Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide

Version 10.0

Last Updated July 30, 2010

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

Text Part Number: OL-22985-01

Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide

CONTENTS

About this Guide

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

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

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

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

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

Contacting Customer Support

Use the information in this section to contact customer support.

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

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

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

Chapter 1
PDN Gateway Overview

The Cisco® ASR 5000 provides wireless carriers with a flexible solution that functions as Packet Data Network (PDN) Gateway (P-GW) in 3GPP2 evolved High Rate Packet Data (eHRPD) and Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks.

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

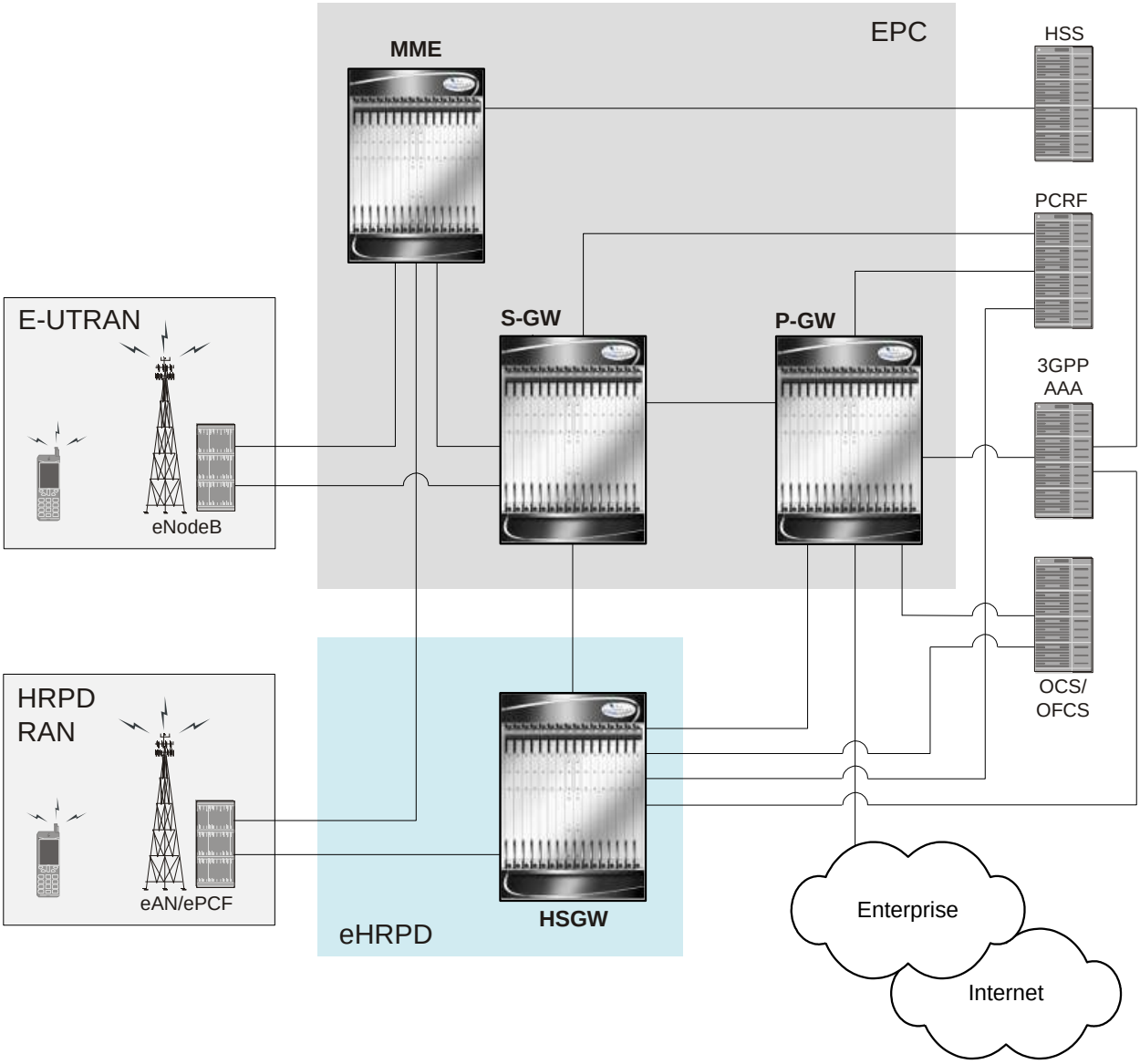
- eHRPD Network Summary
- SAE Network Summary
- Product Description
- Product Specifications
- Network Deployment(s)
- Features and Functionality - Base Software
- Features and Functionality - Inline Service Support
- Features and Functionality - External Application Support
- Features and Functionality - Optional Enhanced Feature Software
- How the PDN Gateway Works
- Supported Standards

eHRPD Network Summary

In a High Rate Packet Data (HRPD) network, mobility is performed using client-based mobile IPv6 or Client Mobile IPv6 (CMIPv6). This involves the mobile node with an IPv6 stack maintaining a binding between its home address and its care-of address. The mobile node must also send mobility management signaling messages to a home agent.

The primary difference in an evolved HRPD (eHRPD) network is the use of network mobility (via proxy) allowing the network to perform mobility management, instead of the mobile node. This form of mobility is known as Proxy Mobile IPv6 (PMIPv6).

One of the eHRPD network's functions is to provide interworking of the mobile node with the 3GPP Evolved Packet Core (EPC). The EPC is a high-bandwidth, low-latency packet network also know as System Architecture Evolution (SAE), supporting the Long Term Evolution Radio Access Network (LTE RAN). The following figure shows the relationship of the eHRPD network with the EPC.



eHRPD Network Components

The eHRPD network is comprised of the following components:

Evolved Access Network (eAN)

The eAN is a logical entity in the radio access network used for radio communications with an access terminal (mobile device). The eAN is equivalent to a base station in 1x systems. The eAN supports operations for EPS – eHRPD RAN in addition to legacy access network capabilities.

Evolved Packet Control Function (ePCF)

The EPCF is an entity in the radio access network that manages the relay of packets between the eAN and the HSGW. The ePCF supports operations for the EPS – eHRPD RAN in addition to legacy packet control functions.

The ePCF supports the following:

- Main service connection over SO59
    - Uses PDN-MUX and allows multiplexing data belonging to multiple PDNs
- Signaling over Main A10
    - LCP messages for PPP link establishment
    - EAP messages used for authentication
    - VSNCP messages for establishment of PDNs
    - VSNP for establishment of EPS bearers and QoS mappings (RSVP)

HRPD Serving Gateway (HSGW)

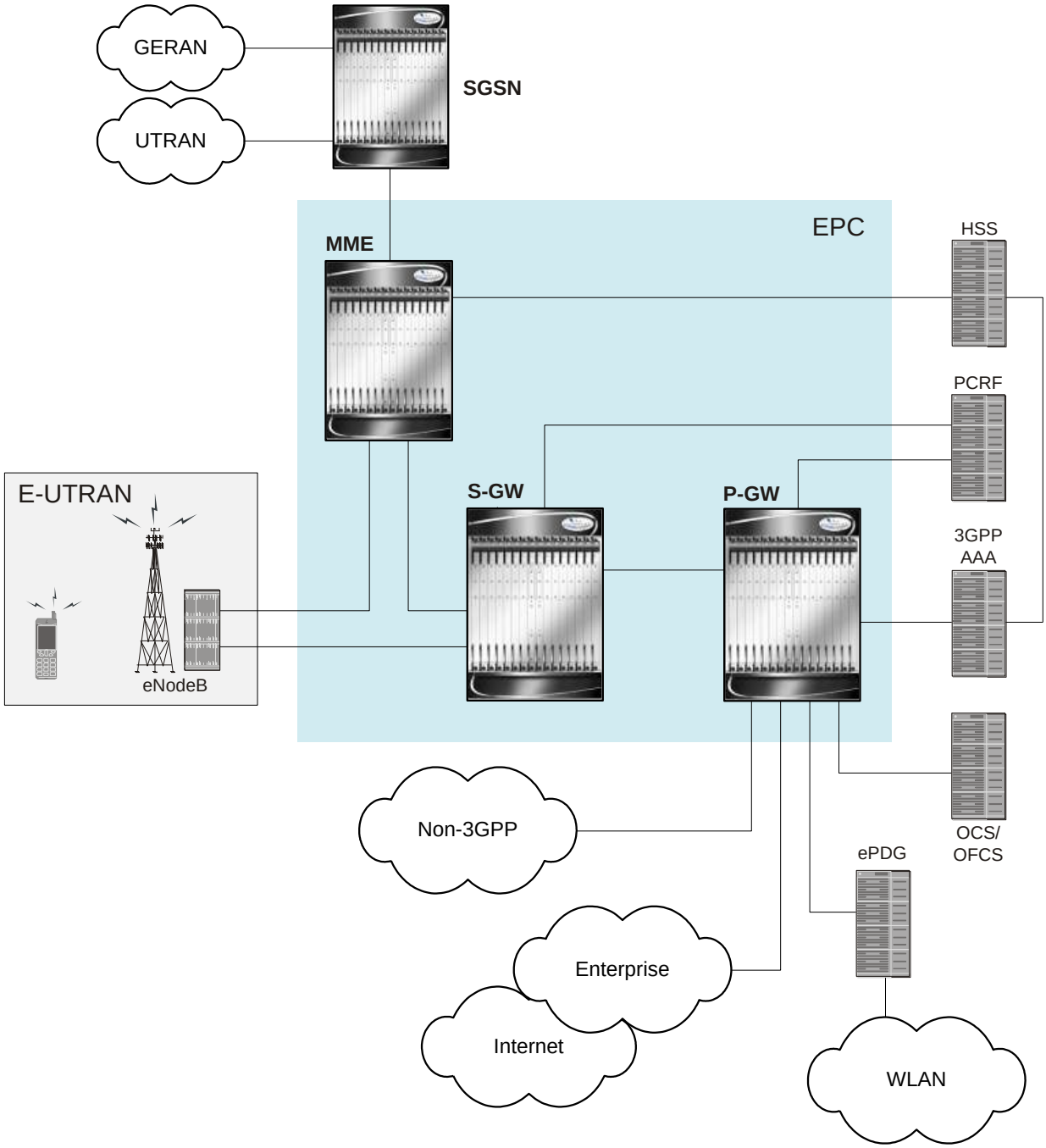
The HSGW is the entity that terminates the HRPD access network interface from the eAN/PCF. The HSGW functionality provides interworking of the AT with the 3GPP EPS architecture and protocols specified in 23.402 (mobility, policy control (PCC), and roaming). The HSGW supports efficient (seamless) inter-technology mobility between LTE and HRPD with the following requirements:

- Sub 300ms bearer interruption
- Inter-technology handoff between 3GPP E-UTRAN and HRPD
- Intra-technology handoff between an HSGW and an existing PDSN
- Support for inter-HSGW fast handoff via PMIPv6 Binding Update

SAE Network Summary

The System Architecture Evolution was developed to provide a migration path for 3GPP systems and introduce higher data rates and lower latency for a variety of radio access technologies. SAE defines the packet network supporting the high-bandwidth radio network as the Evolved Packet Core (EPC). The EPC provides mobility between 3GPP (GSM, UMTS, and LTE) and non-3GPP radio access technologies, including CDMA, WiMAX, WiFi, High Rate Packet Data (HRPD), evolved HRPD, and ETSI defined TISPAN networks.

