Pure S calls
S	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
M+S	n/a	Pure S	Yes	No	2 SAEGW trace files generated	
M+R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R+S	n/a	Pure S	No	No	None	Not a valid trace configuration.
n/a	M	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	S	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	M+S	Pure P	No	Yes	2 SAEGW trace file generated	
n/a	M+R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R+S	Pure P	No	Yes	None	Not a valid trace configuration

Session Trace File Example

This section provides an example of a signaling trace file.

Figure 114: Signaling Trace File Example (1 of 3)

```
<<<<OUTBOUND  10:04:53:997 Eventid:141005(3)
[MME-S11]GTPv2C Tx PDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x000004D3, Message type: EGTP_TRACE_SESSION_ACTIVATION (0x47)
Sequence Number: 0x000401 (1025)
GTP HEADER
        Version number: 2
        TEID flag: Present
        Piggybacking flag: Not present
        Message Length: 0x003A (58)

INFORMATION ELEMENTS
        IMSI:
            Type: 1  Length: 8  Inst: 0
            Value: 123456789012345
            Hex: 0100 0800 2143 6587 0921 43F5

        Trace Info:
            Type: 96  Length: 34  Inst: 0
            Value:
                MCC: 123
                MNC: 456
                Trace Id: 03039

                Triggering Event: 1/0: Event shall be traced / not traced.
                    MSC Server:
                        SS: 0
                        HANDOVERS: 0
                        LU/IMSI ATT/DET: 0
                        MO & MT SMS: 0
                        MO & MT CALLS: 0

                    MGW:
                        CONTEXT: 0

                    SGSN:
                        MBMS CONTEXT: 0
                        RAU/GPRS ATT/DET: 0
                        MO & MT SMS: 0
                        PDP CONTEXT: 0

                    GGSN:
                        MBMS CONTEXT: 0
                        PDP CONTEXT: 0

                    MME:
                        HANDOVERS: 1
                        BEARER ACT/MOD/DEL: 1
                        UE INIT PDN DISC: 1
                        INIT ATT/TAU/DET: 1
                        SERVICE REQUEST: 1
                        UE INIT PDN CON REQ: 1
```

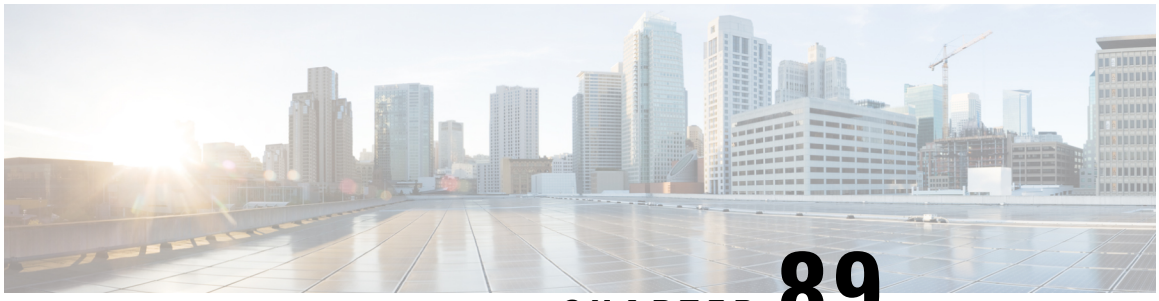
335925

Figure 115: Signaling Trace File Example (2 of 3)

```
PGW:
                            BEARER ACT/MOD/DEL: 1
                            PDN CONN TERMINATE: 1
                            PDN CONN CREATE: 1

                        SGW:
                            BEARER ACT/MOD/DEL: 0
                            PDN CONN TERMINATE: 0
                            PDN CONN CREATE: 0

                    List of NE Types: 1/0: Trace Session activated/ not activated.
                        SGW: 0
                        MME: 1
                        BMSC: 0
                        RNC: 0
                        GGSN: 0
                        SGSN: 0
                        MGW: 0
                        MSC-S: 0
                        ENODEB: 1
                        PDN-GW: 1

                    Trace Depth:
                        Value: 5 (MAXIMUM w/o Vendor Specific Extension)

                    List of Interfaces: 1/0: Interface will be traced/ not traced.
                        MSC Server:
                            CAP: 0
                            MAP-F: 0
                            MAP-E: 0
                            MAP-B: 0
                            MAP-G: 0
                            MC: 0
                            IU: 0
                            A: 0
                            MAP-C: 0
                            MAP-D: 0

                        MGW:
                            IU-UP: 0
                            Nb-UP: 0
                            MC: 0

                        SGSN:
                            GE: 0
                            GS: 0
                            MAP-GF: 0
                            MAP-GD: 0
                            MAP-GR: 0
                            GN: 0
                            IU: 0
                            GB: 0

                        GGSN:
                            GMB: 0
                            GI: 0
                            GN: 0
                                                                        335926
```

Figure 116: Signaling Trace File Example (3 of 3)

```
                RNC:
                    UU: 0
                    IUB: 0
                    IUR: 0
                    IU: 0

                BMSC:
                    GMB: 0

                MME:
                    S11: 1
                    S10: 1
                    S6A: 1
                    S3: 1
                    S1-MME: 1

                SGW:
                    GXC: 0
                    S11: 0
                    S8B: 0
                    S5: 0
                    S4: 0

                PDN-GW:
                    SGi: 0
                    S8B: 1
                    GX: 1
                    S6B: 0
                    S5: 1
                    S2C: 0
                    S2B: 0
                    S2A: 0

                ENODEB:
                    UU: 0
                    X2: 1
                    S1-MME: 1

            TCE IP Addr:
                IPV4 Addr: 1.1.1.1


        Hex: 6000 2200 2163 5400 3039 0000 0000 0000
             003F 7040 0305 0000 0000 0000 0000 1F00
             6803 0101 0101                          335927
```



CHAPTER 89

S-GW Restoration Support

This chapter describes the S-GW Restoration support feature.

- Feature Description, on page 1235
- How it Works, on page 1236
- Configuring S-GW Restoration Support, on page 1237
- Monitoring and Troubleshooting S-GW Restoration Support, on page 1238

Feature Description

S-GW Restoration helps in handling the S-GW failure in the EPC network. It allows affected PDNs that fail due to S-GW to be restored by selecting another S-GW to serve the affected PDNs. This avoids unnecessary flooding of signaling for PDN cleanup.

The P-GW maintains the sessions in case path failure is detected or if S-GW restart is detected during recovery IE on GTP-C signaling. The P-GW will ensure that any dropped packets in this scenario are not charged. The P-GW also rejects any bearer additions or modification requests received for the PDN connection maintained after the S-GW failure detection. This occurs until the PDN is restored.

Once the session has been restored by the MME and the P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW, then the P-GW continues forwarding any received downlink data and start charging them.

When a subscriber is in S-GW restoration phase, all RARs (expect for Session Termination) reject the PCEF. The P-GW rejects all internal updates which can trigger CCR-U towards the PCRF. The P-GW triggers a CCR-U with AN-GW changes for the PDNs that are restored if the S-GW has changed on restoration.

The MME/S4-SGSN is locally configured to know that the P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at the P-GW, it supports it for all S-GWs/MMEs.



Important Only MME/S4-SGSN triggered S-GW restoration procedure will be supported.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

The P-GW Restart Notification may also be used to signal that the peer P-GW has failed and not restarted. In this case, the P-GW Restart Notification contains a cause value: P-GW not responding. While sending the PRN, the S-GW includes the cause with this new cause value depending on the echo response.

Relationships to Other Features

GTP-C path failure detection should be enabled for enabling this feature.

How it Works

Changes at P-GW

If a path failure is detected at the Demux, then the path failure notification is sent to all session managers at the P-GW. Next, the session manager cleans up the ongoing transactions. Once all the transactions are deleted, the sessmgr-egtpc deletes the tunnels by adding them into the pacing queue.

The P-GW will not delete the session immediately after detecting path failure with the S-GW restoration in place. The P-GW discards downlink packets received for a maintained PDN connection and stop charging for maintained PDN connections after an S-GW failure that has not been restored.

The MME/S4-SGSN controls the pace of the S-GW relocations to avoid core network node overload. The MME/S4-SGSN prioritizes the S-GW relocation for UEs engaged in a Service Request for RAU/TAU procedures over UEs which are not engaged in any mobility product procedure and do not have a signaling connection to MME/S4-SGSN.

If a session is marked for S-GW restoration and if a new request results in context replacement, then the existing session is aborted followed by a new request indication event.

Changes at the E-GTPC

When the Demux informs the eGTP-C about the path failure, abort all active procedures. The abort procedure indicates to the P-GW if S-GW restoration is enabled to for the session. Add all the session in the queue and start the session hold timer for S-GW. The MME restores these sessions by relocating sessions to the new or the same S-GW. When the MBReq is received at the P-GW and if the session is marked with S-GW restoration, then the S-GW flag is reset. At this point, the session hold timer expires and S-GW restoration is removed.

Changes at the MME and SGSN

When the MME and SGSN detects path failure towards the S-GW and the MME supports S-GW restoration, then MME relocates sessions from the failed S-GW to another S-GW.

S-GW restoration is supported in MME from Release 21.3 onwards. However, for SGSN, S-GW restoration is not supported.

Demux Failure Detection

The EGTPIN manager detects a path failure and informs all session managers about the failure. Then, the session manager gets the path failure notification and S-GW restoration is enabled so it will stop all ongoing transactions. The Sessmgr-egtpc informs the P-GW-drv about the path failure. The P-GW deletes the session.

Next, the eGTP-C starts the session hold timer. If the MME triggers the S-GW service restoration before the session hold up timer, then sessions from the old S-GW will move to the new S-GW. This ensures that no sessions are handed over and none are deleted.

Once the session hold timer expires, all the sessions with that peer are cleaned up. At this point, new sessions are not moved to the new S-GW.

Important If the S-GW goes down and comes back up in a very short interval, then the P-GW will not detect the path failure. In this case, S-GW restoration does not occur. If the old S-GW comes up again before the hold timer expires, then there is a chance that only some partial sessions move to the new S-GW. In this case, the eGTP-C does not need to delete the remaining sessions with that peer. The eGTP-C will stop the timer.

If the session manager detects the path failure, then it informs the Demux manager. The above, scenario still occurs in this case.

After detecting the path failure, the Demux will not send ECHO messages towards the S-GW. If the new session addition occurs or a new session is restored from the node, then the Demux sends the ECHO messages towards the peer.

Standards Compliance

The S-GW Restoration functionality complies with the following standards:

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point

Configuring S-GW Restoration Support

The session-hold timer is a configurable parameter. The operator can configure this parameter using the **egtpc sgw-restoration session-hold timeout seconds** CLI command.

The **sgw-restoration** keyword enables S-GW restoration functionality and configure session hold timeout on a P-GW service.

When the P-GW detects that the peer S-GW is down (detection is based on restart counter change or PATH failure due to an ECHO response failure), it moves all PDN sessions associated with the peer S-GW to the SGW-RESTORATION-STATE. Also the P-GW starts a timer with the value provided for session-hold timeout per peer S-GW. After timer expiry, the P-GW cleans up all the sessions which are in the SGW-RESTORATION-STATE.

Important By default, S-GW restoration support will not be enabled.

Sample Configuration

Use the following example to enable S-GW Restoration Support.

```
configure
   context context_name
      pgw-service service_name
         egtpc sgw-restoration session-hold timeout seconds
         { default | no } egtpc sgw-restoration session-hold
         end
```

Notes:

- **session-hold timeout** configures session hold timer for S-GW restoration.
- *seconds* must be an integer from 1 to 3600. Default: 0 (disabled).
- On S-GW failure indication, the P-GW checks if the S-GW restoration feature is enabled or not. If enabled, the P-GW maintains all the affected sessions for session-hold timeout. After session-hold timeout, the P-GW clears all the sessions which are not recovered yet.

Verifying the S-GW Configuration

To verify the S-GW Restoration configuration, use the following command:

show pgw-service all

The following fields have been added to display configuration information for S-GW restoration.

- EGTP SGW Restoration Handling
- Session Hold Timer
- Timeout

Monitoring and Troubleshooting S-GW Restoration Support

This section includes show commands in support of the S-GW Restoration.

S-GW Show Commands

This section provides information regarding show commands and/or their outputs in support of the S-GW Restoration.

show ims-authorization policy-control statistics

The following fields have been added to display the statistics introduced in support of S-GW Restoration Support.

- SGW Restoration
- RAR Reject
- Internal Updates Dropped
- Revalidation Timeout

- Pending Updates

show pgw-service statistics all

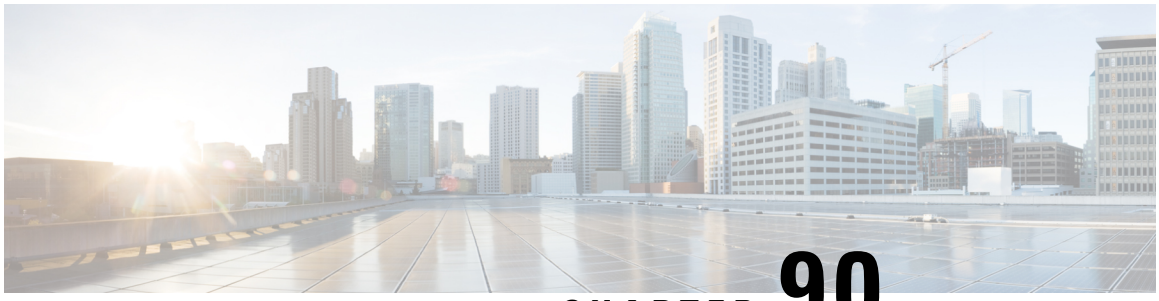
The following counters have been added to display S-GW Restoration Support.

- SGW Restoration Statistics
- PDNs Total
- In Restoration State
- Recovered
- Released
- Drops During SGW Restoration State
- Packets
- Bytes

show subscribers pgw-only full all

The following fields and counters have been added to display S-GW Restoration Support.

- Bearer State
- in packet dropped sgw restoration state
- in bytes dropped sgw restoration state
- out packet dropped sgw restoration state
- out bytes dropped sgw restoration state



CHAPTER 90

Support for Execution-Time AVP in Override-Control AVP

- Feature Summary and Revision History, on page 1241
- Feature Description, on page 1242
- How It Works, on page 1242
- Monitoring and Troubleshooting, on page 1245

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• ECS • P-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*ECS Administration Guide*

Revision History

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

Revision Details	Release
In this release, support is added for Execution-Time AVP in Override-Control AVP to allow the overridden parameters to be specified for a rule (static or predefined), for one or all charging actions (using a wildcard), with the ability to exclude certain rules.	21.3
First introduced.	Pre 21.2

Feature Description

The Override Control (OC) feature, introduced in an earlier release, allowed you to dynamically modify the parameters of static or predefined rules with parameters sent by the PCRF over the Gx interface. Any OC parameters received in RAR/CCA messages was applied immediately by the PCEF. There was no way to enforce the installation of OC at a specified time in future.