The following figure shows the interworking of the EPC with the different radio access technologies.



E-UTRAN EPC Network Components

The E-UTRAN EPC network is comprised of the following components:

eNodeB

The eNodeB is the LTE base station and is one of two nodes in the SAE Architecture user plane (the other is the S-GW). The eNodeB communicates with other eNodeBs via the X2 interface. The eNodeB communicates with the EPC via the S1 interface. The user plane interface is the S1-U connection to S-GW. The signaling plane interface is the S1-MME connection to MME.

Basic functions supported include:

- Radio resource management, radio bearer control, and scheduling
- IP header compression and encryption of user data streams
- Selection of MME at UE attachment (if not determined by information sent from the UE)
- Scheduling and transmission of paging messages (originated from the MME)
- Scheduling and transmission of broadcast information (originated from the MME or OA&M)
- Measurement & measurement reporting configuration for mobility and scheduling

Mobility Management Entity (MME)

The MME is the key control-node for the LTE access-network. The MME provides the following basic functions:

- NAS
  - signalling
  - signalling security
- UE access in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area (TA) list management
- P-GW and S-GW selection
- MME selection for handovers with MME change
- SGSN selection for handovers to 2G or 3G 3GPP access networks
- Terminates interface to HSS (S6a)
- Authentication
- Bearer management functions including dedicated bearer establishment
- HRPD access node (terminating S101 reference point) selection for handovers to HRPD
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows

Serving Gateway (S-GW)

For each UE associated with the EPS, there is a single S-GW at any given time providing the following basic functions:

- Terminates the interface towards E-UTRAN (S1-U)
- Functions (for both the GTP-based and the PMIP-based S5/S8) include:
  - local mobility anchor point for inter-eNodeB handover
  - mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and PDN GW)
  - ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
  - lawful intercept
  - packet routing and forwarding
  - transport level packet marking in the uplink and the downlink (e.g. setting the DiffServ Code Point)
  - Accounting
- Handling of Router Solicitation and Router Advertisement messages if PMIP based S5 and S8 are used
- MAG for PMIP based S5 and S8

PDN Gateway (P-GW)

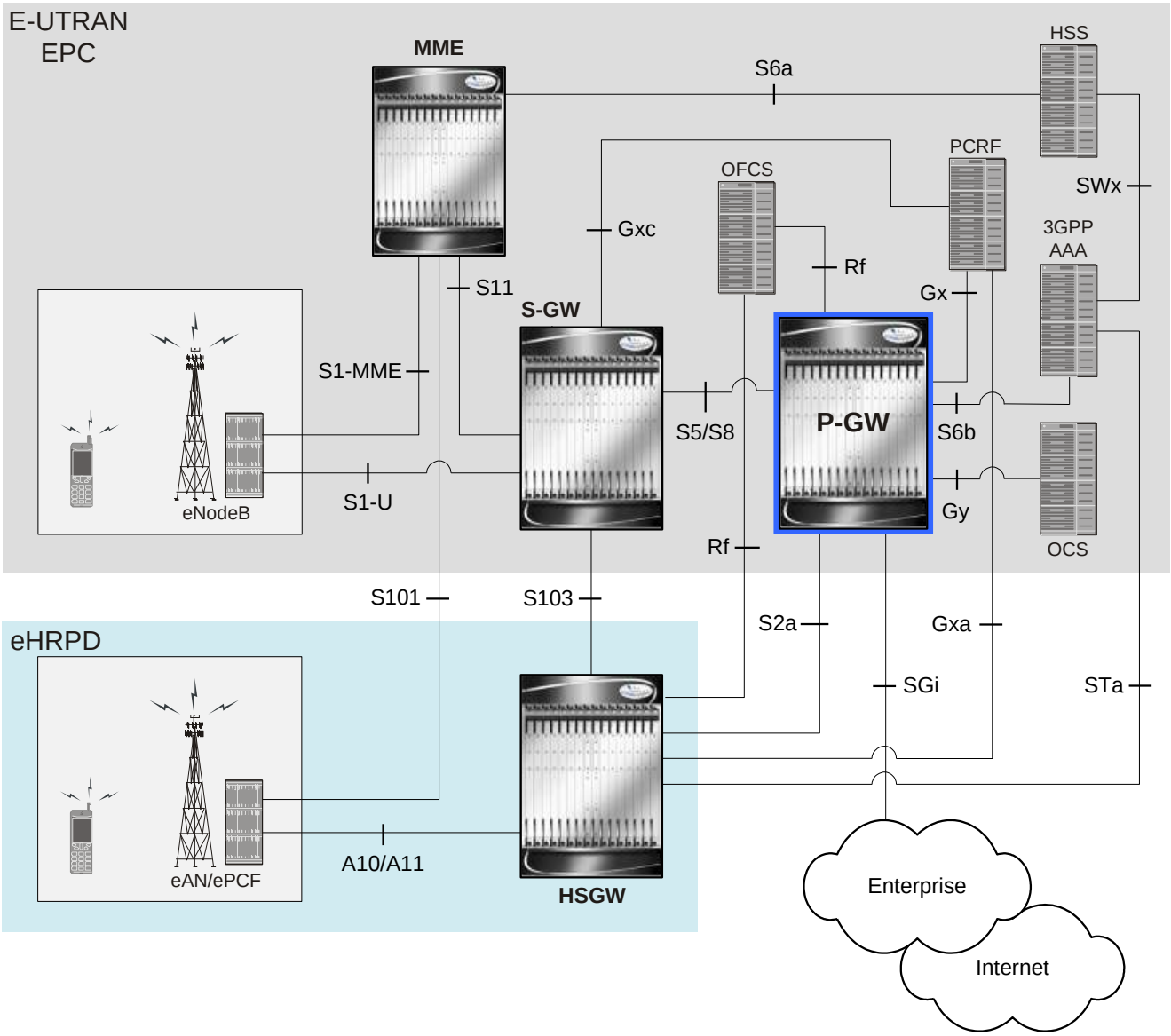
For each UE associated with the EPS, there is at least one P-GW providing access to the requested PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides the following basic functions:

- Terminates the interface towards the PDN (SGi)
- PGW functions (for both the GTP-based and the PMIP-based S5/S8) include:
  - per-user packet filtering (e.g. deep packet inspection)
  - lawful intercept
  - UE IP address allocation
  - UL and DL service level charging, gating control, and service level rate enforcement
  - DL rate enforcement based on AMBR (Aggregate Max Bit Rate) and based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI
  - DHCPv4 and DHCPv6 functions (client, relay and server)
- LMA for PMIPv6

Product Description

The PDN Gateway 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. Basic E-UTRAN/EPC and eHRPD Network Topology



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.

Product Specifications

The following information is located in this section:

- Licenses
- Hardware Requirements
- Operating System Requirements

Licenses

The P-GW is a licensed product. A session use license key must be acquired and installed to use the P-GW service.

The following licenses are available for this product:

- P-GW Software License, 10k Sessions - 600-00-7642
- P-GW Software License, 1k Sessions - 600-00-7649

Hardware Requirements

Information in this section describes the hardware required to enable P-GW services.

Platforms

The P-GW service operates on the following platforms:

- ASR 5000 Chassis

Components

The following application and line cards are required to support P-GW functionality on an ASR 5000 platform:

- **System Management Cards (SMCs)**: Provides full system control and management of all cards within the ASR 5000 platform. Up to two SMC can be installed; one active, one redundant.

- **Packet Services Cards (PSCs/PSC2s)**: Within the ASR 5000 platform, PSCs/PSC2s provide high-speed, multi-threaded PDP context processing capabilities for 4G P-GW services. Up to 14 PSCs/PSC2s can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs)**: Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, central office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Line Cards:** Installed directly behind PSCs, these cards provide the physical interfaces to elements in the E-UTRAN EPC data network. Up to 26 line cards can be installed for a fully loaded system with 13 active PSCs/PSC2s, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs do not require line cards.
    - Ethernet 10/100 and/or Ethernet 1000 line cards for IP connections to other network elements.
- **Redundancy Crossbar Cards (RCCs)**: Installed in the lower-rear chassis slots directly behind the SPCs/SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs.

Important: Additional information pertaining to each of the application and line cards required to support LTE-SAE services is located in the Hardware Platform Overview chapter of the *ASR 5000 Series Product Overview Guide*.

Operating System Requirements

The P-GW is available for the ASR 5000 chassis running StarOS Release 9.0 or later.

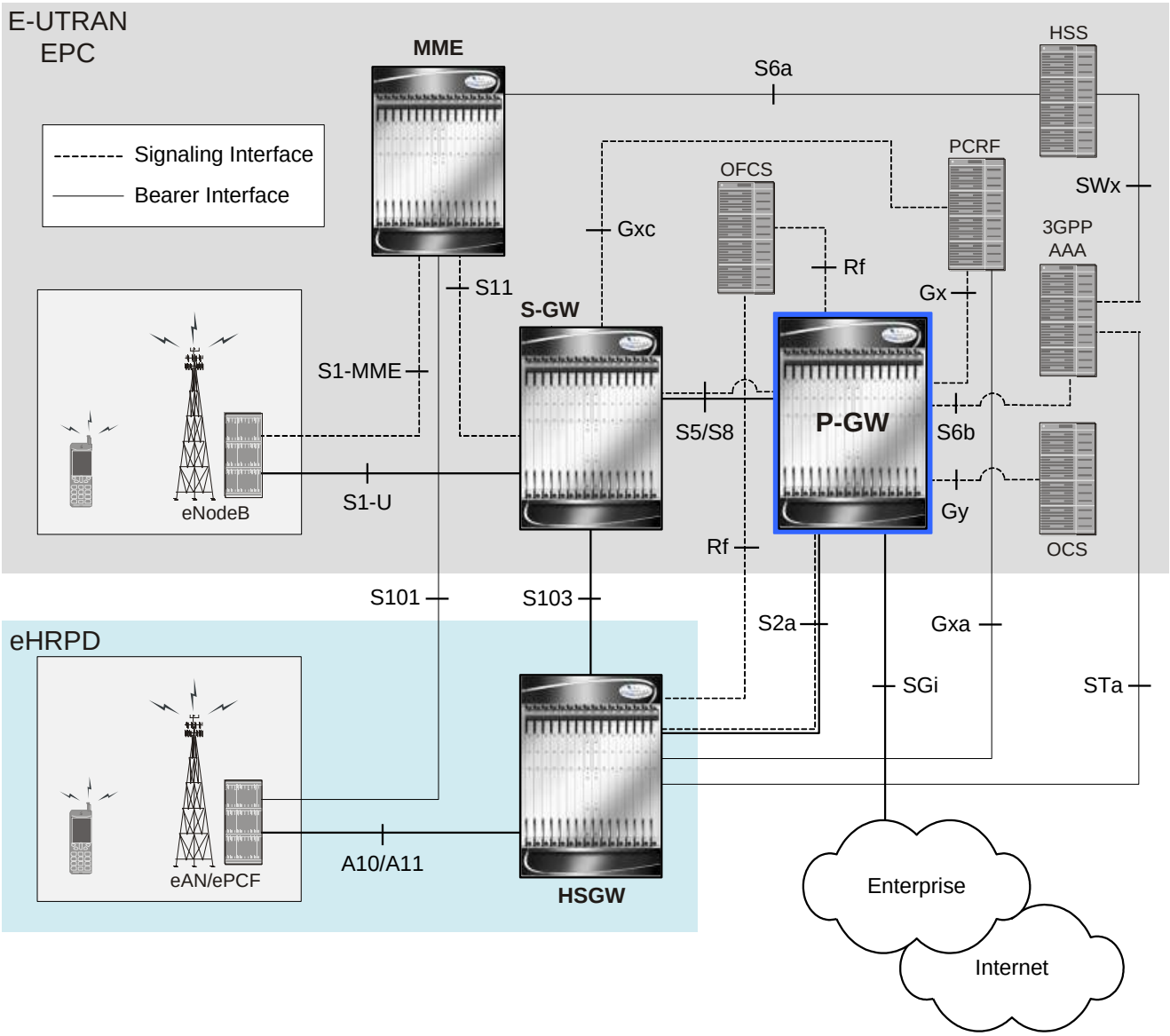
Network Deployment(s)

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

PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity

The following figure displays a simplified network view of the P-GW supporting an eHRPD network and how it interconnects with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

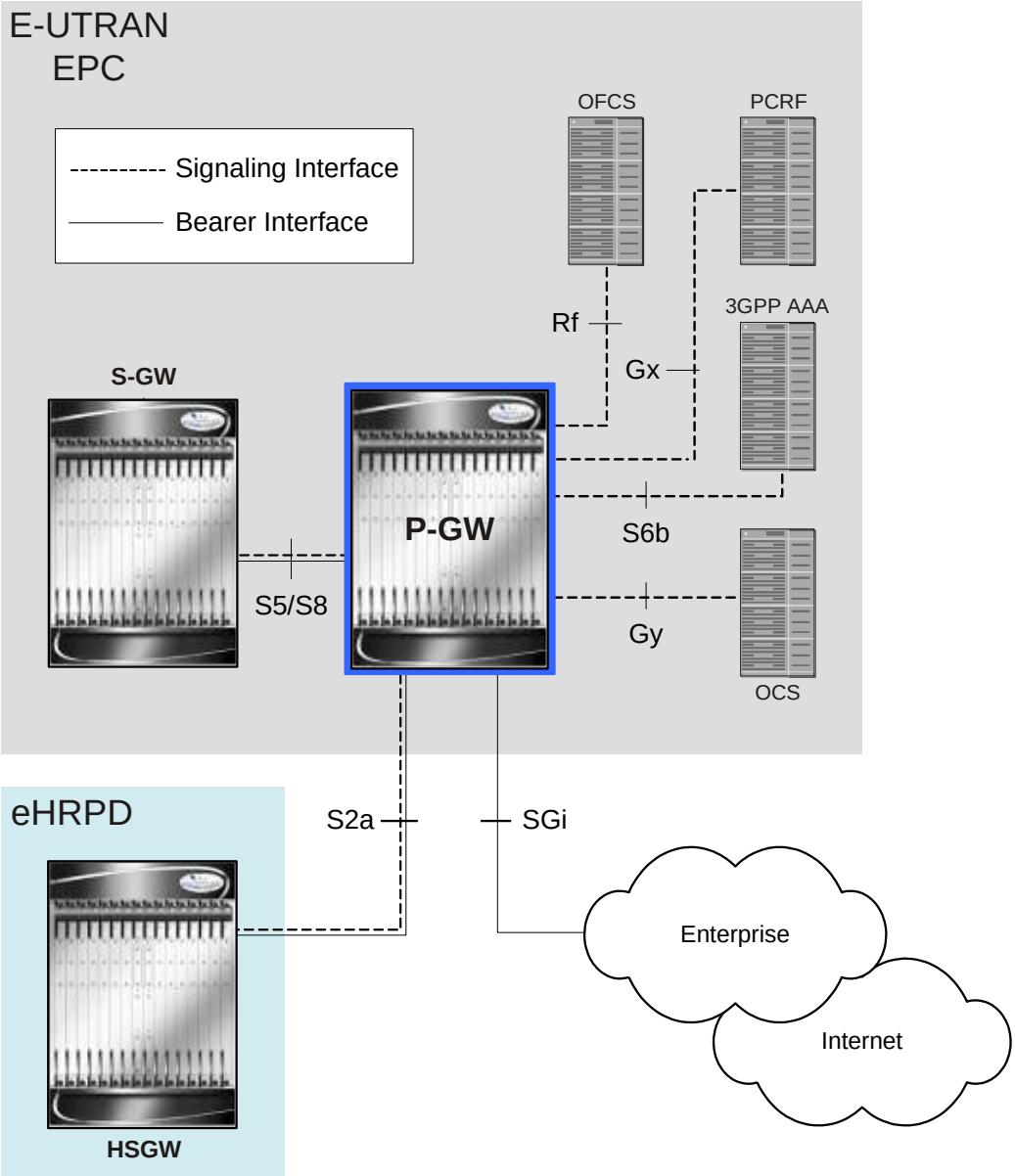
Figure 2. P-GW in the E-UTRAN/EPC Network Supporting the eHRPD Network



Supported Logical Network Interfaces (Reference Points)

The following figure displays the network interfaces between a PDN Gateway, other E-UTRAN network devices, a packet data network, and an HSGW in an eHRPD network.

Figure 3. P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity



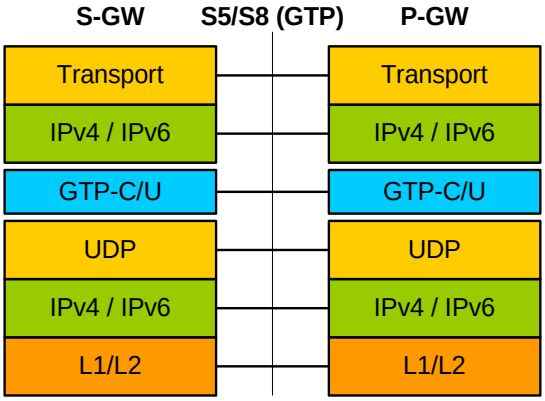
The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW. The S8 interface is used for roaming scenarios. The S5 interface is used for non-roaming.

Supported protocols:

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

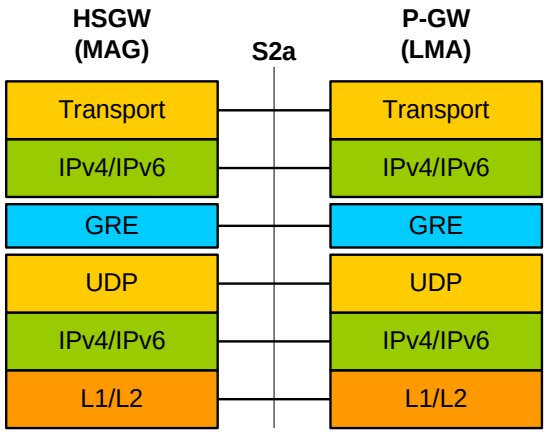


S2a Interface

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

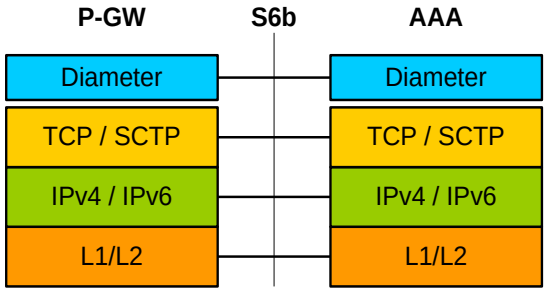


S6b Interface

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.

Supported protocols:

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

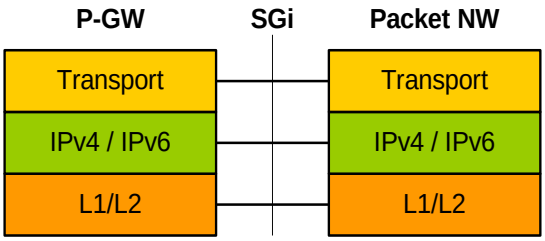


SGi Interface

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

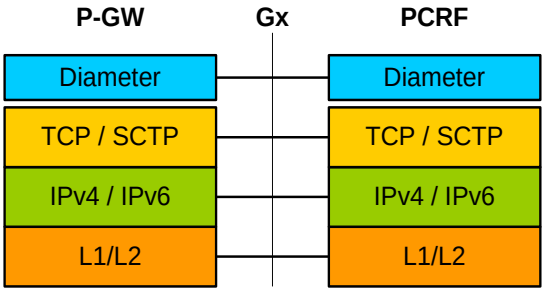


Gx Interface

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.

Supported protocols:

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



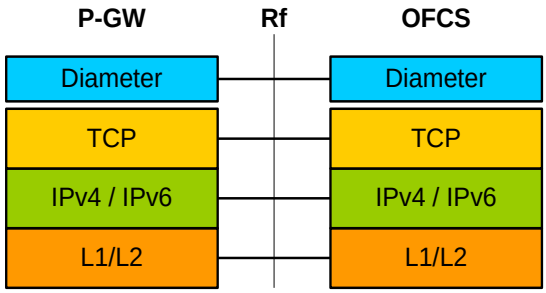
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface) in the Features and Functionality - Base Software section of this guide.

Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 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



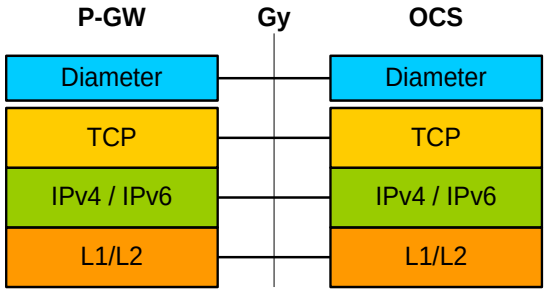
For more information on Rf accounting, refer to the section in the Features and Functionality - Base Software section of this guide.