The implementation of this feature allows the overridden parameters to be specified for a rule (static or predefined), for one or all charging actions (using a wildcard), with the ability to exclude certain rules. These overrides are sent by the PCRF using the AVP construct in a CCA or RAR message.

As part of this feature, the P-GW supports the following two new AVPs within the proprietary Override-Control grouped AVP:

- Execution-Time (AVP code 132025): This AVP is of type Time. It indicates the Unix Epoch at which the provided Override-Control instance takes effect.
- Override-Control-Pending-Queue-Action (AVP code 132078): This AVP of type ENUM with allowed values FLUSH (0) and RETAIN (1). It indicates the action the gateway takes on the Pending-OC-Queue.

Both the AVPs are included in the Override-Charging-Action-Parameters grouped AVP.

How It Works

The Execution-Time AVP is an optional AVP in the Override-Control grouped AVP, sent in RAR/CCA message by the PCRF. It is valid for Rule-level, Charging-action level, and Wildcard-level OC.

Whenever Override-Control AVP is sent in RAR/CCA message from PCRF, and:

1. it does not contain the Execution-Time AVP, then the existing OC application procedure is adopted for backward compatibility. In other words, the OC parameter is applied immediately by the PCEF.
2. it contains Execution-Time AVP which is in the “Past”, then it is treated as if no Execution-Time AVP was sent and the OC parameter is applied immediately by the PCEF.
3. it contains Execution-Time AVP which is in “Future”, then the PCEF marks the OC as “Pending” and installs the OC when the Execution-Time is reached.

Session Recovery and ICSR

The Pending OCs are recovered on intra/inter chassis session recovery. The PCEF checkpoints Execution-Time using the existing framework that is used for check-pointing of other OC parameters. When the Session Manager restarts or ICSR switchover occurs, timer is started for each of the recovered OC with Execution-Time AVP. The value of this new timer is equal to the time left for the OC to be activated or applied on the call.

If the timer expires during the recovery, then the OC is applied immediately after the recovery.

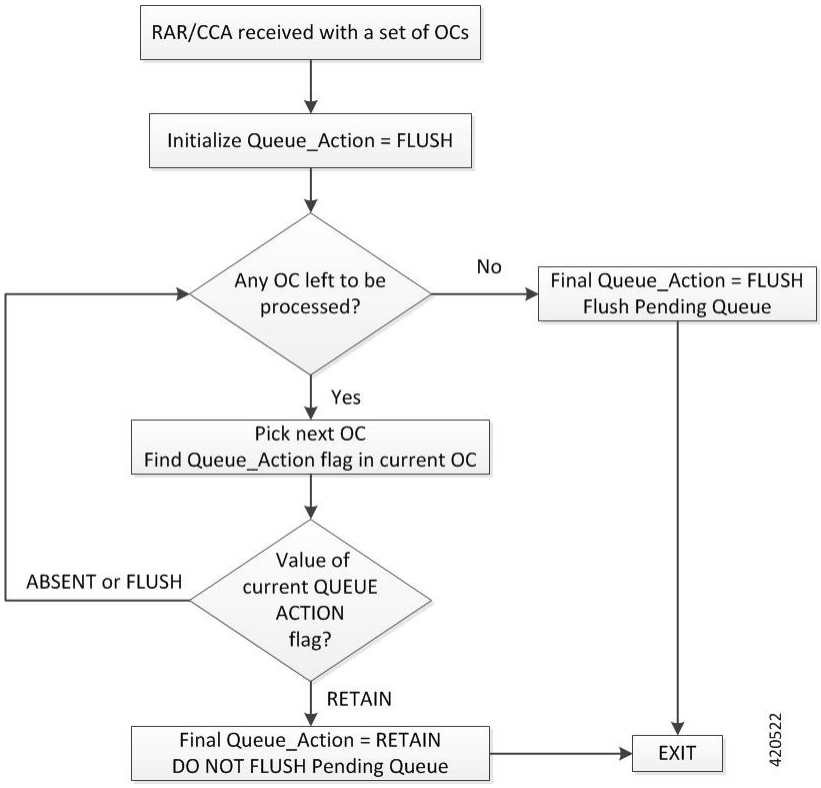
During downgrade from N to N-1 build, the pending OCs on currently active N chassis are not check-pointed to the standby N-1 chassis.

Flushing the Pending OCs

The PCEF decides whether to flush or retain already pending OCs for a subscriber, based on the presence or absence of the Override-Control-Pending-Queue-Action AVP.

On receiving a new OC (with or without Execution-Time AVP) in a new RAR/CCA message, the PCEF flushes all the previous pending OCs for that subscriber. The PCEF either buffers or applies the newly received OC, based on the presence or absence of the Execution-Time AVP respectively. This behavior is the default behavior.

When the requirement is that the Pending OCs should not be flushed, the new AVP, Override-Control-Pending-Queue-Action, is sent within at least one of the Override-Control AVPs in the RAR/CCA message, as shown in the following figure.

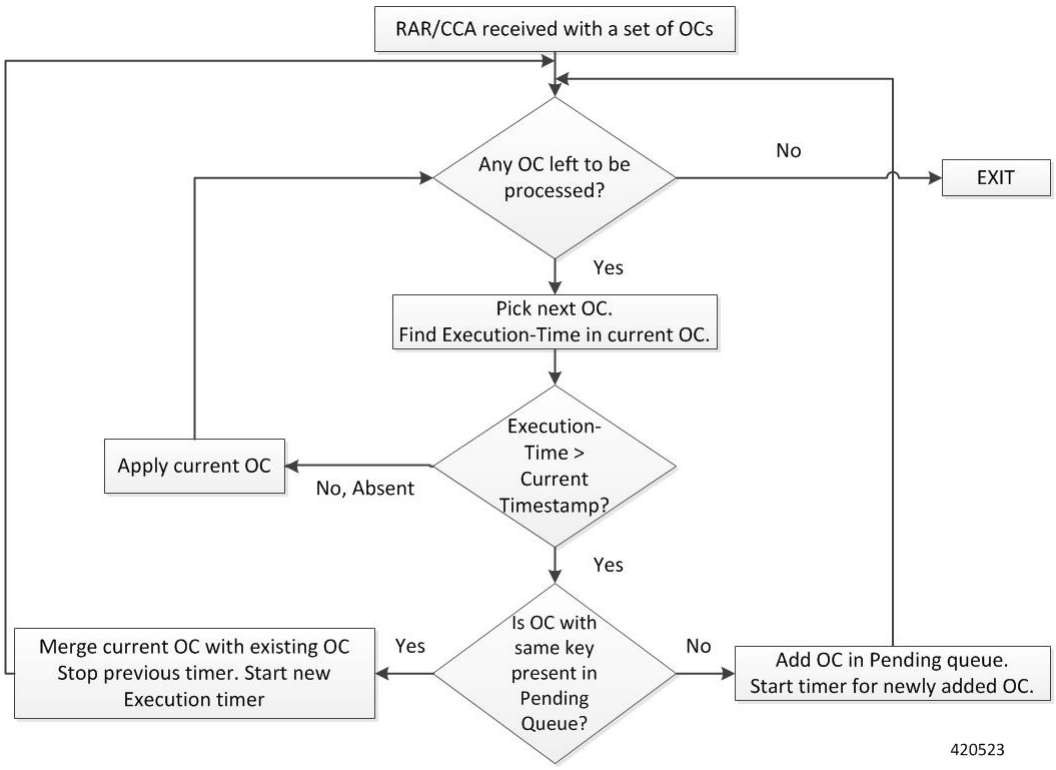


Adding OC in the Pending Queue

The PCEF processes all the instances of Override-Control grouped AVPs received from PCRF in RAR/CCA message. If an Override-Control AVP has an Execution-Time AVP with “Future” time stamp, the PCEF marks it “Pending” for that subscriber. If an OC is received with Execution-Time AVP and there is already an OC pending with same OC identifier, then the newly received OC is merged with the pending OC. The Execution-Time of the merged OC is that of the newly received OC.

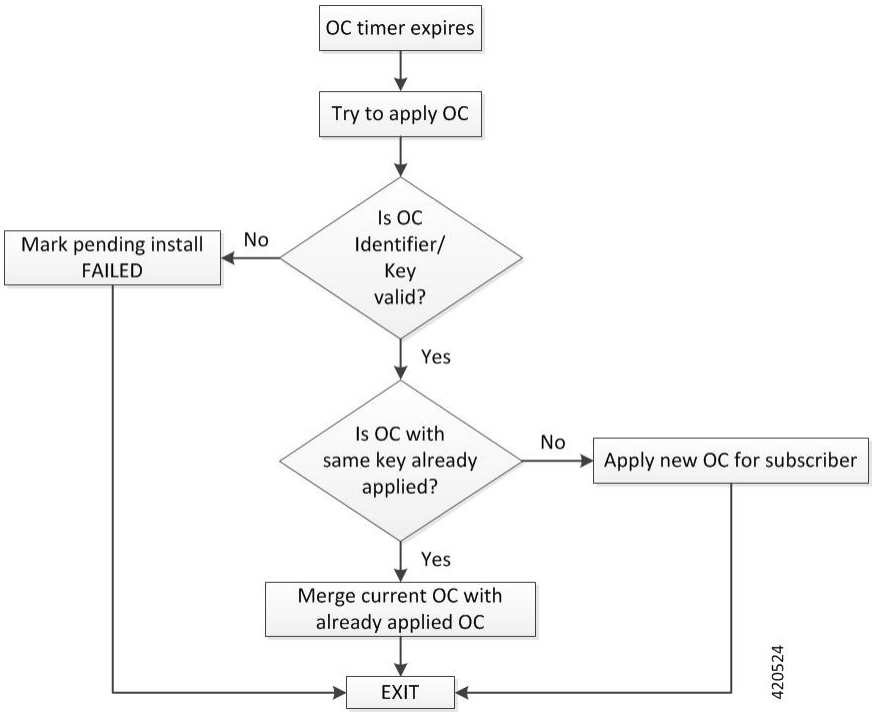
The Override-Control grouped AVP received without the Execution-Time AVP, or with Execution-Time already in “Past”, is not added in the list; in other words, it is applied immediately.

The following figure describes the adding of OC in Pending Queue.



Installing the Pending OC

The PCEF also stores the Execution-Time of all such Pending OCs so that, when the Execution-Time of an OC is reached, the OC is applied to the subscriber as described in the following figure.



Limitations

Following are the known limitations and restrictions of this feature:

- The Execution-Time AVP is supported only for OC without name.
- The maximum time for which an OC can be buffered is 44 days.
- There is no hard limit on number of OCs that can be buffered for a subscriber. However, the decision to buffer an OC depends on the availability of the system resources.
- The OCs with same identifier and different future Execution-Time is merged in the order in which PCEF processes them, and may not be same as the order of occurrence in RAR/CCA. The resultant OC has the Execution-Time of the OC which gets processed at the end.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the feature.

Show Commands and/or Outputs

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

show active-charging subscribers callid <call_id> override-control pending

This new show command has been introduced to check the pending OCs at subscriber-level. Following is a sample output:

```
show active-charging subscribers callid 00004e21 override-control pending
CALLID: 00004e21
Override Control :
  Rule Name :
                     qci2
  Charging Parameters:
    Rating Group     : 100
    Offline Enabled  : TRUE
  Execution-Time     : <Day Month DD HH:MM:SS GMT YYYY>
Override Control :
  Rule Name :
                     qci1
  Charging Parameters:
    Rating Group     : 100
    Offline Enabled  : TRUE
  Policy Parameters:
    QCI              : 4
    ARP Byte         : 81
    MBR UL           : 25000
    MBR DL           : 13000
    TOS UL           : af23 (22)
    TOS DL           : af23 (22)
    NEXTHOP ADDR     : 10.20.10.10
    CF State       : 0
  Execution-Time     : <Day Month DD HH:MM:SS GMT YYYY>
```

show active-charging sessions full all

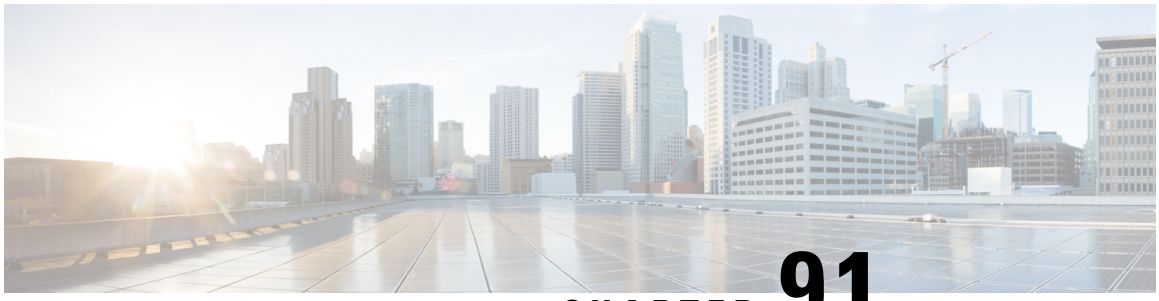
The output of this CLI command has been modified to show information related to pending OCs at subscriber-level. Following is a partial sample output:

```
show active-charging sessions full all
.
.
.
Override Control:
    Installs Received:              2
    Installs Succeeded:             1  Installs Failed:             0
    Install Pending:
      Total  :                      2
      Merged :                      0
      Flushed:                      0
      Failed :                      0
    Disables Received:              0
    Disables Succeeded:             0  Disables Failed:             0

No Charging ruledef(s) match the specified criteria
No Firewall ruledef(s) match the specified criteria

  Post-processing Rulestats : No Post-processing ruledef(s) match the specified criteria
Dynamic Charging Rule Name Statistics: n/a
Total Dynamic Rules:             0
Total L7 Dynamic Rules:          0
Total Predefined Rules:          0
Total ADC Rules:                 0
Total Firewall Predefined Rules: 0
Total Override Control:          0
Total Override Control Pending:  3
```

show active-charging rulebase statistics name <rulebase_name>

The output of this CLI command has been modified to show information related to pending OCs at rulebase-level. Following is a partial sample output:

```
show active-charging rulebase statistics name cisco

    Override Control Statistics:
       Total number of Installs Received:                6
       Total number of Installs Succeeded:               1
       Total number of Installs Failed:                  1
       Install Pending:
         Total:                                          4
         Merged:                                         1
         Flushed:                                        1
         Failed:                                         1
       Total number of Disables Received:                0
       Total number of Disables Succeeded:               0
       Total number of Disables Failed:                  0
       Total number of Subscribers:                      1
```



CHAPTER 91

Support for One Million S1-U Peer-to-Peer Connections

This chapter describes StarOS support for the One Million S1-U Peer-to-Peer Connections feature.