Gy Interface

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

Supported protocols:

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

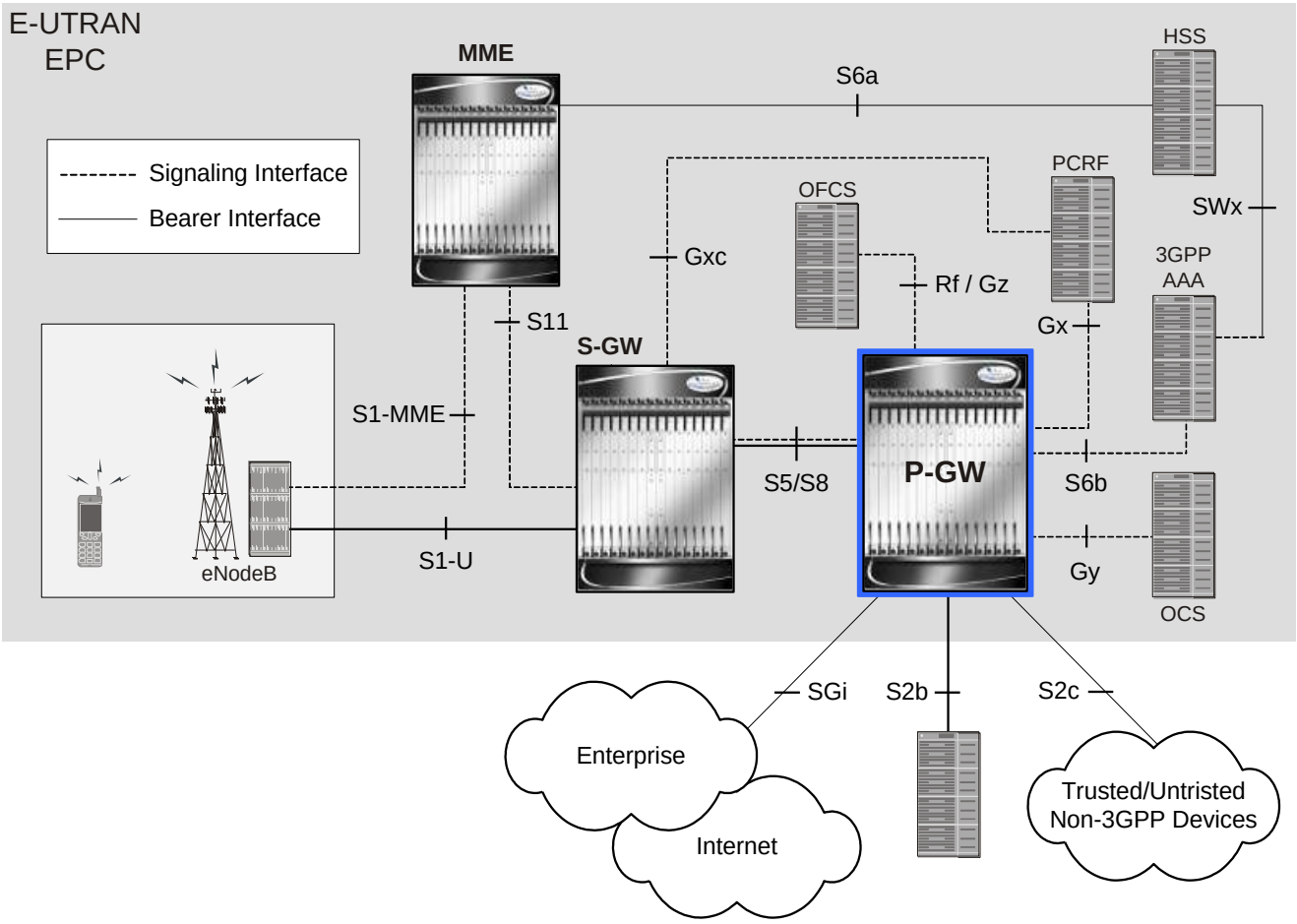


For more information on the Gy interface and online accounting, refer to Gy Interface Support in the Features and Functionality - Base Software section of this guide.

PDN Gateway in the E-UTRAN/EPC Network

The following figure displays a simplified network view of the P-GW and how it interconnects with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

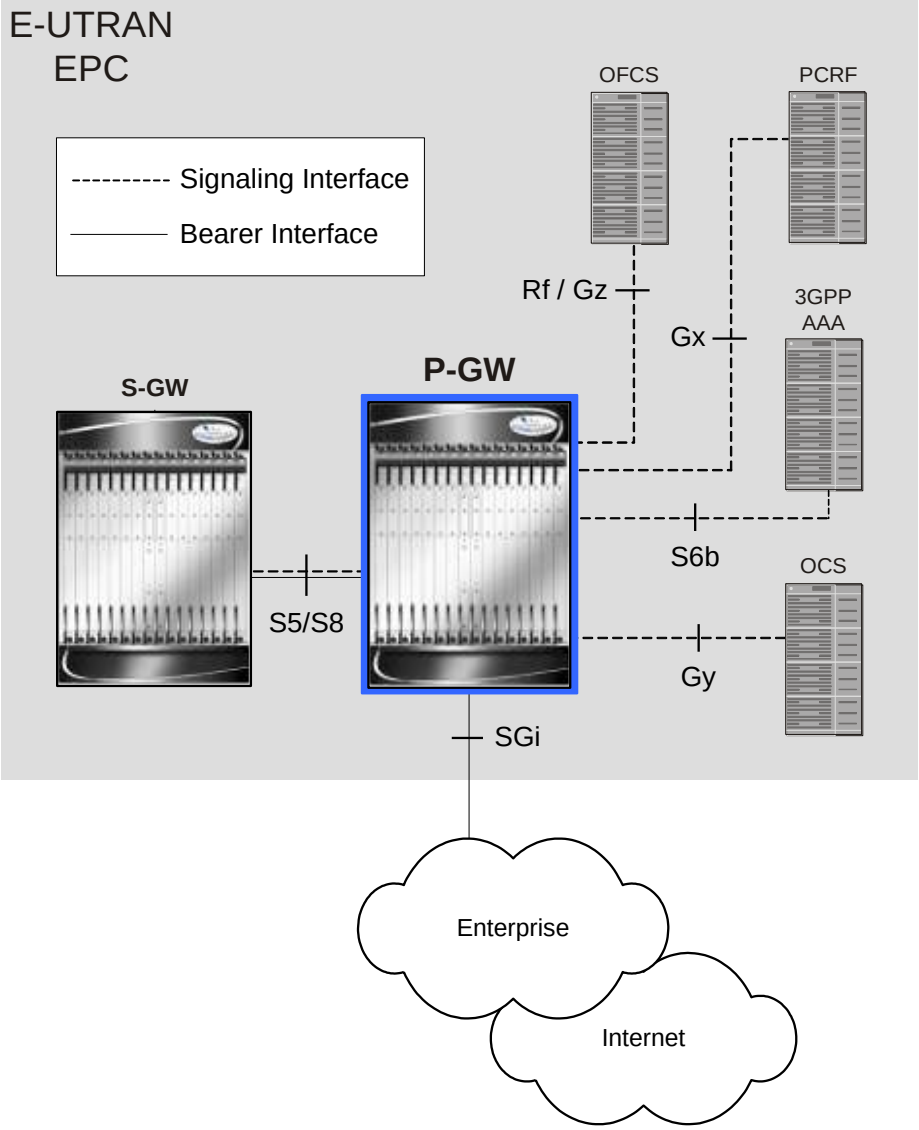
Figure 4. P-GW in the E-UTRAN/EPC Network



Supported Logical Network Interfaces (Reference Points)

The following figure displays the network interfaces between a PDN Gateway, other E-UTRAN network devices, a packet data network, and an HSGW in an eHRPD network.

Figure 5. P-GW Interfaces in the E-UTRAN/EPC Network



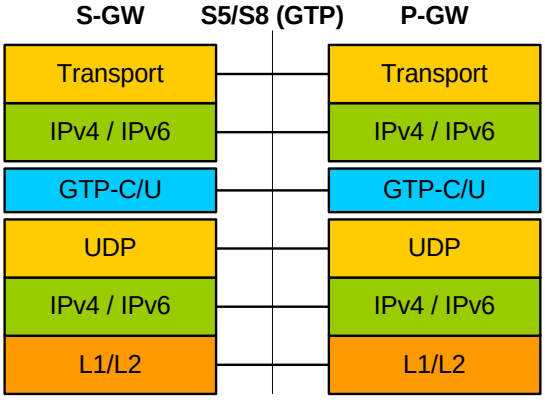
The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW. The S8 interface is used for roaming scenarios. The S5 interface is used for non-roaming.

Supported protocols:

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

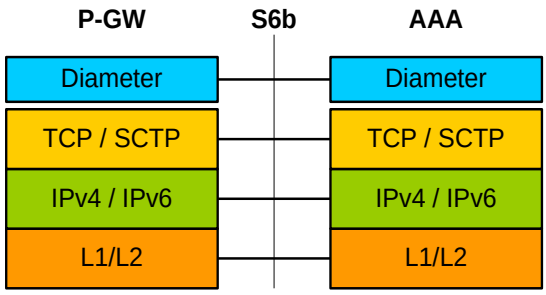


S6b Interface

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.

Supported protocols:

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

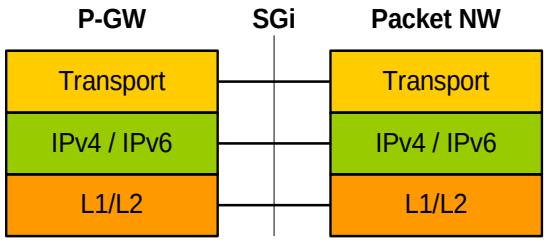


SGi Interface

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

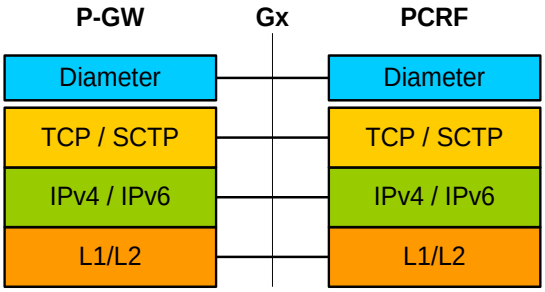


Gx Interface

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.

Supported protocols:

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



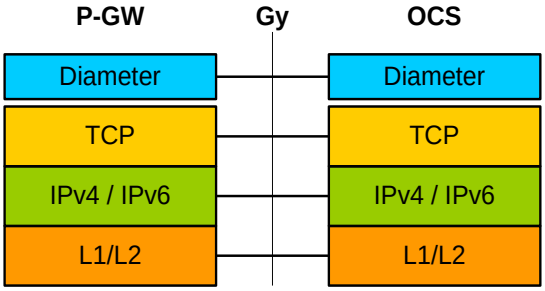
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface) in the Features and Functionality - Base Software section of this guide.

Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 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 in the Features and Functionality - Base Software section of this guide.

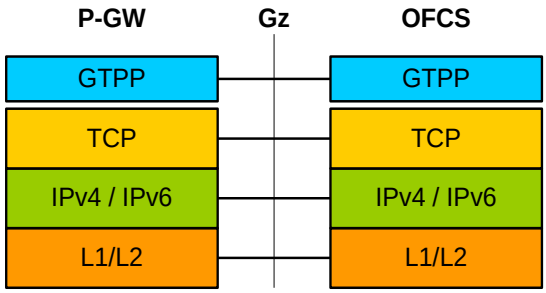
Gz Interface

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

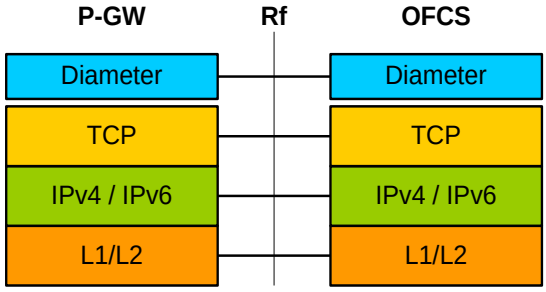


Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 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



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.

The following feature groups are supported and described in this section:

- Subscriber Session Management Features
- Quality of Service Management Features
- Network Access and Charging Management Features
- Network Operation Management Functions
- System Management Features

Subscriber Session Management Features

This section describes the following features:

- IPv6 Capabilities
- Source IP Address Validation
- Default and Dedicated EPC Bearers
- Lawful Intercept
- Local Break-Out
- Subscriber Level Trace
- Proxy Mobile IPv6 (S2a)
- Mobile IP Registration Revocation
- Session Recovery Support

IPv6 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 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 native IPv6 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.

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)

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 UE's 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.

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, 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 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.

Note: This release supports only 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-GW's.

Lawful Intercept

Provides a standardized architecture for lawful monitoring and interception of subscriber call content and control events as mandated by a court ordered warrant from a law enforcement agency.

In accordance with 3GPP TS 33.108 Release 8 requirements the Cisco P-GW supports the Lawful Intercept Access Function for intercepting control and data messages of mobile targets. Law Enforcement Agencies request the network operator to start the interception of a particular mobile user based on court ordered subpoenas.

The Cisco EPC gateways provide access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target and services related to the target on behalf of Law Enforcement Agencies. In this release the P-GW supports the following three interfaces:

- X1 provisioning interface from Administrative Function (ADMF) using CLI over SSH: Intercept targets can be provisioned using subscriber information including MSISDN, IMSI and MEI. Interception of only events (IRI) or events and call content (IRI + CC) can be provisioned.
- X2 event delivery interface for transferring Intercept Related Information (IRI) to a Delivery Function/Mediation server: Intercepted events include QoS information (if available), bearer activation (Default and Dedicated bearer), start of intercept with bearer active, bearer modification, bearer deactivation, and UE requested bearer resource modification.
- X3 content delivery: Includes intercepted call content for all default and dedicated EPS bearers.

The intercepted call control data is encoded in a Cisco proprietary message header format using an optional TLV field to pack the IRI information. The message header also includes other identifying information including sequence numbers, timestamps and session & correlation numbers to correlate session and bearer related information with interception on other EPC elements. If provisioning is activated while the call is active for the target identity then the intercepted information is immediately forwarded to the mediation server. Otherwise camp-on monitoring is used and the system waits for the call to become active (ECM CONNECTED state) and compares the IMSI, MSISDN and MEI against the LI monitoring list as a trigger to begin the intercept.

A total of 20,000 simultaneous LI triggers can be provisioned on the Cisco P-GW. Cisco's LI solution is currently interoperable with leading mediation solutions from a number of partners.

Important: For more information on Lawful Intercept support, refer to the *Lawful Intercept Configuration Guide*.

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 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 and P-GW's in the visited EPC network.

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

Note: Once the trace is provisioned it can be provisioned through the access cloud via various signaling 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 5000 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.

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 (PCO's) it can also be used to transfer P-CSCF or DNS server addresses

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 the *System Enhanced Feature Configuration Guide*.

Session Recovery Support

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 Enhanced Feature Configuration Guide*.

Quality of Service Management Features

This section describes the following features:

- QoS Bearer Management
- DSCP Marking

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 (SDF's) 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 codepoints 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.

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 and Shaping: 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 (SDF's) 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. When traffic shaping is enabled the P-GW enqueues the non-conforming session to the provisioned memory limit for the user session. When the allocated memory is exhausted, the inbound/outbound traffic for the user can be transmitted or policed in accordance with operator provisioned policy.

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

Network Access and Charging Management Features

This section describes the following features:

- Enhanced Charging Service (ECS)
- Online/Offline Charging
- AAA Server Groups
- Dynamic Policy Charging Control (Gx Reference Interface)

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
- Content Service Steering

- Support for Multiple Detail Record Types
- Diameter Credit Control Application
- Accept TCP Connections from DCCA Server
- Gy Interface Support

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 the Support for Multiple Detail Record Types section 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 the Diameter Credit Control Application section 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 licenses. For more information on ECS, refer to the *Enhanced Charging Service 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 *Enhanced Charging Service 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 Enhanced Feature Configuration Guide*.

Important: For more information on ACLs, refer to the IP Access Control Lists chapter of the *System Enhanced Feature Configuration 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 *Enhanced Charging Service 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 *Enhanced Charging Service 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, refer to the AAA Interface Administration and Reference and for ECS configuration, refer to the *Enhanced Charging Service Administration Guide*.

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.

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 Interface:

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 Release 8 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 SGSN's is enabled, the GGSN service on the P-GW records G-CDR's to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW and P-GW's 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 5000 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 CGF's. 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.

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: Due to additional memory requirements, this service can only be used with 8GB Packet Service Cards (PSCs).

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 includes enhancements to conform with 3GPP TS 29.212 and 29.230 Release 8 functions. The Gx reference interface uses Diameter transport and IPv6 addressing. The subscriber is identified to the PCRF at session establishment using IMSI based NAI's 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

Network Operation Management Functions

This section describes the following features:

- Support Interfaces (Reference Points)
- Multiple PDN Support
- Congestion Control
- IP Access Control Lists

Support Interfaces (Reference Points)

S5/S8 GTP (E-UTRAN EPC)

In accordance with 3GPP TS 23.401 the Cisco P-GW platform supports GTPv2-C and GTPv1-U call control and user plane tunnelling. A GTP tunnel is identified in each node with a Tunnel Endpoint ID (TEID), an IP address and a UDP port number. The S-GW and P-GW nodes provision separate GTP tunnels for each attached subscriber and for the individual PDN connections initiated by the UE. The StarOS distributed software architecture enables each function to run as independent stand-alone services on separate chassis or as simultaneous combination services running on the same platform.

The S5 reference interface provides user plane tunnelling and tunnel management between an S-GW and P-GW located within the same administrative domain. 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.

The S8 reference interface is an inter-PLMN reference point providing user and control plane between the S-GW in the V-PLMN and the P-GW in the H-PLMN. It is based on the Gp reference point as defined between SGSN and GGSN. S8a is the inter PLMN variant of S5.

S6b (E-UTRAN EPC)

The S6b reference interface is run between the P-GW and 3GPP AAA server using Diameter transport and IPv6 addressing. The EPC core network uses the S6b interface to authenticate non-3GPP traffic from e-HRPD access networks. When the P-GW receives PMIP binding update messages from adjacent HSGW's it initiates an authorization request to the 3GPP AAA server. It is also possible for the AAA server to initiate reauthorization in cases where the subscriber profile is modified at the HSS. S2a (PMIPv6) sessions can be terminated based on requests from the HSS server or HSGW.

SGi

SGi is the reference point between the P-GW and one or more external Packet Data Networks (PDN's). Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provisioning of IMS services. From the external IP network's point of view, the P-GW is seen as a normal IP router. The L2 and L1 layers are operator specific.

The access to the external PDN may involve specific functions that include user authentication/authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, IPv6 address auto-configuration, accounting of user traffic, or connectivity to an external application server.

The SGi interface is used to support the following functions. The P-GW deduces from the APN the servers to be used for different functions:

- For external IP address allocation if needed (DHCP)
- For authentication if required by Protocol Configuration Option (PCO)
- For auto-configuration using DHCP
- For DNS service
- For application functions (E.g. CSCF FQDN, etc)
- For IP address auto configuration (IPv6)

S2a (eHRPD)

The Cisco P-GW can anchor non 3GPP calls from a trusted e-HRPD access network using the Proxy Mobile IPv6 protocol. In a PMIPv6 implementation, the P-GW includes the function of a Local Mobility Anchor Point (LMA) according to draft-ietf-netlmm-proxymip6. Network-based mobility provides mobility for Simple IPv6 capable access devices without host involvement. This approach to supporting mobility does not require the mobile node to be involved in the exchange of signalling messages between itself and the LMA. A Mobility Access Gateway (MAG) function on the HSGW provides the proxy mobility agent and performs the signalling and mobility management with the LMA on behalf of the attached subscriber device.

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 offdeck 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 LMA's. 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, APN's and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.

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 Enhanced Feature Configuration Guide*.

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 Enhanced Feature Configuration Guide*.

System Management Features

This section describes following features:

- Management System Overview
- Bulk Statistics Support
- Threshold Crossing Alerts (TCA) Support
- ANSI T1.276 Compliance

Management System Overview

The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (Cisco Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems - giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