- Feature Description, on page 1249
- How it Works, on page 1249
- Configuring the Feature, on page 1250
- Show Command Output, on page 1251

Feature Description

Due to production forecasts, support has been added to the StarOS for one million S1-U connections on a single S-GW.

The S1-U interface is the user plane interface carrying user data between an eNodeB and an S-GW received from the terminal. The StarOS now has the capability to scale the number of S1-U peers to one million per VPN context.

A CLI command enables operators to set the number of S1-U peers for which statistics should be collected. The limit is restricted to less than one million peers (128k) due to StarOS memory limitations.

How it Works

The gtpumgr uses the following guidelines while allocating peers:

- When a session installation comes from the Session Manager, a peer is created. If statistics are maintained at the Session Manager, the gtpumgr also creates the peer record with the statistics.
- Peer records are maintained per service.
- The number of peers is maintained at the gtpumgr instance level. The limit is one million S1-U peers per gtpumgr instance.
- If the limit of one million peers is exceeded, then peer creation fails. It causes a call installation failure in the gtpumgr, which leads to an audit failure if an audit is triggered.

The feature changes impact all the interfaces/services using the gtpu-service including GGSN/S4-SGSN/S-GW/P-GW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW for:

- The Gn and Gp interfaces of the General Packet Radio Service (GPRS)
- The Iu, Gn, and Gp interfaces of the UMTS system
- The S1-U, S2a, S2b, S4, S5, S8, and S12 interfaces of the Evolved Packet System (EPS)

Recovery/ICSR Considerations

- After a session manager/gtpumgr recovery or after an ICSR switchover, the same set of peers configured for statistics collection is recovered.
  - Peers with 0 sessions and without statistics are not recovered.
  - Peers with 0 sessions and with statistics are recovered.
  - Peers with Extension Header Support disabled are recovered.
- While upgrading from a previous release, ensure the newer release chassis **gtpu peer statistics threshold** is equal to or greater than the previous release. This way the GTPU peer statistics are preserved during the upgrade. For example, if you are upgrading from StarOS release 19.0 to 20.2, and the StarOS 19.0 system has 17,000 GTPU sessions, then configure the threshold on the StarOS 20.2 system to 17,000 as well.

Configuration and Restrictions

- Due to the large number of GTP-U entities connecting to the StarOS, Cisco recommends disabling the GTP-U Path Management feature.
- The configured threshold is not the hard upper limit for statistics allocation because of the distributed nature of system. It is possible that total GTP-U peers with statistics exceeds the configured threshold value to some extent.
- It is assumed that all 1 million peers are not connected to the node in a point-to-point manner. They are connected through routers.
- There will not be any ARP table size change for the StarOS to support this feature.

Configuring the Feature

This section describes how to configure support for the One Million S1-U Peer Connections feature.

gtpu peer statistics threshold

This new command has been added to *Context Configuration Mode* to specify the number of S1-U peers for which the StarOS will maintain statistics.

Use the following example to configure the feature:

```
configure
  context context_name
    gtpu peer statistics threshold value
    end
```

Notes :

- *value* represents the number of S1-U peers for which statistics will be maintained. Valid entries are from 16000 to 128000. The default setting is 16000.
- The threshold cannot be configured to a lower value than the current value.

Show Command Output

This section describes the show command output changes made to support the One Million S1-U Peers feature.

clear gtpu statistics peer-address

The **all** keyword has been added to this command to enable operators to clear statistics for all S1-U peers for which statistics are being maintained.

```
clear gtpu statistics peer-address all
```

show gtpu statistics

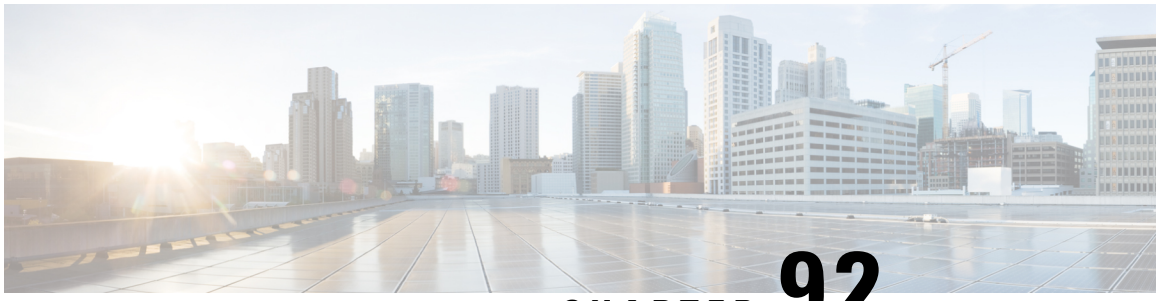
The output of this command has been enhanced to show the total number of GTPU peers, and the total number of GTPU peers configured for statistics collection.

- Total GTPU Peers:
- Total GTPU Peers with stats:

show session subsystem facility sessmgr

The output of this command has been enhanced to provide the total number of S1-U (GTP-U) peers that are configured for statistics collection.

- Total Gtpu Peers with stats



CHAPTER 92

Tethering Detection Bypass Interface ID

- Feature Summary and Revision History, on page 1253
- Feature Description, on page 1253
- Configuring tethering-detection bypass interface-id, on page 1254
- Monitoring and Troubleshooting, on page 1255

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*Command Line Interface Reference*

Revision History

Revision Details	Release
The Tethering Detection Bypass mechanism is enhanced to support multiple interfaces.	21.24.2

Feature Description

In P-GW, the Tethering Detection feature supports up to 10 interface IDs through the CLI and allows bypassing subscribers from tethering rules. If the tethered data flow comes with the configured IPv6 interface IDs, P-GW

bypasses that data from tethering. P-GW also allows deletion of all or multiple interface IDs from the tethering detection bypass list.

Configuring tethering-detection bypass interface-id

Use the following configuration to add, remove, or delete multiple interface IDs.

```
configure
  active-charging-service service_name
    [ no ] tethering-detection {  bypass interface-id ipv6 ifid | tac-db
bypass interface-id ipv6 ifid  }
     default tethering-detection
     exit
  exit
```

NOTES:

- **tethering-detection { bypass interface-id** *ipv6 ifid* **}**: Configures multiple interface IDs. You can configure a maximum of 10 interface IDs.

  ```
  Example for Multiple interface Ids: tethering-detection bypass
  interface-id 00-00-00-05-47-00-37-44 00-00-00-05-47-00-37-45
  00-00-00-05-47-00-37-46 00-00-00-05-47-00-37-4700-00-00-05-47-00-37-48
  00-00-00-05-47-00-37-49 00-00-00-05-47-00-37-50 00-00-00-05-47-00-37-51
  00-00-00-05-47-00-37-52 00-00-00-05-47-00-37-53
  ```

- **default tethering-detection**: Removes all the configured interfaces.
- **no tethering-detection bypass interface-id** *if-id1 if-idn*: Removes the specified *if-id1* and *if-idn* interfaces if configured.

  If no interface IDs are present, then all the configured intreface IDs are removed.

- **tac-db bypass interface-id** *ipv6 ifid*: Enables TAC-db lookup for specified interface IDs.

Verifying the Configuration

Use the following commands to verify the tethering-detection bypass interface ID configuration.

- **show configuration**
- **show configuration verbose**

Use the following sample commands to verify the configuration.

```
configure
  active-charging-service service_name
    tethering-detection { bypass interface-id  ipv6 ifid  }
    exit
  exit
```

Monitoring and Troubleshooting

This section provides information regarding show commands available for the Tethering Detection feature.

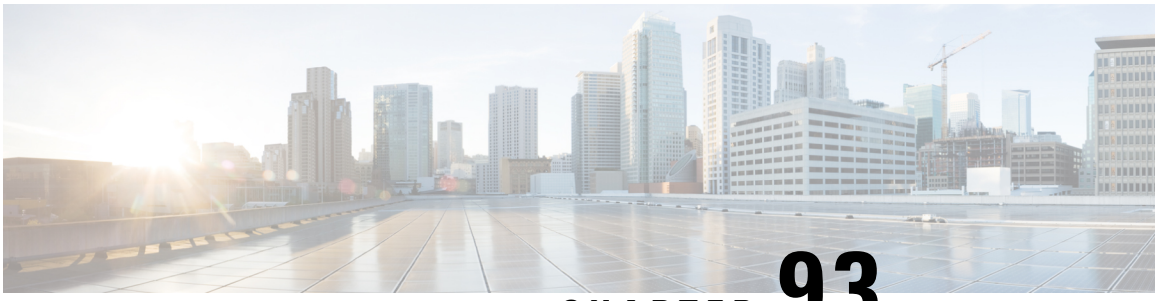
Show Command and Output

This section describes the show command and output to view the current configuration for tethering-detectiion attribute.

show active-charging-tethering-detection statistics

The output of this command includes the following field:

- **Total flows bypassed for scanning**: If a flow gets by-passed on a configured interface Id, the Total flows bypassed for scanning counter is incremented.



CHAPTER 93

TEID Collision with ULI Change

- Feature Summary and Revision History, on page 1257
- Feature Description, on page 1258
- How It Works, on page 1258
- Configuring TEID Collision with ULI Change, on page 1261
- Monitoring and Troubleshooting, on page 1262

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • GGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
With this release, P-GW and GGSN configuration to reject a Tunnel Endpoint Identifier (TEID) collision request with ULI change feature is supported.	21.6.13
First introduced.	Pre 21.2

Feature Description

During Tunnel Endpoint Identifier (TEID) collision scenario, P-GW or GGSN allocates a TEID to a home subscriber. In case of a stale session, in an S-GW or SGSN, the same TEID that is allocated by P-GW or GGSN, is allocated to a roaming subscriber. Then, S-GW sends BRCmd, DBCmd, and MBR messages to P-GW. SGSN sends the Update PDP Context message to P-GW. Due to the same TEID allocation to both the home subscriber and the roaming subscriber, and P-GW having no information on duplicate TEID allocation, P-GW accepts the request. The duplicate use of same TEID leads to the billing for the home subscriber for the data that is used by the roaming subscriber.

To eliminate this scenario, TEID Collision with User Location Information (ULI) change feature is introduced. With this feature, you can configure P-GW and GGSN to reject a request when TEID collision occurs.

TEID Collisions with ULI change feature allows comparison with only Mobile Country Code (MCC) instead of comparison of mcc+mnc. This functionality supports the MOCN scenario on P-GW, SAEGW, and GGSN.

How It Works

The following section provides an overview of the TEID Collision with ULI change feature.

Architecture

For 4G calls, you can configure the TEID Collision with ULI Change feature through CLI in pgw-service in P-GW. For 3G calls, you can configure this feature through CLI in ggsn-service in GGSN. This feature works in the following way for P-GW and GGSN:

- For a home user equipment (UE) in P-GW, a request is rejected if the mobile country code and mobile network code (mcc_mnc) information in ULI differs from the ULI information available in the session for the UE on P-GW. The request is for one of the following messages:
  - Bearer Resource Command
  - Modify Bearer Request
  - Delete Bearer Command
- For a home UE in GGSN, a request is rejected if the mobile country code and mobile network code information in ULI differs from the ULI information available in the session for the UE on GGSN. The request is for the following message:
  - Update PDP context

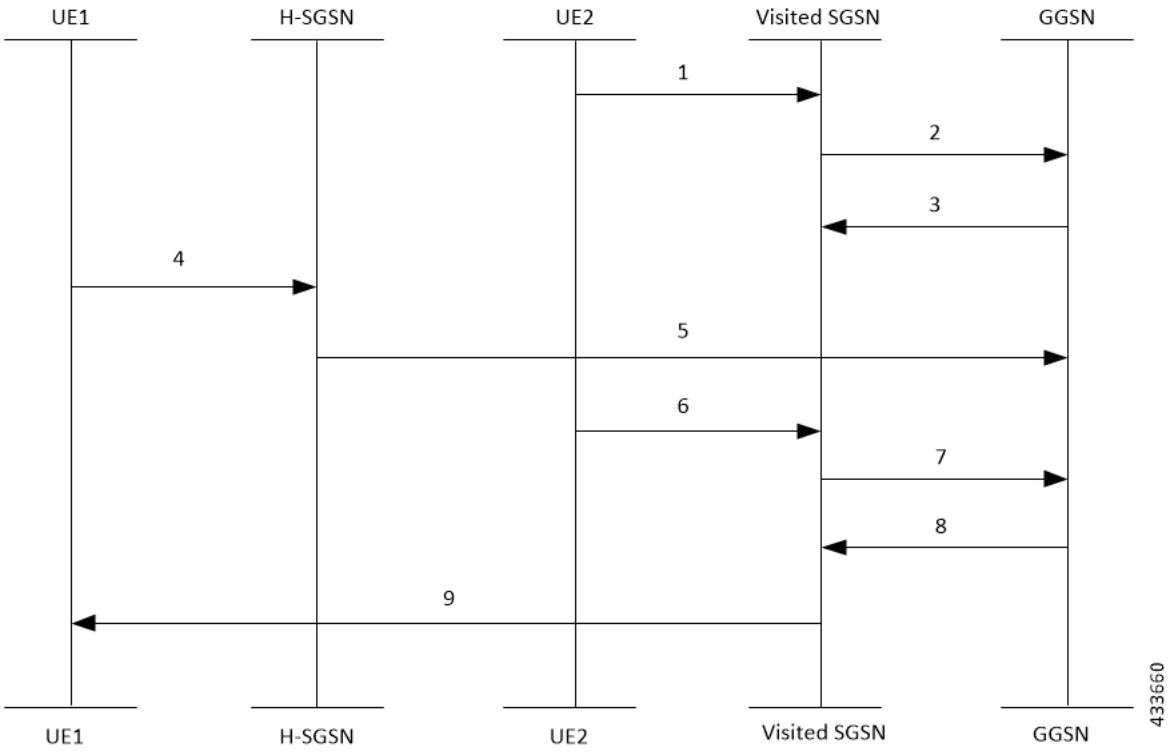
Call Flows

Following call flows show the handling of TEID collision with the ULI change for both P-GW and GGSN.

TEID Collision with ULI Change on GGSN Configuration

Following call flow shows the handling of TEID Collision with ULI Change on GGSN:

Figure 117: GTPC-Based TEID Collision Detection as per ULI Change



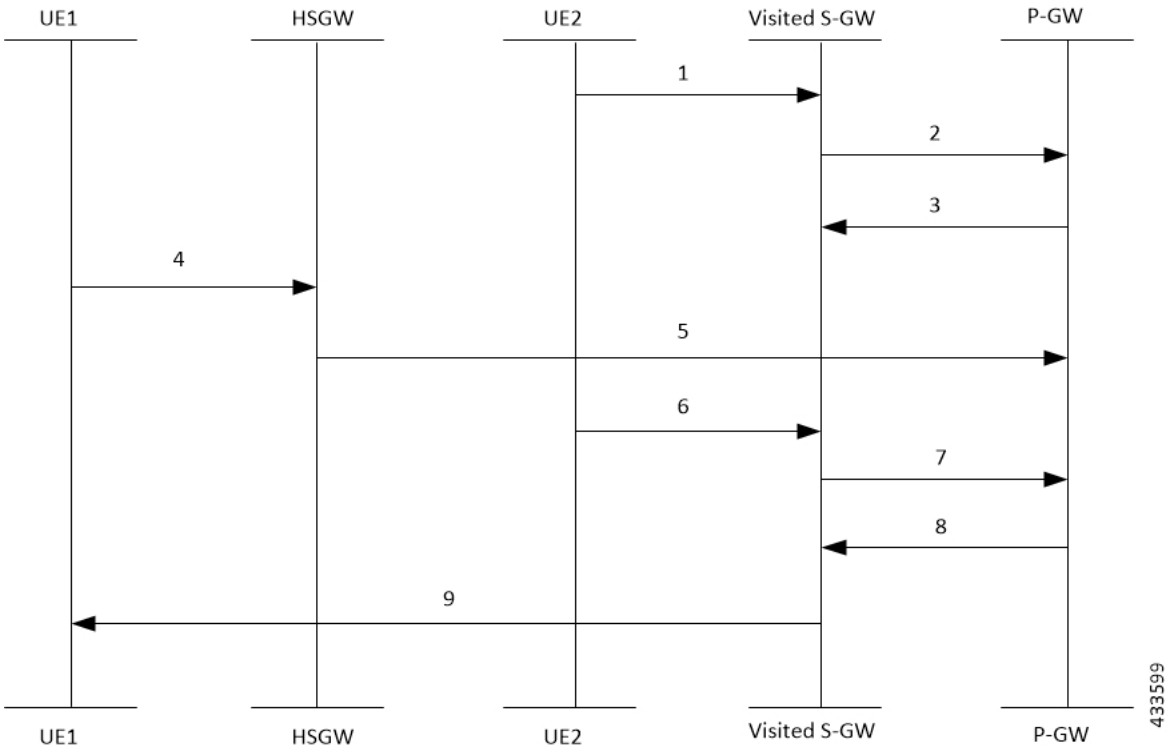
The call flow steps are listed below:

1. When a call is received from roaming subscriber, UE2 attempts to connect to GGSN through visited SGSN.
2. Roaming UE is allocated a TEID-x by the GGSN.
3. After the UE2 disconnects from the network, the session closes on GGSN. However, this session still continues on the visited SGSN.
4. The home UE attach happens on GGSN through home SGSN.
5. GGSN allocates the same TEID-x that was earlier assigned on GGSN.
6. Roaming UE returns to the GGSN. As the session on visited SGSN still exists, same TEID-x is used from visited SGSN.
7. If the TEID Collision with ULI Change feature is enabled at GGSN and the UE1 is in the home PLMN (as in Step 4), all the control requests (GTPv1-C) are processed at GGSN to check for a TEID-based collision as per the ULI change.
8. GGSN checks for MCC only of the ULI against the PLMN-List of the GGSN-Service. If there is no match, GGSM rejects the request. For example, for a HOME UE in GGSN, if the mcc in ULI information differs from PLMN list of the message, the request will be rejected
9. In case of a match, the request is sent for further processing.

TEID Collision with ULI Change for P-GW Configuration

Following call flow shows the handling of TEID Collision with ULI Change on P-GW:

Figure 118: EGTPC-Based TEID Collision Detection as per ULI Change



The call flow steps are listed below:

1. When a call is received from roaming subscriber, UE2 attempts to connect to P-GW through visited S-GW.
2. Roaming UE is allocated a TEID-x by the P-GW.
3. After the UE2 disconnects from the network, the session closes on P-GW. However, this session still continues on the visited S-GW.
4. The home UE attach happens on P-GW through home S-GW.
5. P-GW allocates the same TEID-x that was earlier assigned on P-GW.
6. Roaming UE returns to the P-GW. As the session on visited S-GW still exists, same TEID-x is used from visited S-GW.
7. If the TEID Collision with ULI Change feature is enabled at P-GW and the UE1 is in the home PLMN (as in Step 4), all the control requests (GTPv2-C) are processed at P-GW to check for a TEID-based collision as per the ULI change.
8. P-GW checks only MCC of the ULI against the PLMN-LIST of the PGW-Service. If there is no match, P-GW rejects the request.
9. In case of a match, the request is sent for further processing.

Configuring TEID Collision with ULI Change

This section provides information on the configuration of CLI command to reject a request in a TEID collision scenario on P-GW and GGSN.

Configuring TEID Collision with ULI Change on GGSN

Use the following configuration commands to configure P-GW to reject a request when TEID collision occurs.

```
configure
  context context_name
    ggsn-service service_name
      [ default | no ] gtpc update-pdp-resp reject uli-mismatch mcc-only

        end
```

NOTES:

- **default**: Resets the command to it its default setting—Disabled.
- **no**: Disables the GTPC parameters.
- **update-pdp-resp reject**: Updates the PDP Response reject options.
- **uli-mismatch**: Rejects the update PDP request message if the ULI is not part of the home PLMN session.
- **mcc-only**: Sends update PDP response with NON_EXISTENT (CC 192) cause code if MCC that is received in update PDP request does not match to the HOME PLMN.

Configuring TEID Collision with ULI Change on P-GW

Use the following configuration commands to configure P-GW to reject a request when TEID collision occurs.

```
configure
  context context_name
    pgw-service service_name
      [ default | no ] egtp bearer-req reject uli-mismatch mcc-only
        end
```

Notes:

- **default**: Resets the command to it its default setting—Disabled.
- **no**: Disables the GTPC parameters.
- **bearer-req**: Performs configuration related to handling a Bearer Request.
- **reject**: Shows the Bearer Request reject options.
- **uli-mismatch**: Sends Bearer response with CONTEXT_NOT_FOUND (CC 64) cause code if the ULI that is received in Bearer request does not match with the ULI of the existing session.
- **mcc-only**: Sends Bearer Response with CONTEXT_NOT_FOUND (CC 64) cause code if the ULI with MCC that is received in Bearer request does not match with the MCC of the existing session.

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

This section provides information about show commands and the fields that are introduced in support of TEID Collision with ULI Change.

show egtpc statistics

The output of this show command has been modified to display the following fields for TEID Collision with ULI Change:

- Modify Bearer Request
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Retrans RX
  - Discarded
  - No Rsp RX
- Modify Bearer Response
  - Total TX
  - Initial TX
  - Accepted
  - Denied
  - Retrans TX
  - Total RX
  - Initial RX
  - Accepted
  - Denied
  - Discarded
- Bearer Resource Command
  - Total TX
  - Initial TX

- Retrans TX
- Total RX
- Initial RX
- Retrans RX
- Discarded
- No Rsp RX

- Bearer Resource Failure Indication
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Discarded

- Delete Bearer Command
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Discarded

- Modify Bearer Request Without MME S11u TEID:
  - Local teid Mismatch:
    - Remote teid Mismatch
    - GnGp Call MBReq rejected FTEID absent
    - Tun Remote TEID Updated
    - Teid Collision with uli mismatch for BRcmd
    - Teid Collision with uli mismatch for DBCmd

show gtpc statistics

The output of this show command has been modified to display the following fields for TEID Collision with ULI Change:

- Update PDP Context RX
- Update PDP Context TX

show pgw-service name

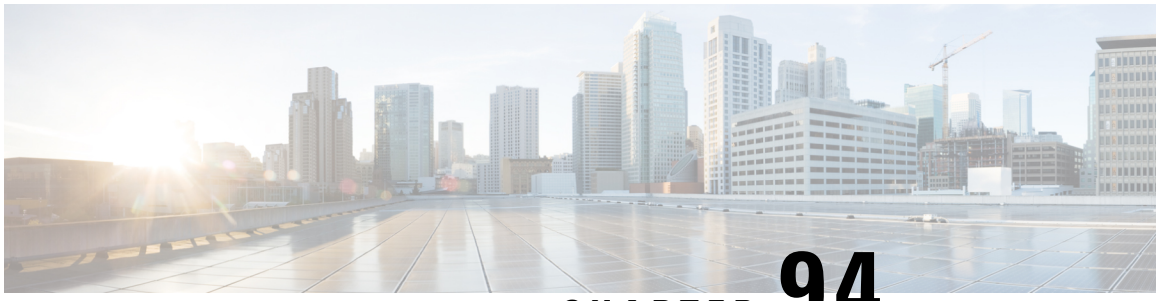
The output of this show command has been modified to display the following fields for TEID Collision ULI Change with only MCC mismatch:

```
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Enabled
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Disabled
```

show ggsn-service name ggsn-service | more

The output of this show command has been modified to display the following fields for TEID Collision ULI Change with only MCC mismatch:

```
GTPC Update PDP Response with Non Existent cause if IMSI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if ULI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if MCC mismatch : Enabled
```



CHAPTER 94

Time-Based Rule Activation and Deactivation

- Feature Summary and Revision History, on page 1265
- Feature Description, on page 1265
- How It Works, on page 1266
- Configuring Time-Based Rule Activation and Deactivation, on page 1268
- Monitoring and Troubleshooting, on page 1269

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
With this release, Time-Based Rule Activation and Deactivation feature is supported.	21.10
First introduced.	Pre 21.2

Feature Description

The 3GPP specification 29.212 allows Policy and Charging Rules Function (PCRF) to send a Policy and Charging Control (PCC) rule, along with Network Time Protocol (NTP) time, at which the rule is activated through Rule-Activation-Time AVP. In earlier releases, StarOS installed the PCC rule when the PCC rule

was received with Rule-Activation-Time. StarOS also created a dedicated bearer, if required, to reserve the network resources. This approach led to the wastage of the network resources and their unavailability in several scenarios, such as:

- When Policy and Charging Rules Function (PCRF) sent a PCC rule.
- When a PCC rule has the Rule-Deactivation-Time AVP, the rule remained installed even after the rule deactivation time completed.

To elimate the wastage of network resources and utilize them as required, the Time-Based Rule Activation and Deactivation feature is developed. With this feature:

- You can install time-based PCC rules after Rule-Activation-Time.
- You can remove time-based PCC rules after Rule-Activation-Time.
- Predefined and dynamic rule maintain their existing behavior.
- Session Recovery and ICSR are supported.

How It Works

The following section provides an overview of the time-based PCC rule activation and deactivation feature.

Architecture

To configure time-based PCC rule activation and deactivation, StarOS saves these rules separately till the rule activation time. When the rules are activated, they are processed and installed as PCC rules. A dedicated bearer is created, if required. The deactivated PCC rules are removed to generate a request to update or delete a bearer.



Note This feature is CLI-controlled to maintain backward compatibility.

Rule Modification Scenarios

When a PCC rule is available with Rule-Activation-Time, StarOS verifies if this feature is enabled or disabled. If the feature is enabled, StarOS does not install the PCC rule immediately. When the Rule-Activation-Time times out, the PCC rule is installed.

Following are some of the rule modification scenarios and the StarOS behaviour in these scenarios:

- If PCRF modifies the rule, for which the timer is running, then StarOS stops the existing timer and starts a new timer by using Rule-Activation-Time.
- If the rule modification does not include Rule-Activation-Time AVP, then StarOS installs the rule immediately. In this scenario, Rule-Activation-Time is not carried forward.
- During the rule modification of time-based rules, parameters of the rules are not merged. It implies that only the parameters that are received in the latest definition are applied.

For example, a time-based rule is received with definition rating-group as 500, charging-id as 10 and Rule-Activation-Time as T1. After some time (before T1), the rule is modified with a new definition of rating-group as 400 and Rule-Activation-Time as T2, then after T2, the rule is installed with parameters rating-group as 400. Here the charging-id is not received for T2 and parameters rating-group has no charging-id.

Default Bearer QoS Change

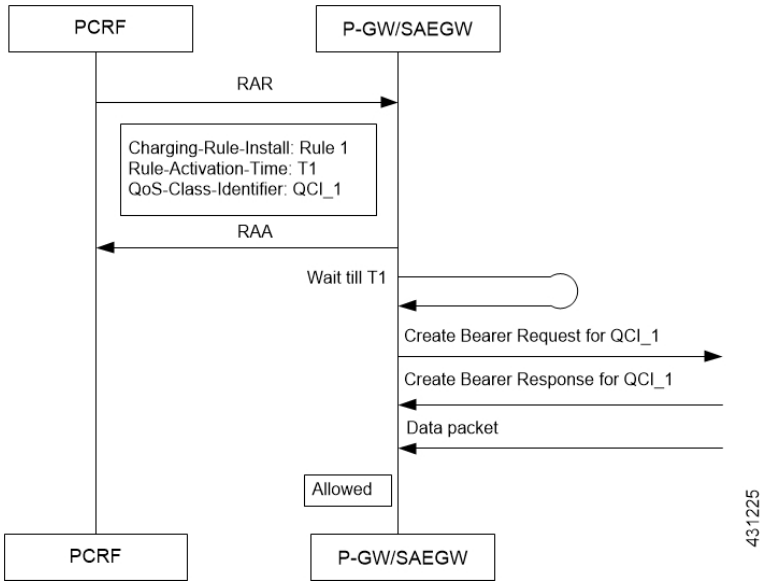
A subscriber has default bearer QoS as QCI_8. PCRF sends the Rule1 rule with QCI_5 and Rule-Activation-Time as T1. Before T1 expires, the default bearer QoS is changed to QCI_5. After T1 expires, the Update Bearer Request is sent on the default bearer to install the Rule1 rule.