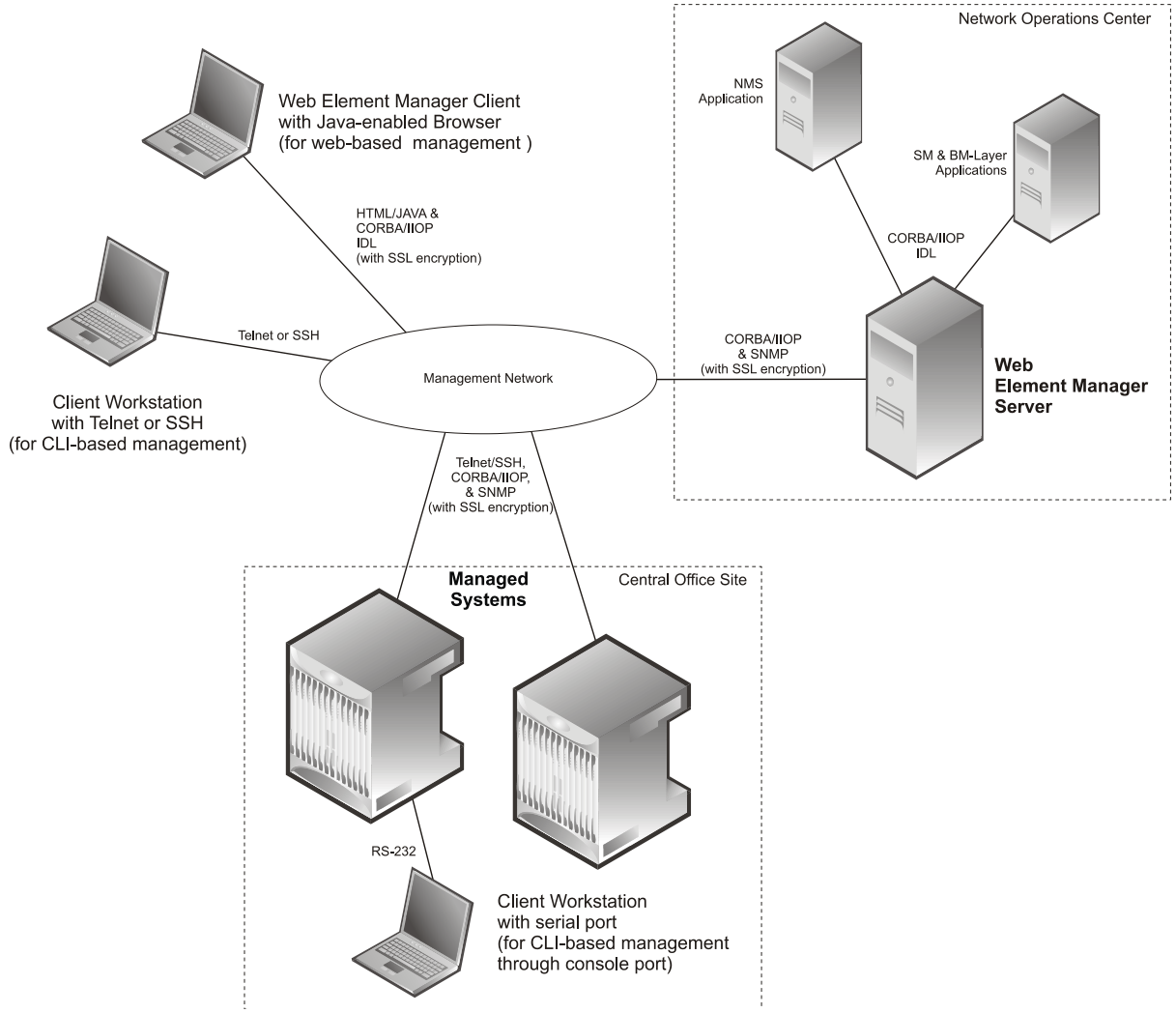
Cisco's O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

- Using the command line interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the Console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG’s) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 6. Element Management Methods



Important: P-GW management functionality is enabled by default for console-based access. For GUI-based management support, refer to the Web Element Management System section in this chapter.

Important: For more information on command line interface based management, refer to the *Command Line Interface Reference*.

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 the Web Element Manager, 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 partial list of supported schemas:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **LMA**: Provides LMA service statistics
- **P-GW**: Provides P-GW node-level service statistics
- **IP Pool**: Provides IP pool statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **APN**: Provides Access Point Name 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 the Web Element Manager 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 the Web Element Manager 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 the Web Element Manager server.

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

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 the Alarm Management menu in the Web Element Manager.

  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*.

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 5000 and the Web Element Manager 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.

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 URL's or URI's in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.
- Content Filtering ICAP Interface: This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5000 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 5000 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 5000 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.

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 *Peer to Peer Detection Administration Guide*.

Features and Functionality - External Application Support

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

- Web Element Management System

Web Element Management System

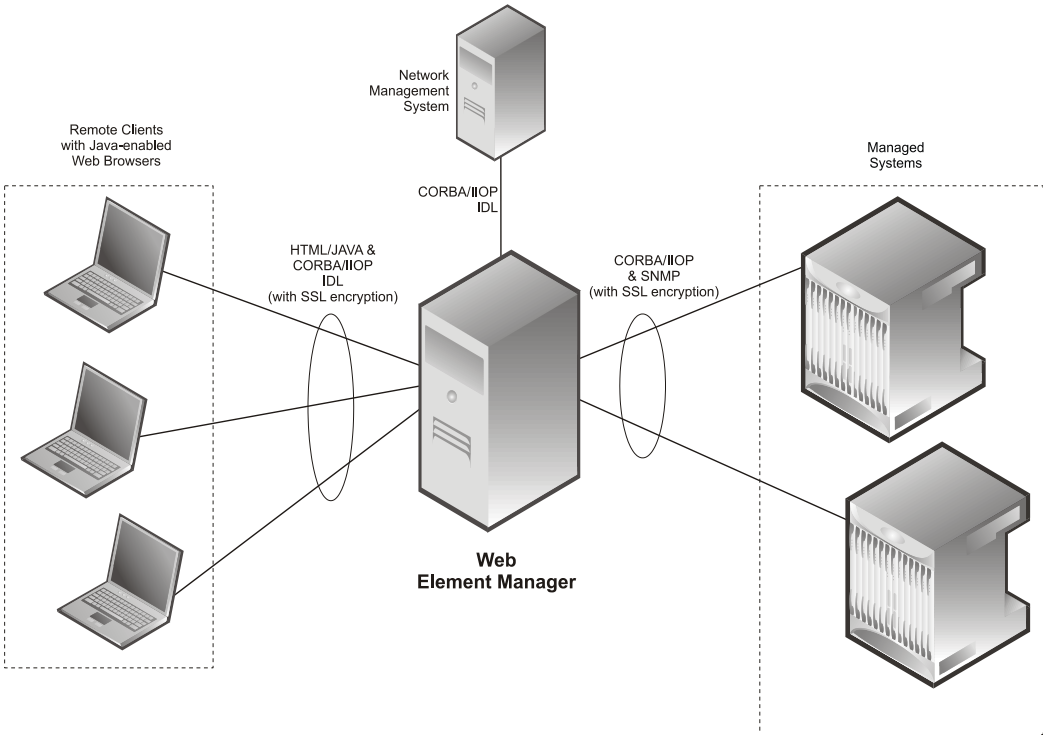
Provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management of the ASR 5000.

The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete fault, configuration, accounting, performance, and security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates various interfaces between the Cisco Web Element Manager and other network components.

Figure 7. Web Element Manager Network Interfaces



Important: For more information on WEM support, refer to the WEM Installation and 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 require the purchase of an additional license to implement the functionality with the P-GW service.

This section describes following features:

- Inter-Chassis Session Recovery
- IP Security (IPSec) Encryption
- Traffic Policing and Shaping
- Layer 2 Traffic Management (VLANs)

Inter-Chassis Session Recovery

The ASR 5000 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.

License Keys: The part number and cost will be determined two months before First Customer Shipment.

Important: For more information on inter-chassis session recovery support, refer to the Interchassis Session Recovery chapter in the *System Enhanced Feature Configuration Guide*.

IP Security (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 IP Security chapter in the *System Enhanced Feature Configuration Guide*.

Traffic Policing and Shaping

Traffic policing and shaping allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers. Shaping allows you to buffer excesses to be delivered at a later time.

Traffic Policing

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".

Traffic Shaping

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

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

Important: For more information on traffic policing and shaping, refer to the Traffic Policing and Shaping chapter in the *System Enhanced Feature Configuration Guide*.

Layer 2 Traffic Management (VLANs)

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 Enhanced Feature Configuration Guide*.

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 IPv6IPv4 Access
- PMIPv6 Lifetime Extension without Handover
- PDN Connection Release Initiated by UE
- PDN Connection Release Initiated by HSGW
- PDN Connection Release Initiated by P-GW

Initial Attach with IPv6/IPv4 Access

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

Figure 8. Initial Attach with IPv6/IPv4 Access Call Flow

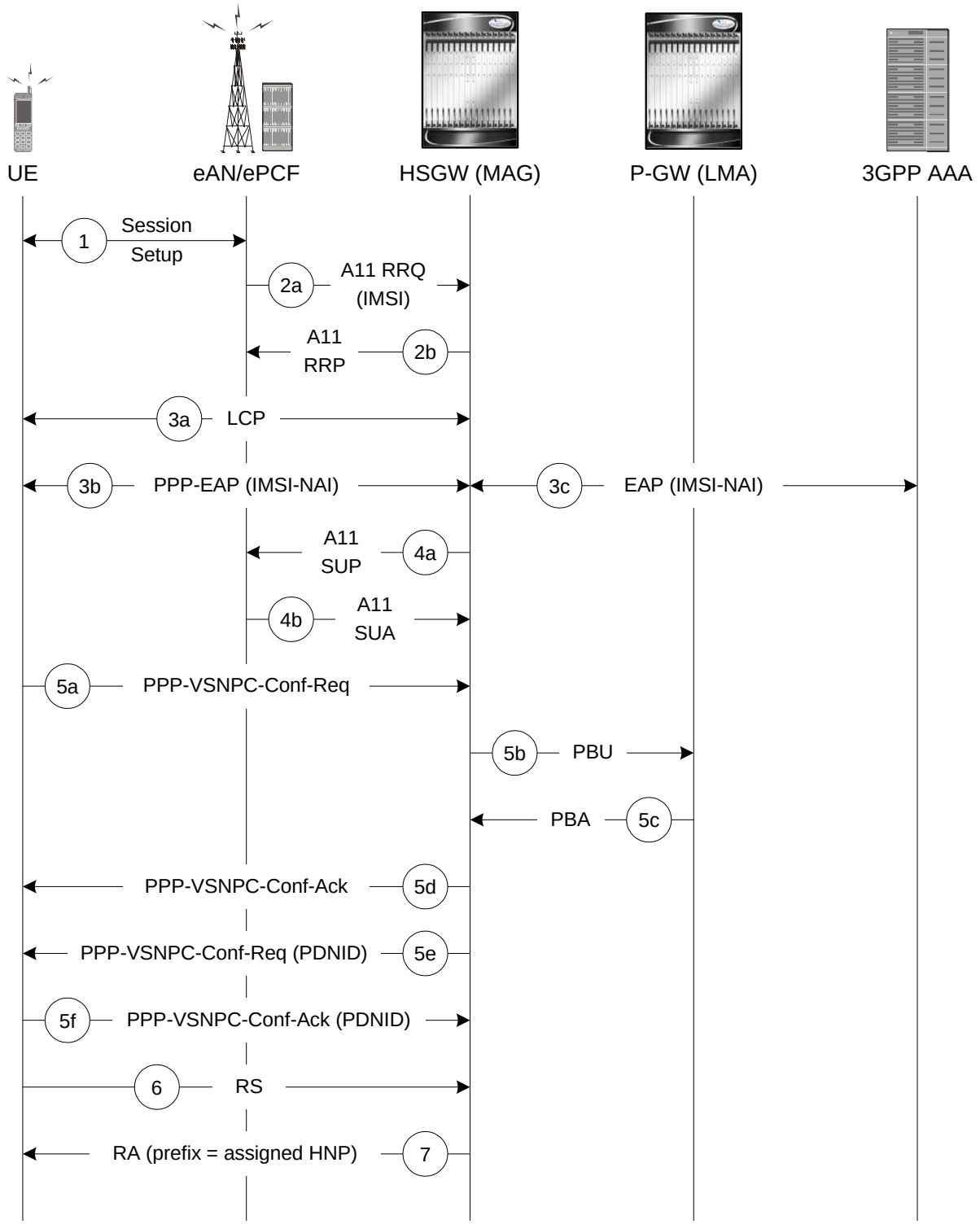


Table 2. Initial Attach with IPv6/IPv4 Access Call Flow Description

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.
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.