Call Flows

Following call flows show the handling of Rule-Activation-Time and Rule-Deactivation-Time.

Rule-Activation Time Configuration

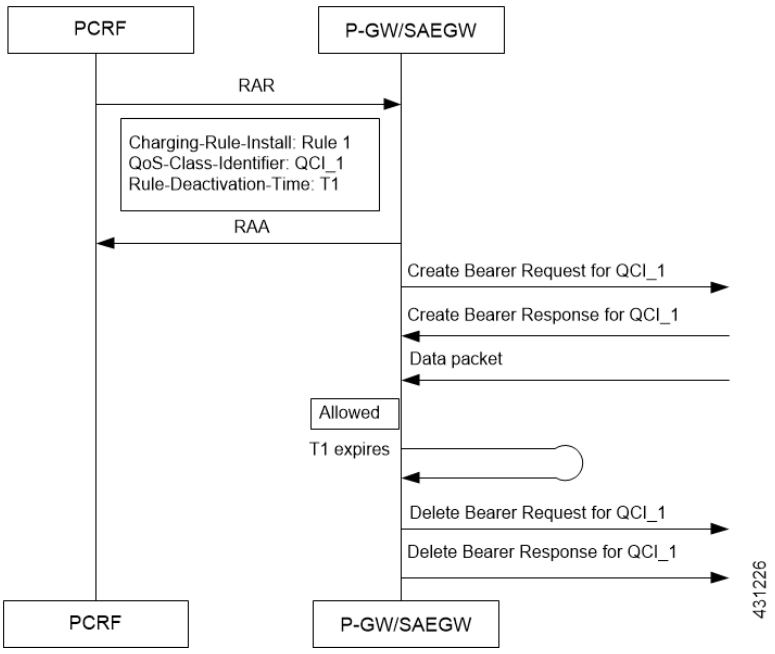
Following call flow shows the handling of Rule-Activation-Time:



In this call flow, no bearer is available with QCI_1 QoS-Class-Identifier. If a bearer with QCI_1 is available, then Update Bearer Request is expected after the T1 timer expires.

Rule-Deactivation Time Configuration

Following call flow shows the handling of Rule-Deactivation-Time:



In this call flow, the bearer with QCI_1 QoS-Class-Identifier has only one rule, which is Rule 1. In case of multiple rules on the bearer, an Update Bearer Request is expected after the T1 timer expires.

Configuring Time-Based Rule Activation and Deactivation

This section provides information on the configuration of CLI command to activate and deactive a time-based PCC rule.

Configuring Time-Based PCC Rule

Use the following configuration commands to configure time-based PCC rule.

```
configure
   require active-charging
   [ default | no ] policy-control time-based-pcc-rule
install-on-activation-time remove-on-deactivation-time
     end
```

Notes:

- **default**: Resets the command to it its default setting—Disabled.
- **no**: Disables the time-based activation or deactivation of a PCC rule.
- **policy-control**: Configures the ACS Policy Control.
- **time-based-pcc-rule**: Configures the PCC rule with activation or deactivation time.
- **install-on-activation-time**: Installs the PCC rule only on activation time.
- **remove-on-deactivation-time**: Removes the PCC rule on the deactivation time.

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

This section provides information about show commands and the fields that are introduced in support of time-based PCC rule activation and deactivation.

show active-charging sessions full callid *callid*

The output of this show command has been modified to display the following fields for Time Based PCC Rule:

- Installs Deferred
- Total Time Based Pending PCC Rules

show active-charging service statistics

The output of this show command has been modified to display the following fields:

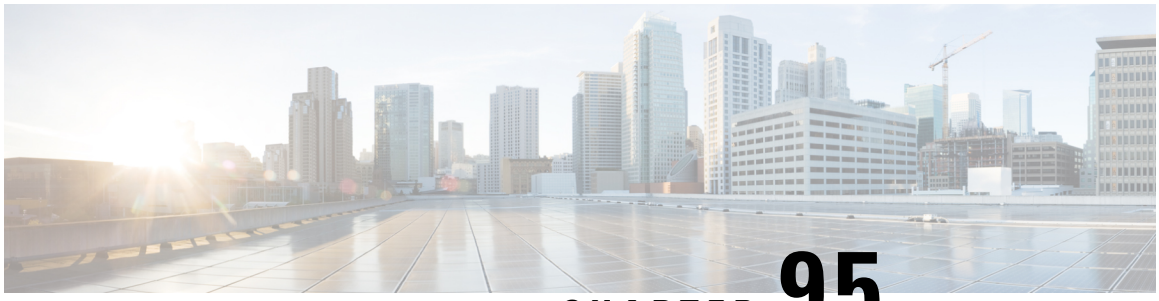
- Time Based PCC Rule Statistics
  - Dynamic Rule
    - Activation-Time Received
    - Deactivation-Time Received
    - Removed received before Activation
    - Removed due to Deactivation
  - Predefined Rule
    - Activation-Time Received
    - Deactivation-Time Received
    - Removed received before Activation
    - Removed due to Deactivation

show active-charging subscribers callid *callid* pending-pcc-rules

The output of this show command has been modified to display the following fields:

- CALLID
- Dynamic Charging Rule Definition(s) Configured
  - Name
  - Prior

    - Content-Id
    - Chrg-Type
    - Rule Parameters
- Status
- Service Identifier
- QoS Class Identifier
- ARP Priority Level
- Reporting Level
- Metering Method
- Uplink MBR
- Downlink MBR
- Uplink GBR
- Downlink GBR
- Rule Activation Time
- Rule De-activation Time
- Filter 1
- Direction
- Protocol
- Dst Addr
- Filter 2
- Direction
- Protocol
- Src Addr
- Predefined Rules Enabled List



CHAPTER 95

Timestamp Accuracy Improvement

- Feature Summary and Revision History, on page 1271
- Feature Description, on page 1272
- Monitoring and Troubleshooting, on page 1272

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
The **show active-charging flows full debug-info all** command is enhanced to display timestamp accuracy between VPP and session manager. For more information, see the *VPP Metric Enhancement* chapter in the *P-GW Administration Guide.*	21.27

Feature Description

When data packets get offloaded, the calculated ticks from the last arrived packet time lag behind the Starent Network Transmission (SNX) global tick time in the session manager. This results in non-synchronization of time between VPP and session manager. As the flow timeout is deducted incorrectly, the flow gets removed from the session.

The **show active-charging flows full debug-info all** command is enhanced to display the correct flow idle timeout.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

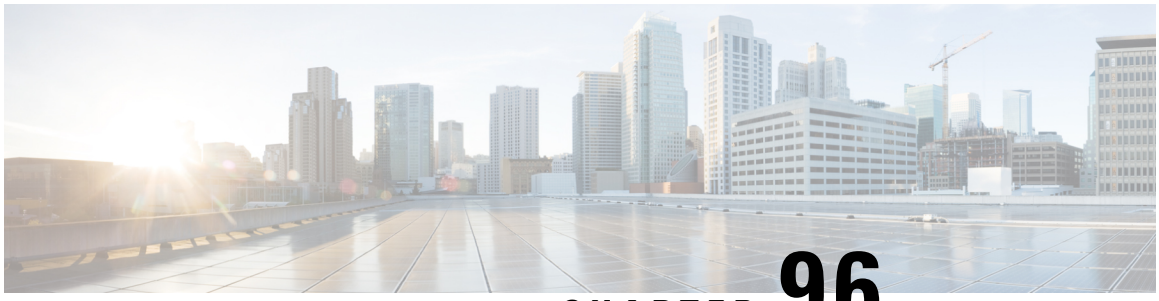
Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging flows full debug-info all

Table 126: show active-charging flows full debug-info all Command Output Descriptions

Field	Description
Last Active Tick Time	Specifies the last active tick time for the data packet.
Current Tick Time	Specifies the current system tick time.



CHAPTER 96

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:

- Feature Description, on page 1273
- Traffic Policing, on page 1273
- Traffic Shaping, on page 1274
- Traffic Policing Configuration, on page 1274
- Traffic Shaping Configuration, on page 1277
- Configuring Traffic Shaping, on page 1280
- RADIUS Attributes, on page 1282

Feature Description

This section describes the traffic policing and traffic shaping for individual subscribers.

Traffic Policing

Traffic policing enables 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.

The Traffic Policing feature uses the Token Bucket algorithm (a modified trTCM) as specified in RFC2698. The algorithm measures the following criteria to determine 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". 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. 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 that provides a buffer facility for packets exceeded the configured limit. Once the packet that exceed 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 uplink directions independently. If there is no more buffer space available for subscriber data the system can be configured to either drop the packets or transmit for the next scheduled traffic session.

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, the 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.

Procedure

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 the APN template's QoS profile in support of Traffic Policing.

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

The 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 converts this rate to a value that is permitted by GTP as shown in the following table:

Table 127: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (for example, 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (for example, 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (for example, 576000, 640000, 704000, ... 86400
From 8,700,000 to 16,000,000	100,000 bps (for example, 8700000, 8800000, 8900000, 16000000)

Procedure

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.

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.

Procedure

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 the APN template's QoS profile in support of Traffic Shaping.

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

The 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 converts this rate to a value that is permitted by GTP as shown in the following table.

Table 128: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (for example, 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (for example, 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (for example, 576000, 640000, 704000, ... 8640000
From 8,700,000 to 16,000,000	100,000 bps (for example, 8700000, 8800000, 8900000, .. 16000000)

Procedure

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*.

Configuring Traffic Shaping

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.

Procedure

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 the APN template's QoS profile in support of Traffic Shaping.

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

The 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 converts this rate to a value that is permitted by GTP as shown in the following table.

Table 129: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (for example, 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (for example, 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (for example, 576000, 640000, 704000, ... 8640000
From 8,700,000 to 16,000,000	100,000 bps (for example, 8700000, 8800000, 8900000, .. 16000000)

Procedure

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 configure Traffic Policing for CDMA subscribers (PDSN and HA) that are configured on remote RADIUS servers. See the *AAA Interface Administration and Reference* for more information on these attributes.

Table 130: RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers

Attribute	Description
SN-QoS-Tp-Dnlk (or SN1-QoS-Tp-Dnlk)	Enable or 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:** This parameter must be configured to the greater of the following two values: 1) 3 times greater than packet MTU for t subscriber connection, OR 2) 3 seconds worth of token accumula 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.

Attribute	Description
SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink committed data rate in bps.
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** This parameter must be configured to at least the greater of following two values: 1) 3 times greater than packet MTU f subscriber connection, OR 2) 3 seconds worth of token accum 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.

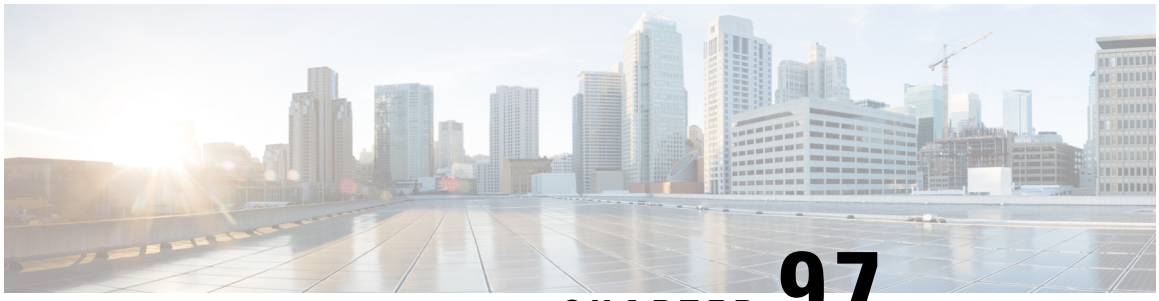
Traffic Policing for UMTS Subscribers

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 131: 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.

Attribute	Description
SN-QoS-Background-Class (or SN1-QoS-Background-Class)	Specifies the QOS Background Traffic Class.
SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)	This compound attribute simplifies sending QoS values for Tra 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 cla If Class is set to 0, it applies across all traffic classes.



CHAPTER 97

Type of Service/Traffic Class Configuration for Predefined Rules

- Feature Summary and Revision History, on page 1285
- Feature Description, on page 1286
- How It Works, on page 1286
- Configuring the TOS/Traffic Class for Predefined Rules , on page 1287
- Monitoring and Troubleshooting, on page 1288

Feature Summary and Revision History

Summary Data

Applicable Product(s) and Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First Introduced	21.3

Feature Description

A traffic flow template (TFT) is an information element that specifies parameters and operations for a Packet Data Protocol (PDP) context. This information element may be used to transfer extra parameters to the network (for example, the Authorization Token; see 3GPP TS 24.229 [95]). The TFT may contain packet filters for the downlink direction, uplink direction, or for both directions.

The packet filters determine the traffic mapping to PDP contexts. Ideally, the network uses the downlink packet filters while the mobile stations use the uplink packet filters. This behavior is also seen for a packet filter that applies to both the directions.

The TFT is a type 4 information element with a minimum length of 3 octets. The maximum length for the IE is 257 octets.

Currently, there is a requirement for an Operator to identify and filter data traffic based on the “Type of Service (TOS)/Traffic class” information. This information needs to be configured as part of the Predefined or Dynamic rules (or both). Also, the Operator wants to send “Type of Service (TOS)/Traffic Class" information as part of TFT in the Create Bearer Request (CBR) and Update Bearer Request (UBR) messages, which can be triggered via the Local Policy or PCRF.

For Dynamic rules, the P-GW already supports "Type of Service (TOS)/Traffic class" information that is used to identify specific data traffic. However, for Predefined rules, there is no option available to configure "Type of Service(TOS)/Traffic class" information as part of packet filter configuration.

This feature introduces the **ip tos-traffic-class** CLI to configure Type of Service (TOS)/Traffic class information in the packet filter configured under charging action to address the Operator requirements.

How It Works

The new CLI configures the packet filter associated with the Predefined rules, with the "Type of Service (TOS)/Traffic Class" configuration. These Predefined rules can be triggered via Local Policy or as part of PCRF communication.

The CLI syntax to configure "Type of Service (TOS)/Traffic Class" information under Predefined rules is in-line with "Type of Service (TOS)/Traffic Class" AVP information that is received as part of the Dynamic rules from PCRF.

According to 3GPPP 24.008 - Section 10.5.6.12, “For "Type of service/Traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet Type-of-Service/Traffic Class field and a one octet Type-of-Service/Traffic Class mask field. The Type-of-Service/Traffic Class field shall be transmitted first.”

For example:

```
toS/traffic class: 0x20 0xff
```

Also, now the P-GW includes both the "Type of Service (TOS)/Traffic class" information under TFT IE, as part of the Create Bearer Request (CBR) and Update Bearer Request (UBR) messages (which is in line with 3GPP 29.212 Section 5.3.14).

Important

- The CLI is added in “packet-filter” configuration mode to configure TOS/Traffic class information.
- While triggering the Create or Update Bearer Request towards a peer, P-GW populates the "Type of Service (TOS)/Traffic class" information under TFT IE if the Predefined rule associated with that bearer is configured with "Type of Service (TOS)/Traffic class" information.
- There is no impact of Session Manager Recovery or ICSR on existing bearer packet filter information.

Limitations

Following are the limitations of this feature:

- Operator should configure TOS along with mask and there are no default values for TOS value and mask.
- For any change of "Type of Service (TOS)/Traffic class" configuration under packet filter, the behavior is in line with the other packet filter parameter configuration change.
- Current PGW/GGSN/SAEGW behavior is that if the Predefined rules installed on the different bearers have ToS/Traffic class configured for uplink traffic on one bearer and downlink traffic on another bearer, then uplink and downlink packets for the same flow go through different bearers accordingly. However, if these Predefined rules with configured ToS/Traffic class are removed on the fly, still uplink and downlink packets for the same flow will go through different bearers.
- Consider the scenario where there are two dedicated bearers installed with Predefined rules such that the uplink traffic with a particular ToS/Traffic class say t1, matches first dedicated bearer and the downlink traffic with another ToS/Traffic class say t2, matches downlink traffic. If the IP ToS/Traffic class CLI is disabled in the corresponding Predefined rules followed by SESSMGR restart, the downlink packets with ToS/Traffic class "t2" will go through the first dedicated bearer instead of second if there is an uplink packet with the same flow (source IP, source port, destination IP, destination port) received before this downlink packet.

Configuring the TOS/Traffic Class for Predefined Rules

The following section provides the configuration command to enable or disable the feature.

Enabling or Disabling the ip tos-traffic-class Command

The modified command, **ip tos-traffic-class**, is used to configure ToS/Traffic class under charging action in the Packet filter mode.

This CLI is disabled by default.

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

```
configure
   active-charging service service_name
      packet-filter packet_filter
         [ no ] ip tos-traffic-class { type_of_service | traffic class } mask
{ mask_value }
         end
```

Notes:

- **no** : If previously configured, deletes the ToS/Traffic class under charging action.
- **tos-traffic-class** = { *type_of_service* | *traffic class* }: Specifies the Type of Service (TOS)/Traffic Class" value that is used to filter the traffic. Enter an integer, ranging from 0 to 255.
- **mask** { *mask_value* }: Validates the dynamic rules for automatic recovery after a switchover. Enter an integer, ranging from 0 to 255.

Monitoring and Troubleshooting

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

Show Commands

This section lists all the show commands available to monitor this feature.

show configuration

This command has been modified to display the following output:

```
show configuration
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      ip  tos-traffic-class = 32 mask = 255
      exit
```

show active-charging packet-filter

This command has been modified to display the following output:

When ToS/Traffic class is enabled/configured:

```
show active-charging packet-filter { all | name }
Service Name: acs

   Packet Filter Name: abcd
      IP Proto: 6
     Local Port: Not configured
     Remote Port: 226
     Remote IP Address: Not configured
     Direction: Bi-Directional
     Priority: None
```

```
    Tos-traffic-class: 32
    Tos-traffic-class-mask: 255
```

When ToS/Traffic class is disabled/not configured:

```
show active-charging packet-filter { all | name }

Service Name: acs

   Packet Filter Name: abcd
      IP Proto: 6
     Local Port: Not configured
     Remote Port: 226
     Remote IP Address: Not configured
     Direction: Bi-Directional
     Priority: None
    Tos-traffic-class: Not configured
    Tos-traffic-class-mask: Not configured
```

show configuration verbose

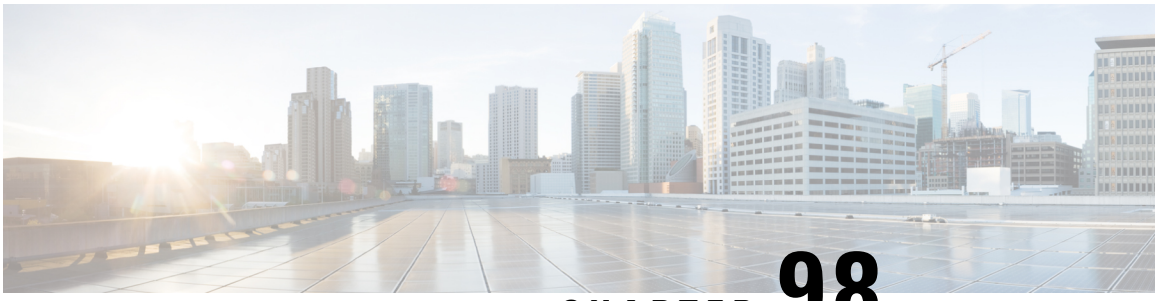
This command has been modified to display the following output:

When ToS/Traffic class is enabled/configured:

```
show configuration verbose
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      ip  tos-traffic-class = 32 mask = 255
      ---
      exit
```

When ToS/Traffic class is disabled/not configured:

```
show configuration verbose
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      no ip   tos-traffic-class
      ---
     exit
```



CHAPTER 98

UE Overload Protection

- Feature Summary and Revision History, on page 1291
- Feature Description, on page 1292
- How it Works, on page 1293
- Limitations, on page 1293
- Configuring ue-overload-control-profile, on page 1294
- Configuring ue-overload Criteria, on page 1294
- Monitoring and Troubleshooting, on page 1296

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.22

Feature Description

The UE Overload Protection feature provides a mechanism to monitor resource utilization of system bandwidth, channel drop rate, SM CPU, SM memory and VPP CPU. When resources exceed configured threshold, certain identified UEs shall be impacted. For example, when system bandwidth resource, which is global, exceeds the configured threshold, the UEs across the system enabled for this feature shall be impacted. Remaining resources are considered as local to CPU complex.

Currently, P-GW supports managing or throttling of traffics and includes the following functions as part of the UE Overload protection functionality:

- Identification of subscriber impact to a P-GW
- Setting thresholds or conditions on the impact of subscriber to a P-GW
- Sending responses to these thresholds by throttling one or more subscribers who exceeded the threshold.

The UE Overload protection feature works only with VPP-enabled ASR 5500 with DPC2 card and other platforms. Threshold handling is applicable only for DPC2 cards (maximum of 6DPC2 cards) that does not include any Demux card. Now you can configure this feature through CLI globally: The following functions are supported:

- Configuration of UE Overload control profiles.
- Managed through PCRF– Enables or disables *ue overload protection* feature for each subscriber and based on the AVP received during the session establishment.
- Allows you to specify configuration actions when thresholds are met. You can adjust the APN-AMBR-DL and APN-AMBR-UL temporarily until the overload condition persists. UE Overload APN AMBR UL/DL values applied to the UEs are reverted to their original values in case of Session Manager restarts, Card migration, and ICSR.



Note If an UE session is under throttling, then APN-AMBR values get modified immediately if the new APN_AMBR values are lesser than the currently applied values. Otherwise, the values are not programmed in the fast path, instead, it gets applied once the threshold is relaxed.

- Allows you to receive periodic load condition (including VPP load) from Resource manager and provision to set up overload condition in Session Manager.
- **show status**: To optimize the system load the **show status** command is organized to show the recent status for up to 18 records and along with system-wide criteria. When the system criteria is met as a lower priority criteria, complex wide higher priority can still override for every complex level based on the complex level threshold crossing. You can view the following results through **show status**:
  - All "met" parameters, when a CPU complex is in throttled state due to one threshold parameter and if other threshold parameters meet on that same CPU complex.

    All threshold parameters, if multiple threshold parameters are met within a given configured criteria.

    The system bandwidth threshold, if met, is displayed as a separate row (last row) in the **show status**. The **Activation Time** for system bandwidth can be any one of the CPU complex activation times.

How it Works

In StarOS, all sessions are distributed across multiple Session Managers. Demux Manager acts as a central element of resource utilization collection at the CPU complex level. When the network traffic speed increases in conjunction with the deployment of 5G, P-GW allows subscribers to manage the performance of the network, such as high-speed downloads, User Equipment (UE) overload detection or recovery scenarios with the help of Demux Manager.

The UE Overload protection feature works on a detection algorithm, which is designed to work and targeted for the DPC2 card-based architecture. However, this algorithm works across different line cards. Following table explains the Overload detection algorithm steps.

Table 132: Workflow

Step	Description
1	Collects resource information at CPU complex level.
2	CLI defines the threshold of the resource utilization.
3	A programmable timer (time provided through CLI) runs the detection algorithm on its expiry and checks against the upper threshold for any of the resource utilizations has crossed the upper threshold limit: • If crossed, then scans for the offending users part of the instance of VPP thread or Session Manager and applies the temporary **APN-AMBR-DL** and **APN-AMBR-UL** threshold values. • Else, waits for the next cycle.
4	Checks recovery algorithm loop (with checks for resource utilization have gone below lower threshold value, which is configured through CLI. If the condition is crossed, then scans for the **APN-AMBR-DL** and **APN-AMBR-UL** instances and replaces with the original **APN-AMBR-DL** and **APN-AMBR-UL** values.
5	Records incidents in the counters to update statistics.
6	Applies timestamp when a criterion is met and used for checking the dampening expiry.

Limitations

The limitations are:

- Works only with VPP-enabled ASR 5500 whereby the load monitoring is performed on the DPC2 card.
- As the intent of this feature is to bring down the system load by throttling the user traffic through AMBR parameters, the operator should take care of enabling the sessions to be throttled.

- The operator must enter the actual name of the APNs at the time of entering the APN names in the list. This is because there is no validation on this list with respect to the APN names used in the system. For APN name, which is not available in the system, the error is not displayed during configuration.You can view the error through the **show config errors** command.

Configuring ue-overload-control-profile

UE Overload feature is applicable only to the new UE sessions that come up after the UE Overload configuration. When you enable the UE Overload configuration for a valid virtual APN(s) or base APN(s), you cannot modify any existing UE sessions to apply the feature.

Use the following commands to configure the ue- overload control profile settings on ASR5500:

```
configure
    context context_name
     ue-overload-control-profile name
        end
```

Notes:

- **ue-overload-control-profile**: Creates a new UE Overload Control Profile without prompting for confirmation.



Note Deletion of an UE Overload profile or an applied/active criteria or applied/active action profile or parameters results in relaxing of applied threshold(s) on a Card/CPU complex immediately.

Any modification of configuration takes effect only in the next *check-interval*.

Configuring ue-overload Criteria

Use the following commands to configure ue-overload criteria.

```
configure
   context context_name
    ue-overload-control-profile overload-criteria  value priority priority_value

        system
           bandwidth-threshold value
           drop-rate-threshold value
       exit
        sessmgr
           cpu-threshold value
           memory-threshold value
        exit
        vpp
           cpu-threshold value
        exit
```

```
overload action name
exit
apn name
    overload-actionname
    downlink-ambrvalue
    uplink-ambrvalue
check-intervalseconds
dampen-intervalseconds
exit
```

Notes:

- **overload-criteria**: Configures Overload criteria thresholds for system, sessmgr, vpp parameters along with criteria priority.

  overload-action: Configures overload action associated with this overload criteria.

- **sessmgr** : Configures Session Manager threshold for various overload criteria parameters.
- **system** : Configures System threshold for various overload criteria parameters.
- **vpp**: Configures VPP threshold for various overload criteria parameters.
- **apn**: Includes APN names to apply for this UE Overload control profile. APN is added in the UE Overload configuration in the following two ways:
  - enable-by-default – UE Overload feature is applicable to the UE sessions if the **UEOVERLOAD** field is enabled in the Service-Feature AVP or if **UEOVERLOAD** field or Service-Feature AVP is altogether missing.
  - enable-by-gx – UE Overload feature is applicable to the UE sessions only if the **UEOVERLOAD** field is enabled in the Service-Feature AVP.

  check-interval: Configures UE Overload parameters monitoring interval (in seconds). The default value is 30 seconds.

- **dampen-interval** : Configures minimum time defined for the system to be in the Overloaded State or Normal State (in seconds). The default value is 300 seconds.
- **default** : Restores default value assigned for following options.
  - **do** : Spawns an exec mode command which displays information to the administrator.
  - **end**: Exits configuration mode and returns to Exec Mode.
  - **exit**: Exits current configuration mode, returns to previous mode.
  - **no**: Enables or disables the following option:
    - **overload-criteria**: Configures Overload criteria thresholds for system, session manager, and VPP parameters along with criteria priority.

Monitoring and Troubleshooting

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show ue-overload-control-profile

The output of this command includes the following fields:

Field	Description
all	Displays all UE Overload Control Profiles.
full	Displays UE Overload Control profile in detail.
name-Displays UE Overload Control Profile names.	
Status	Displays the current status of an UE Overload Control profile.
APN List	Displays APN list that are configured under UE Overload Control profile.

show ue-overload-action

The output of this command includes the following fields:

Field	Description
ue-overload-action	Displays all UE overlaoad action information or criteria and its statistics..
Statistics	Displays total collected information about criteria applied on UEs since its activation.

show ue-overload-control-profile name

The output of this command includes the following fields:

Field	Description
UE Overload Control Profile	
Profile Name	Displays name of the ue-overload control profile.
Status	Displays the current status of the ue-overload control profile.

show ue-overload-profile full all

The output of this command includes the following fields:

Field	Description
UE Overload Control Profiles	
UE Overload Control Profile Name	Displays name of the ue-overload control profile.
Overload-Criteria (s)	
Name	Displays name of the overload criteria.
Priority	Displays the priority of the ue-overload profile.
System	Displays System threshold for various overload criteria parameters.
Sessmgr	Displays Session Manager threshold for various overload criteria parameters. The percentage must be an integer between 0 to100.
vpp	Displays a VPP CPU utilization threshold in percentage.
Bandwidth threshold	Displays a System bandwidth threshold in percentage.
drop-rate threshold	Displays System drop-rate in pps.
cpu threshold	Displays Session Manager CPU threshold in percentage.
memory threshold	Displays Session Manager memory threshold in percentage.
overload-action	Displays the associated UE Overload action profile.
APN (s)	
enable-by-default	Displays all the APNs enabled by default.
enable-by-gx	Displays all APNs enabled by Gx interface.
Check-interval: Displays check interval in seconds. **check-interval** must be an integer ranging from 15 through 300 seconds.	
Dampen-interval: Displays dampen interval in seconds. The **dampen-interval** must be an integer ranging from 30 through 3000 seconds.	

show ue-overload-action statistics full

To optimize the system load, the statistics entries are limited to seven records (six for the complex level and one for the system wide). System-Wide statistics entry is always shown as the last row.