Figure 9. PMIPv6 Lifetime Extension (without handover) Call Flow

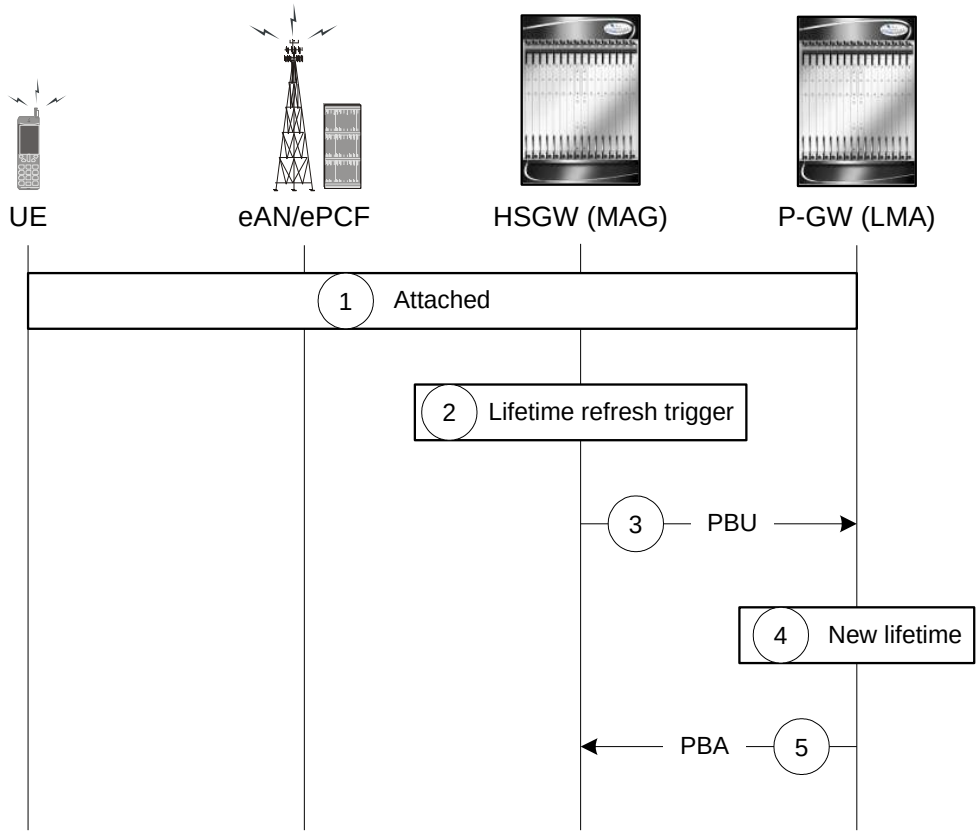


Table 3. PMIPv6 Lifetime Extension (without handover) Call Flow Description

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 Acknowledgement (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.

Figure 10. PDN Connection Release by the UE Call Flow

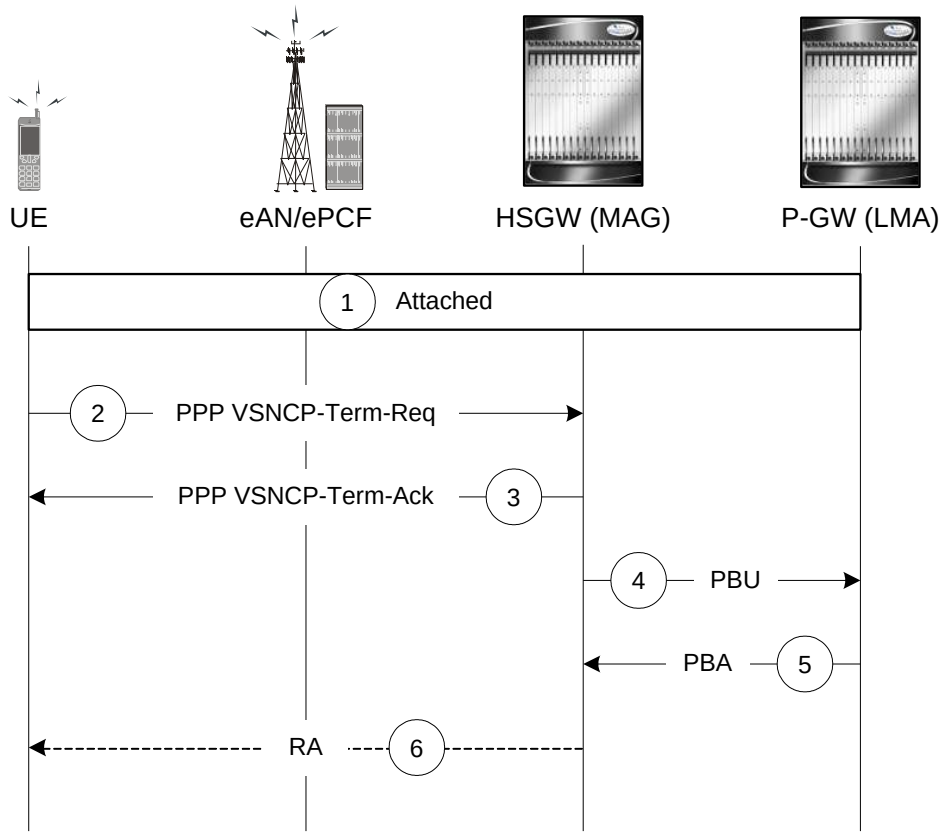


Table 4. PDN Connection Release by the UE Call Flow Description

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.
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.

Figure 11. PDN Connection Release by the HSGW Call Flow

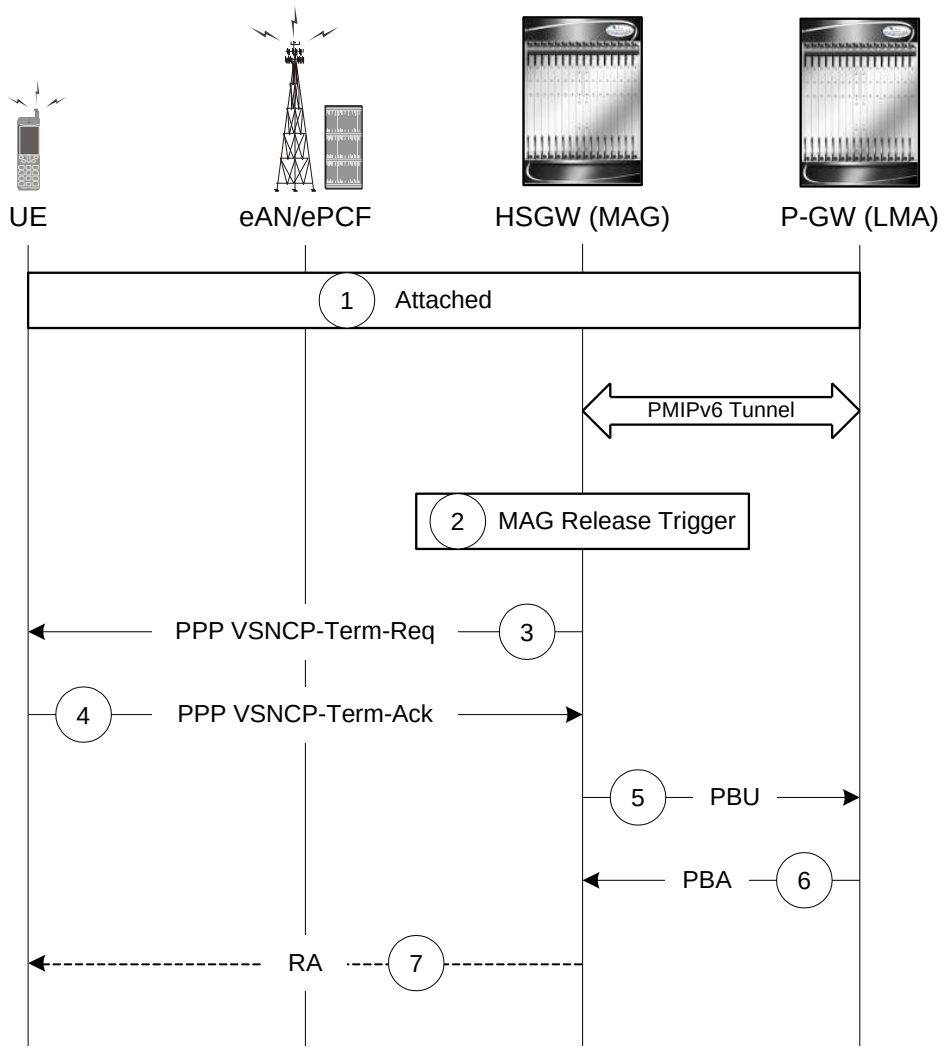


Table 5. PDN Connection Release by the HSGW Call Flow Description

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.

Step	Description
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.
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.