The output of this command includes the following fields.

Field	Description
Profile-name: Displays name of the UE overload profile. **Note** If an UE Overload profile is deleted or if association is removed from SAEGW service, then any statistics collected gets erased.	

Field	Description
Criteria Name (Priority)	Displays Overload criteria name and priority. **Note** In a given criteria, if multiple thresholds are met along with System Bandwidth, then post relaxing the threshold, statistics are collected as part of the System Bandwidth entry.
Activation Time	The activation time of the overload criteria. **Note** For statistics collected post EGTPMGR recovery, the **Activation Time** is displayed as blank.
Activation Duration	The duration up to which the overload criteria was active. **Note** For statistics collected post EGTPMGR recovery, the **Activation Duration** is displayed as blank.
No.of Impacted UEs	Displays the number of UEs for which the temporary UL-AMBR values are applied.
Total UEs	Displays the total number of UEs on the Card/CPU complex **Note** If the **Total UEs** entries are less than the **No.of Impacted UEs**, some UE sessions might go down as the statistics are collected at the Card/CPU-complex when it comes out of threshold.
Card/CPU	The Card/CPU complex for which the particluar criteria was active. If there is a sytem-wide overload action criteria, then it will display as **SYSTEM**. If no UE sessions were throttled on a Card/CPU-complex, then UE session entries are not shown in the statistics even though the Card/CPU complex exceeds any of the configured threshold parameters.

show configuration bulkstats

The following example shows the Bulk Statistics Server Configuration:

```
config
  bulkstats collection
  bulkstats historical collection
  bulkstats mode
    sample-interval 1
    transfer-interval 2
    file 1
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
     receiver 10.105.84.124 primary mechanism ftp login root encrypted password +B3qmvomy0b
 fenh0p6bitcxn3lfs19 febnhcv66ry0uocxu3s2zrze0zompd le3gc7d2bjdm 199d61ny1360gwn1 zr8332rg
 vnjsjvanb4
    #exit
    file 2
      header format UE-AMBR-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
```

```
      receiver 10.105.84.124 primary mechanism ftp login root encrypted password +B0nu
axjhro0b lg2lspsbf12eupo2cxv6ljisgtxb01ap 2239iddb925p69epd in6cc05jm1v96b59uz0moxiz1gsk9qx
 3ijqpsossxi89
    #exit
    file 3
      header format UE-Overload-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
      receiver 10.105.84.124 primary mechanism ftp lo gin root encrypted password
+B3iw43muh3b2j62d9ib6t2jo50232r3dt9ih97iq1ga70qh7r0cbq2a0z j68wpxki22fn9b2t
9i69td06rq782uc83vs2xlfi96h64bi3
      saegw schema ueoverload-stats format
Server1,pgw-apnambrratelimit-ulpktdrop:%pgw-apnambrratelimit-ulpktdrop%,pgw-apnambrratelimit-dlpktdrop:
 %pgw-apnambrratelimit-dlpktdrop%, pgw-apnambrratelimit-ulbytedrop:%pgw-apnambr
ratelimit-ulbytedrop%,
       pgw-apn ambrratelimit-dlbytedrop:%pgw-apn ambrratelimit-
dlbytedrop%,pgw-ueoverload-apnambrratelimit-ulpktdrop:%pgw-ueoverload-apnambrratelimit-ulpktdrop%,
 pgw-ueoverload-apnambrratelimit-dlpktdrop: %pgw-ueoverload-apnambr ratelimit-dlpktdrop%,
       pgw-ueov erload-apnamb rratelimit-ulbytedrop:% pgw-ueoverload-
apnambrratelimit-ulbytedrop%,pgw- ueoverload-apnambrratelimit-dlbytedrop:
%pgw-ueoverload-apnambrratelimit-dlbytedrop%
    #exit
  #exit
end
```

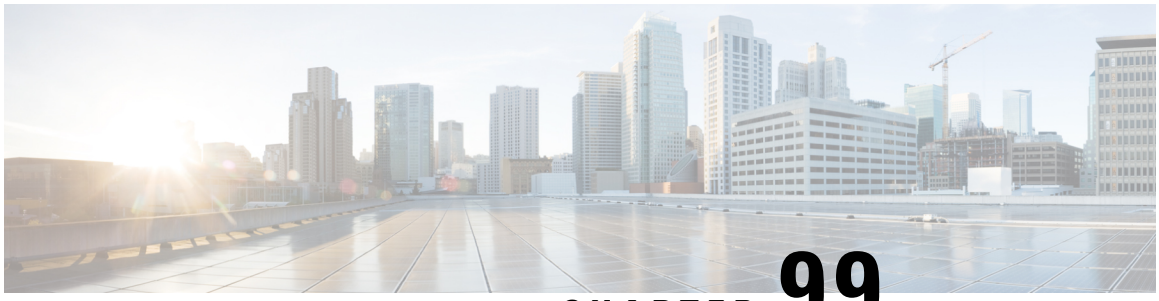
Bulkstats Output on server

```
UE-Overload-drop-stats
Server1,pgw-apnambr ratelimit-ulpktdrop:11060, pgw-apnambrr
atelimit-dlpktdrop:14231,pgw-apnambrra telimit-ulbytedrop:888455,
pgw-apnambrratelimit-dlbytedrop:14965964,
pgw-ueoverload-apnamb rratelimit-ulpktdrop:11060,pgw-ueov erload-apnam br
ratelimit-dlpktdrop:14231,pgw-ueover load-apnambrratelimit-ulbytedrop:888455,
pgw-ueoverload-apnambrratelimit-dl bytedrop:14965964
```

show saegw-service all

The following example shows the results on UE Overload Contol Profile for SAEGW service.

```
Service name                    : SAEGW21
  Service-Id                    : 12
  Context                       : EPC2
  Status                        : STARTED
  sgw-service                   : SGW21
  pgw-service                   : PGW21
  sx-service                    : Not defined
  User Plane Tunnel GTPU Service : Not defined
  Ue Overload Control Profile   : prof-1
  Newcall policy                : n/a
  downlink-dscp-per-call-type   : n/a
  CUPS Enabled                  : No
```



CHAPTER 99

Update Bearer Request Enhancements to Close Charging Gap

- Feature Summary and Revision History, on page 1301
- Feature Description, on page 1302
- How it Works, on page 1302
- Enabling defer default-bearer-rule-removal, on page 1302

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, the P-GW supports deferred rule removal policy to avoid charging discrepancies	21.22

Feature Description

When Re-Auth-Request (RAR) is received on P-GW with **charging-rule-install** and **charging-rule-remove** Attribute Value Pairs (AVPs) with changes in the default bearer Quality of Service Class Index (QCI), P-GW removes the old dynamic charging rule and triggers Update Bearer Request. Only on receiving the Update Bearer Response, the new rule gets applied. This results in charging discrepancies for the time period when no policies are associated with default bearer.

In the StarOS 21.22 and later releases, to avoid charging discrepancies, the rule removal is deferred until Update Bearer Response is received for the above case. This new deferred rule removal policy is applicable only for default bearer with a change in QOS parameters (QCI, GBR, MBR or ARP) and the above condition of **charging-rule-install** and **charging-rule-remove** is satisfied .

How it Works

The Charging rule remove policy is applied after receiving bearer update response and not immediately when RAR is received. This change is supported through CLI configurations and following functions happen::

1. RAR or Credit Control Answer-Update is received by P-GW with Rule remove for Rule1, default bearer QCI update, and Rule install for Rule2.
2. ACS manager verifies the following:
   - Checks for defer rule removal policy.
   - Checks if there is a QOS change for the default bearer and rule remove for default bearer.
   - After Update Bearer Request response is received, removes the stored policy.
3. Verifies if correct QCI, MBR, and GBR values are sent for the Update Bearer Request. Also, verifies if correct default bearer QOS is reflected on the bearer.
4. If update bearer response is not received, then:
   - Performs a timeout handling when you want to cancel the deferred rule removal.
   - Validates the correct bearer QOS restored

Enabling defer default-bearer-rule-removal

Use the following configuration command to enable or disable default bearer rule removal policy.

```
configure
  active-charging service service_name
    [no] policy-controldefer default-bearer-rule-removal
   end
```

Notes:

- **active-charging service**:: Charging actions define the action to take when a rule definition is matched.

- **no**: Disables deferring of dynamic rule remove.
- **defer default-bearer-rule-removal**: Defers removal of rule from default bearer until Update Bearer Response or timeout.



CHAPTER 100

VPP Metric Enhancement

- Feature Summary and Revision History, on page 1305
- Feature Description, on page 1306
- How it Works, on page 1307
- Enabling or Disabling Logging, on page 1307
- Configuring Metrics Collection, on page 1308
- Monitoring and Troubleshooting, on page 1309

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	• Disabled - Configuration Required • Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
The **show active-charging flows full debug-info all** command is enhanced to display timestamp accuracy between VPP and session manager.	21.27
The **show active-charging flows full all** and **show active-charging flows summary**commands are enhanced to get the statistics from VPP.	21.26
The P-GW is enhanced to collect the log messages to monitor offloading and onloading flow transactions between VPP and the session manager.	21.26
The following enhancements were introduced: • Analyzer level statistics (TCP, UDP, P2P, HTTP, HTTPS) • VPP statistics collection using the CLI configuration	21.25
First introduced.	21.24

Feature Description

The Vector Packet Processing (VPP) metrics help to analyze and debug the VPP offloaded traffic. This feature applies only to platforms that support VPP.

Traffic flows are dealt in different ways based on how P-GW recognizes them. For example, some flows are managed with VPP and some are not. To enhance troubleshooting, statistics are added at rulebase, subscriber, and analyzer protocol levels for VPP flows. The supported analyzer protocols include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), peer-to-peer (P2P) analyzer, Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS). System level bulk statistics are supported for troubleshooting.

This feature is partially controlled through the active-charging service configuration. Only the subscriber-specific statistics related to VPP offload are controlled using CLI.

VPP Flow Statistics

The **show active-charging flows full** command is enhanced to receive the per flow information from VPP. This command displays the VPP stream to flow mapping information.

The **show active-charging flows full** and **show active-charging flows summary** commands support the following filters:

- imsi
- ip-address
- msisdn
- username

- callerid
- flow-id
- session-id
- instance



Note Once the idle flow timer expires, the idle flow counters will be incremented. Once the flow is cleared, the counter will be cleared and observed for a short duration of time for the particular flow in idle state.

Monitoring Offloading and Onloading VPP Flow Transactions

The P-GW is enhanced to collect the log messages to monitor offloading and onloading flow transactions between VPP and the session manager. The logs are collected when traffic state changes from offloading to onloading and conversely. The logs are stored in a file. Monitoring can be enabled or disabled using the supported CLI.

Timestamp Accuracy Improvement

When data packets get offloaded, the calculated ticks from the last arrived packet time lag behind the Starent Network Transmission (SNX) global tick time in the session manager. This results in non-synchronization of time between VPP and session manager. As the flow timeout is deducted incorrectly, the flow gets removed from the session.

The **show active-charging flows full debug-info all** command is enhanced to display the correct flow idle timeout.

How it Works

P-GW supports a user-controlled mechanism to monitor traffic offloading to VPP, onloading to sessmgr, and collects the traffic statistics for the monitored period. When the feature is enabled, the logs are saved to */tmp/fpflowchangelog_2021-11-24_02h35m44sEST_1.csv*. Once the logging is disabled, the log file moves to */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv*. If the number of logs exceed 32K, the log file closes and moves to */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_2.csv*. Then, the new file gets created in the rotated index format. The number, for example, *_2.csv* gets incremented and gets saved to */tmp/fpflowchangelog_2021-11-24_02h35m44sEST* with the current stamp. However, the logging continues to happen as usual and the logs are written to the new file.

Enabling or Disabling Logging

The logs are stored in a file in the following format:

```
Timestamp,IMSI, Session-ID, Stream-Idx, Client-IP, Client-Port, Server-IP, Server-Port,
Protocol, Trigger-Type, Trigger-Reason
```

Use the following CLI command in the Exec mode to enable or disable offload and onload logging. By default, the monitoring is disabled:

logging session fp-flow-state-change facility sessmgr instance *instance_number* **number-of-events** *events_value*

logging session fp-flow-state-change facility sessmgr instance *instance_number* **duration** *duration_value*

You will receive the following warning message on enabling the command:

Warning Logging facility for flow state change is now enabled! Logs shall be written to /hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv. Warning: Flow state change logging may have performance impact. Please use with discretion.

If the logging is already enabled when executing the command, you will receive the following message:

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 8 duration
 10
Flow state change event logging is already enabled. Disable before enabling.
```

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 12 duration
 10
Error in flow stream state change logging enable. Invalid parameter.
```

Note Once the configured value for **number-of-events** is met or the duration in seconds elapse, this feature gets disabled automatically.

The event logging must be enabled independent of any other feature or module log.

Configuring Metrics Collection

Use the following sample configuration to enable or disable metrics collection from VPP for subscriber and rulebase.

```
configure
  active-charging service service_name
    [ no ] statistics-collection { all | vpp }
    end
```

NOTES:

- **all**: Configures both Ruledef and VPP statistics collection.
- **vpp**: Configures VPP statistics collection.
- **no**: Resets the seed-time value to the default value of 0.
- By default, this CLI is disabled.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot this feature using show commands and bulk statistics.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging flows full

Table 133: show active-charging flows full Command Output Descriptions

Field	Description
FP-Stream-ID (Up)	Specifies the fastpath stream ID of uplink packets.
FP-Stream-State (Up)	Specifies the fastpath stream state of uplink packets.
FP-Stream-ID (Down)	Specifies the fastpath stream ID of downlink packets.
FP-Stream-State (Down)	Specifies the fastpath stream state of downlink packets.
FP-Client-ID	Specifies the VPP fastpath client ID.
Offload-Stream-at-packet (up)	Specifies the packet number of a stream offloaded from the session manager to VPP when the uplink traffic starts.
Offload-Stream-at-packet (Down)	Specifies the packet number of a stream offloaded from the session manager to VPP when the downlink traffic starts.
VPP FP UL Packets	Specifies the VPP count for uplink packets.
VPP FP UL Bytes	Specifies the VPP count for uplink bytes.
VPP FP DL Packets	Specifies the VPP count for downlink packets.
VPP FP DL Bytes	Specifies the VPP count for downlink bytes.
VPP FP Packets	Specifies total offloaded fastpath packets.
VPP FP Dropped Packets	Specifies dropped packets by VPP.
VPP Onload Succeeded	Specifies total packet onloaded from VPP (onloaded to session manager).
Flow-ID	Identifier for flows.
Session-ID	Identifier for ACS session.
Uplink Packets	The total number of uplinked packets.
Uplink Bytes	The total number of uplinked bytes.

Field	Description
Downlink Packets	The total number of downlinked packets.
Downlink Bytes	Total number of downlinked bytes.
FP Packets	Number of data packets processed in fastpath for this flow.
MS IP	The MS IP address.
MS NAT IP	The MS NAT IP address.
Server IP	The server IP address.
Transport Protocol	The transport protocol: TCP, UDP, ICMP
Application Protocol	The application protocol.
Video Pacing	Indicates whether video pacing is enabled or disabled.
Video Encoded Bit Rate	The currently enforced bit rate for video pacing.
Video Pacing Initial Burst Size	The initial burst size allowed, in bytes, during video pacing.
Video Pacing Normal Burst Size	The normal burst size allowed, in bytes, during video pacing.
Video Pacing Dropped Bytes	The number of data bytes dropped during video pacing.
Video Payload Bytes Sent towards User	The number of data bytes sent to the UE during video pacing.
Video Pacing Duration	The total number of video pacing in seconds.
TCP MS Port	The TCP MS port number.
TCP MS NAT Port	The TCP MS NAT port number. This field is not displayed for one-to-one NAT.
TCP Server Port	The TCP server port number.
TCP State	Indicates the TCP state.
TCP Prev State	Indicates the previous TCP state.
MS Window Size	The mobile window size.
Server Window Size	The server window size.
MS Retries	The total number of mobile subscriber retries.
Server Retries	The total number of server retries.
ITC Action Applied	Indicates that the ITC action is applied.
Throttle-Suppress Countdown	Displays the configured timeout (elapsed time) when flow is throttle-suppressed.

Field	Description
Throttle-Suppress	Displays "n/a" when throttle-suppress is inactive.
Socket Migration Details:	TCP Proxy Socket Migration related information.
State	Indicates the Socket Migration state of the flow. For example, SOCK_MIG_DONE.
Highest ACK Frm Server	The highest acknowledgment number from the server.
Highest Seq Frm Server	The Highest sequence number from the server.
Highest ACK Frm MS	The highest acknowledgement number from the MS.
Highest Seq Frm MS	The highest sequence number from the MS.
Seq Frm MS at Mig	Sequence number from MS at migration.
ACK Frm MS at Mig	Acknowledgement number from MS at migration.
Seq Frm Server at Mig	The sequence number from the server at migration.
ACK Frm Server at Mig	The acknowledgement number from the server at migration.
Data To Be Delivered To MS	Data to be delivered to the MS.
Data To Be Delivered To Server	Data to be delivered to the server.
Highest Seq Frm MS	Highest sequence number from the MS.
Timestamps Enabled	Indicates if timestamps option is enabled.
SACK Enabled	Indicates if selective acknowledgement is enabled.
Wscale From MS	Window scale value from MS.
Wscale From Server	Window scale value from server.
Buffering Statistics:	
Buffered Uplink Packets	The total number of buffered uplink packets.
Buffered Uplink Bytes	The total number of buffered uplink bytes.
Buffered Downlink Packets	The total number of buffered downlink packets.
Buffered Downlink Bytes	The total number of buffered downlink bytes.
Uplink Packets in Buffer	The total number of uplink packets in the buffer.
Uplink Bytes in Buffer	The total number of uplink bytes in the buffer.
Downlink Packets in Buffer	The total number of downlink packets in the buffer.
Downlink Bytes in Buffer	The total number of downlink bytes in the buffer.

Field	Description
Buff Over-limit Uplink Pkts	The total number of uplink packets that are over the limit in the buffer.
Buff Over-limit Uplink Bytes	The total number of uplink bytes that are over the limit in the buffer.
Buff Over-limit Downlink Pkts	The total number of downlink packets that are over the limit in the buffer.
Buff Over-limit Downlink Bytes	The total number of downlink bytes that are over the limit in the buffer.
CAE-Readdressing:	
Requests CAE-Readdressed	The total number of request readdressing done.
Responses CAE-Readdressed	The total number of response readdressing done.
Requests having xheader inserted	The total number of HTTP requests with x-headers inserted.
Total connect failed to CAE	The total number of connections failed to the CAE.
Total CAE-Readdressed Uplink Bytes	The total number of uplink bytes readdressed.
Total CAE-Readdressed Uplink Packets	The total number of uplink packets readdressed.
Total CAE-Readdressed Downlink Bytes	The total number of downlink bytes readdressed.
Total CAE-Readdressed Downlink Packets	The total number of downlink packets readdressed.
Flows connected to CAE	The total number of flows connected to the CAE.
Proxy Disable Success	The total number of flows with proxy disabled.
Proxy Disable Failed	The total number of times the proxy disable function failed.
Link Monitoring	
Average Throughput	The average TCP throughput of downlink TCP traffic towards the mobile device, in kbps.
Average RTT	The average TCP RTT (Round Trip Time) of downlink TCP traffic towards the mobile device, in milliseconds.
Tethering detection performed	Indicates whether tethering detection was performed.
Tethering detected	Indicates whether tethering was detected.
Total ACS flows matching specified criteria	The total number of ACS flows that match the specified criteria.

show active-charging flows full debug-info all

Table 134: show active-charging flows full debug-info all Command Output Descriptions

Field	Description
Last Active Tick Time	Specifies the last active tick time for the data packet.
Current Tick Time	Specifies the current system tick time.

show active-charging flows summary

Table 135: show active-charging flows summary Command Output Descriptions

Field	Description
Current:	
Active Flows	Specifies the total number of active flows currently on the system.
TCP Active flows	Specifies the total number of active flows for TCP traffic.
DNS Active flows	Specifies the total number of active flows for DNS traffic.
ICMPV6 Active flows	Specifies the total number of active flows for ICMPv6 traffic.
Idle Flows:	
TCP Idle flows	Specifies the total number of idle flows for TCP traffic.
UDP Idle flows	Specifies the total number of idle flows for UDP traffic.
ICMPv6 Idle flows	Specifies the total number of idle flows for ICMPv6 traffic.
DNS Idle flows	Specifies the total number of idle flows for DNS traffic.
Cumulative:	
Uplink Packets	Specifies the total number of uplinked packets.
Uplink Bytes	Specifies the total number of uplinked bytes.
Downlink Packets	Specifies the total number of downlinked packets.
Downlink Bytes	Specifies the total number of downlinked bytes.

show active-charging rulebase statistics name

The output of this command displays the following fields:

Table 136: show active-charging rulebase statistics name Command Output Descriptions

Field	Description
VPP Offload Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging subscribers all

The output of this command displays the following fields.

Table 137: show active-charging subscribers all Command Output Descriptions

Field	Description
VPP-PKTS-UP	Total number of packets detected in uplink direction through VPP.

Field	Description
VPP-PKTS-DOWN	Total number of packets detected in downlink direction through VPP.

show-active-charging subscribers full all

The output of this command is enhanced to display the following fields.

Table 138: show active-charging subscribers full all Command Output Descriptions

Field	Description
VPP Offload Statistics: Enabled/Disabled	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging analyzer statistics name

The output of this command displays the following fields. The fields are common for http, secure-http, p2p, tcp, udp.

Table 139: show active-charging analyzer statistics name Command Output Descriptions

Field	Description
Total VPP FP Packets	Total number of Fast Path packets through VPP.
VPP Fastpath Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.

show session fp-flow-state-change statistics

Field	Description
Onload/Offload event logging	Displays the status of logging to show if it is currently enabled or disabled.
Start time	Displays the start time of the last logging. If the logging was never started, the start time shows "NA".
End time	Displays the time when logging was stopped. If logging was never started, the end time shows NA. If the logging is currently enabled, it shows "In progress".
Total events recorded	Displays the total number of logs generated.
Logging enabled for *number of events/ duration*	The number of events or duration in seconds.

Field	Description
Sessmgr Instance	The session manager instance for which the logging is enabled.

Bulk Statistics

The ECS schema includes the following bulk statistics.

ECS Schema

Table 140: Bulk Statistics Variables in the ECS Schema

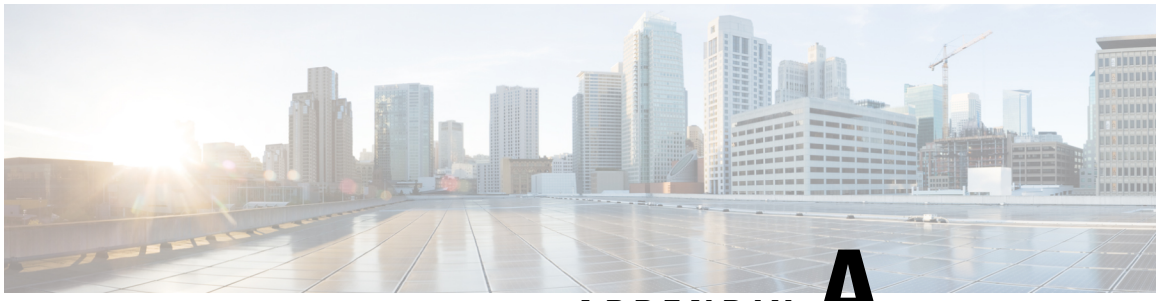
Variables	Description
vpp-tot-flows	Indicates total number of flows through VPP.
vpp-cur-flows	Indicates total number of active current flows through VPP.
IPv4	
vpp-IPv4-uplk-pkts	Indicates total number of IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-pkts	Indicates total number of IPv4 packets detected in downlink direction through VPP.
vpp-IPv4-uplk-bytes	Indicates total number of IPv4 bytes detected in uplink direction through VPP.
vpp-IPv4-dwnlk-bytes	Indicates total number of IPv4 bytes detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in uplink direction through VPP.
vpp-IPv4-dwnlk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in downlink direction through VPP.
IPv6	
vpp-IPv6-uplk-pkts	Indicates total number of IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-pkts	Indicates total number of IPv6 packets detected in downlink direction through VPP.

Variables	Description
vpp-IPv6-uplk-bytes	Indicates total number of IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-bytes	Indicates total number of IPv6 bytes detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in downlink direction through VPP.
TCP	
tcp-vpp-flows-cur	Indicates the current number of flows through VPP for TCP analyzer.
tcp-vpp-flows	Indicates the total number of flows through VPP for TCP analyzer.
tcp-vpp-pkts	The total number of IP packets through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.

Variables	Description
tcp-ipv6-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
UDP	
udp-vpp-flows-cur	Indicates the current number of flows through VPP for UDP analyzer.
udp-vpp-flows	Indicates the total number of flows through VPP for UDP analyzer.
udp-vpp-pkts	Indicates the total number of IP packets through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for UDP analyzer.
HTTP	
http-vpp-flows-cur	Indicates the current number of flows through VPP for HTTP analyzer.
http-vpp-flows	Indicates the total number of flows through VPP for HTTP analyzer.
http-vpp-pkts	Indicates the total number of IP packets through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTP analyzer.

Variables	Description
http-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTP analyzer.
Secure-HTTP	
https-vpp-flows-cur	Indicates the current number of flows through VPP for HTTPS analyzer.
https-vpp-flows	Indicates the total number of flows through VPP for HTTPS analyzer.
https-vpp-pkts	Indicates the total number of IP packets through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTPS analyzer.
P2P	
p2p-vpp-flows-cur	Indicates the current number of flows through VPP for P2P analyzer.
p2p-vpp-flows	Indicates the total number of flows through VPP for P2P analyzer.

Variables	Description
p2p-vpp-pkts	Indicates the total number of IP packets through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for P2P analyzer.



APPENDIX A

P-GW Engineering Rules

This appendix provides PDN Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5500 for your network deployment. General and network-specific rules are located in the appendix of the *System Administration and Configuration Guide* for the specific network type.

The following topics are included:

- Interface and Port Rules, on page 1323
- P-GW Context and Service Rules, on page 1324
- P-GW Subscriber Rules, on page 1324

Interface and Port Rules

The rules discussed in this section pertain to the Ethernet 10/100 line card, the Ethernet 1000 line card and the four-port Quad Gig-E line card and the type of interfaces they facilitate, regardless of the application.

S2a Interface Rules

This section describes the engineering rules for the S2a interface for communications between the Mobility Access Gateway (MAG) service residing on the HSGW and the Local Mobility Anchor (LMA) service residing on the P-GW.

LMA to MAG

The following engineering rules apply to the S2a interface from the LMA service to the MAG service residing on the HSGW:

- An S2a interface is created once the IP address of a logical interface is bound to an LMA service.
- The logical interface(s) that will be used to facilitate the S2a interface(s) must be configured within an ingress context.
- LMA services must be configured within an ingress context.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S2ainterface can be limited in order to allow higher bandwidth per subscriber.

S5/S8 Interface Rules (GTP)

The following engineering rule applies to the S5/S8 interface from the P-GW to the S-GW:

- P-GW preserves an IP address between S2a interface (PMIPv6) and S5/S8 interface (GTP) when the user moves between Wi-Fi and LTE if a common P-GW is used as the anchor point between the two services.

P-GW Context and Service Rules

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

- A maximum of 256 services (regardless of type) can be configured per system.



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.

- The system supports unlimited peer HSGW/MAG addresses per P-GW.
  - The system maintains statistics for a maximum of 8192 peer HSGWs per P-GW service.
  - If more than 8192 HSGWs are attached, older statistics are identified and overwritten.
  - PMIPv6 does not support any peer level statistics (per MAG level statistics).
- The system supports 65,000 S-GW addresses per P-GW.
  - The system maintains statistics for all peer S-GWs per P-GW service.
- The system maintains statistics for a maximum of 64,000 peer P-GWs per HSGW or S-GW service.
- There are a maximum of 8 P-GW assignment tables per context and per chassis.
- The total number of entries per table and per chassis is limited to 256.

P-GW Subscriber Rules

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

- Default subscriber templates may be configured on a per P-GW service.