Figure 12. PDN Connection Release by the HSGW Call Flow

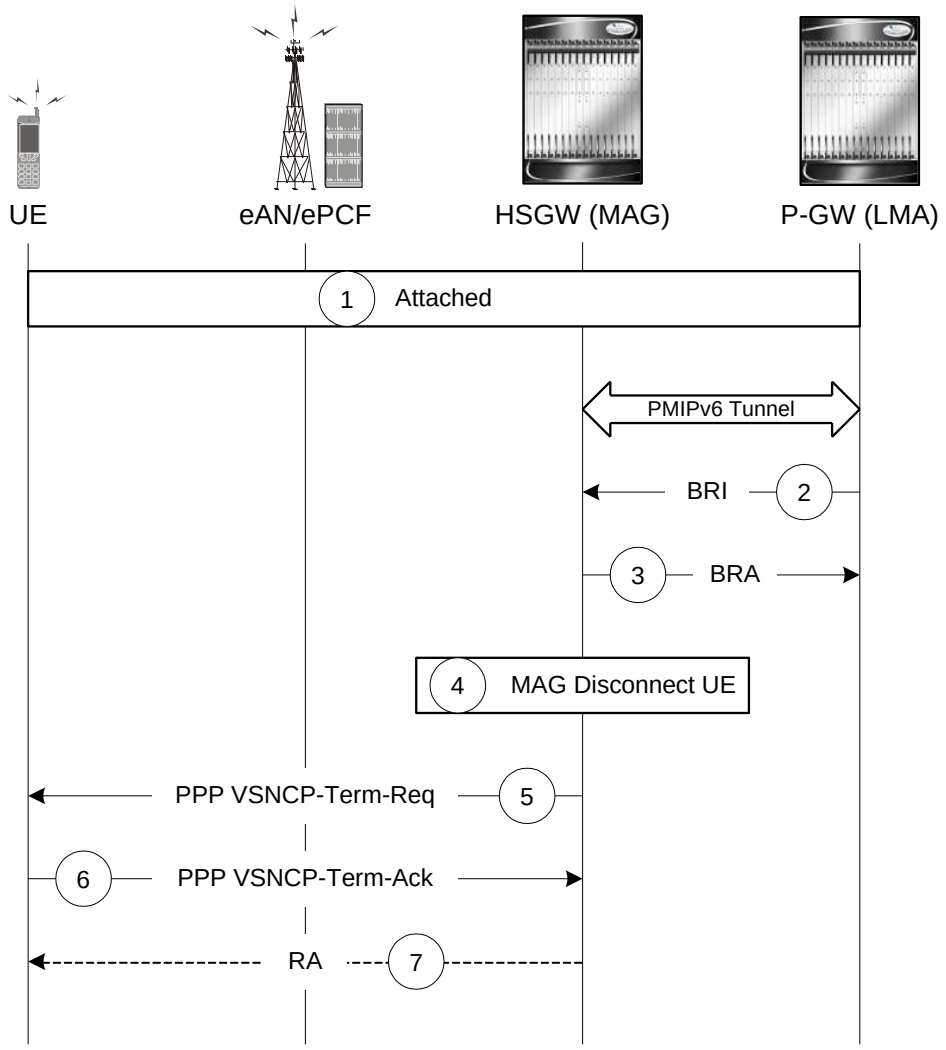


Table 6. PDN Connection Release by the HSGW Call Flow Description

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	A PGW 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 Acknowledgement (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.

Step	Description
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)
- Subscriber-initiated Detach

Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

Figure 13. Subscriber-initiated Attach (initial) Call Flow

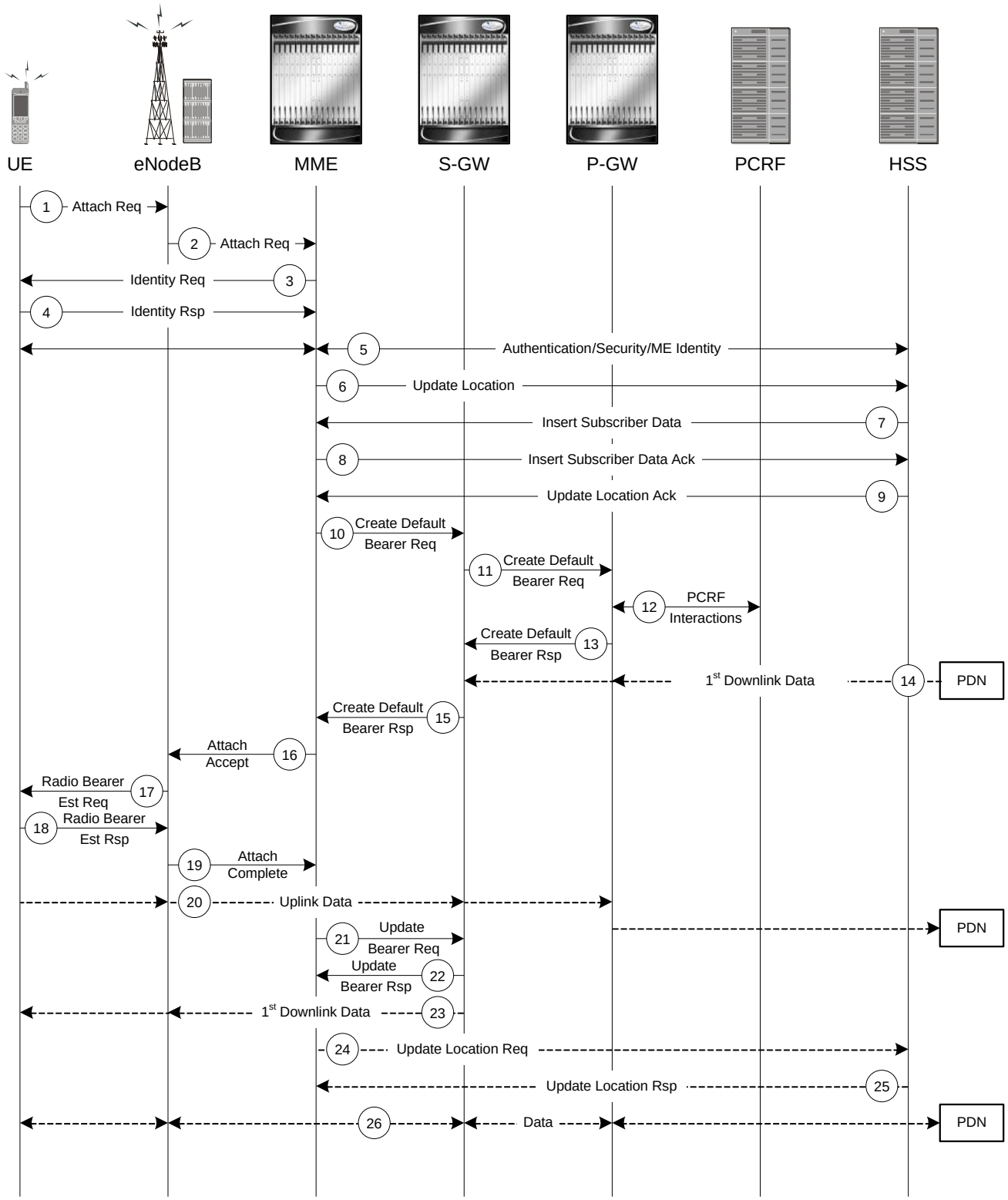


Table 7. Subscriber-initiated Attach (initial) Call Flow Description

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 sends Insert Subscriber Data (IMSI, Subscription Data) message to the MME. 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.
8	The MME validates the UE's presence in the (new) TA. If due to regional subscription restrictions or access restrictions the UE is not allowed to attach in the TA, the MME rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack message to the HSS. If subscription checking fails for other reasons, the MME rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack message to the HSS including an error cause. If all checks are successful then the MME constructs a context for the UE and returns an Insert Subscriber Data Ack message to the HSS. The Default APN shall be used for the remainder of this procedure.
9	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. If the Update Location is rejected by the HSS; the MME rejects the Attach Request from the UE with an appropriate cause.
10	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.
11	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.
12	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
13	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.
14	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
15	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.
16	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.
17	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.
18	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
19	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
20	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 tunnelled to the S-GW and P-GW.
21	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
22	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
23	The S-GW sends its buffered downlink packets.
24	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.
25	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
26	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.

Figure 14. Subscriber-initiated Detach Call Flow

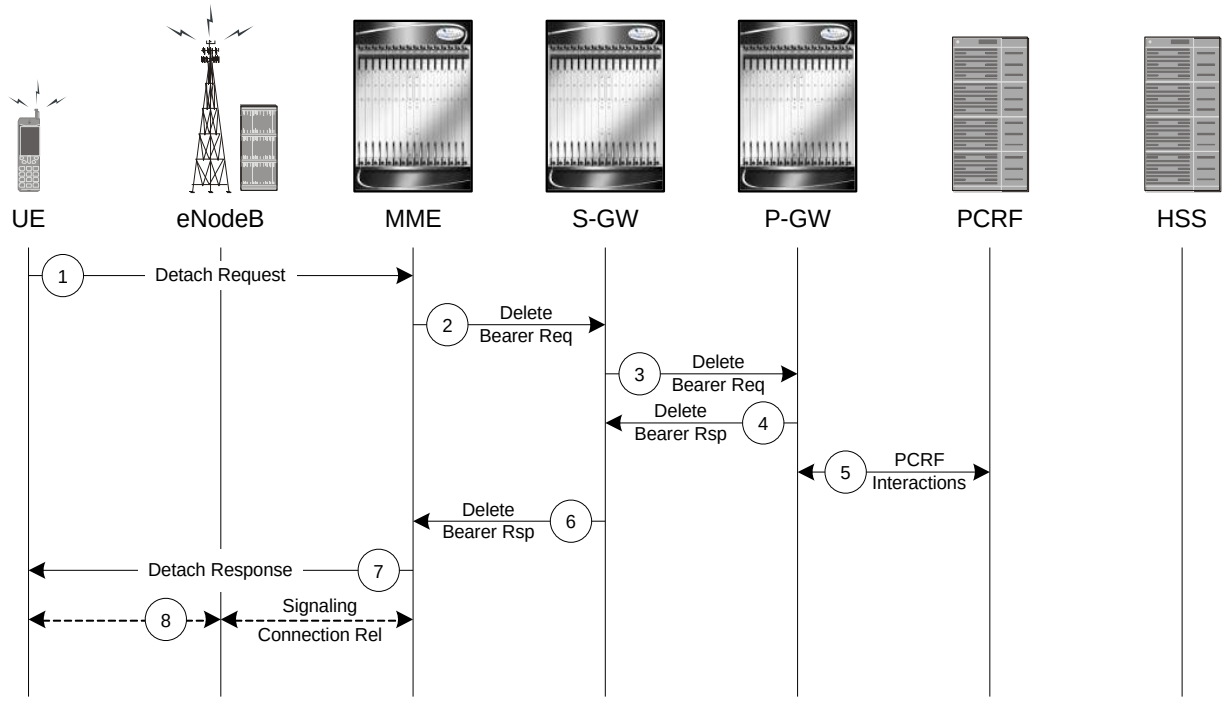


Table 8. Subscriber-initiated Detach Call Flow Description

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.

- 3GPP References
- 3GPP2 References
- IETF References
- Object Management Group (OMG) Standards

3GPP 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 23.107: 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 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 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. Gx application
- 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 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.1.1
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.2.0 (both versions are intentional)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols, version 8.1.0
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 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.P0057-0 v0.11.0 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 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (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 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3775: Mobility Support in IPv6
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5149: Mobile IPv6 Vendor Specific Option
- RFC 5213: Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6

- Internet-Draft (draft-meghana-netlmm-pmipv6-mipv4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-02.txt) IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress

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 *ASR 5000 Series 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 *ASR 5000 Series Command Line Interface Reference*.

The following procedures are located in this chapter:

- Configuring the System as a Standalone eGTP P-GW
- Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network

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 a 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
- How This Configuration Works
- eGTP P-GW Configuration

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 9. 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.

Required Information	Description
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 that will be used to access the system such as telnetd, sshd, and/or ftpd.

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 10. 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 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.

Required Information	Description
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 11. 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.
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.

Required Information	Description
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.
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 12. Required Information for AAA Context Configuration

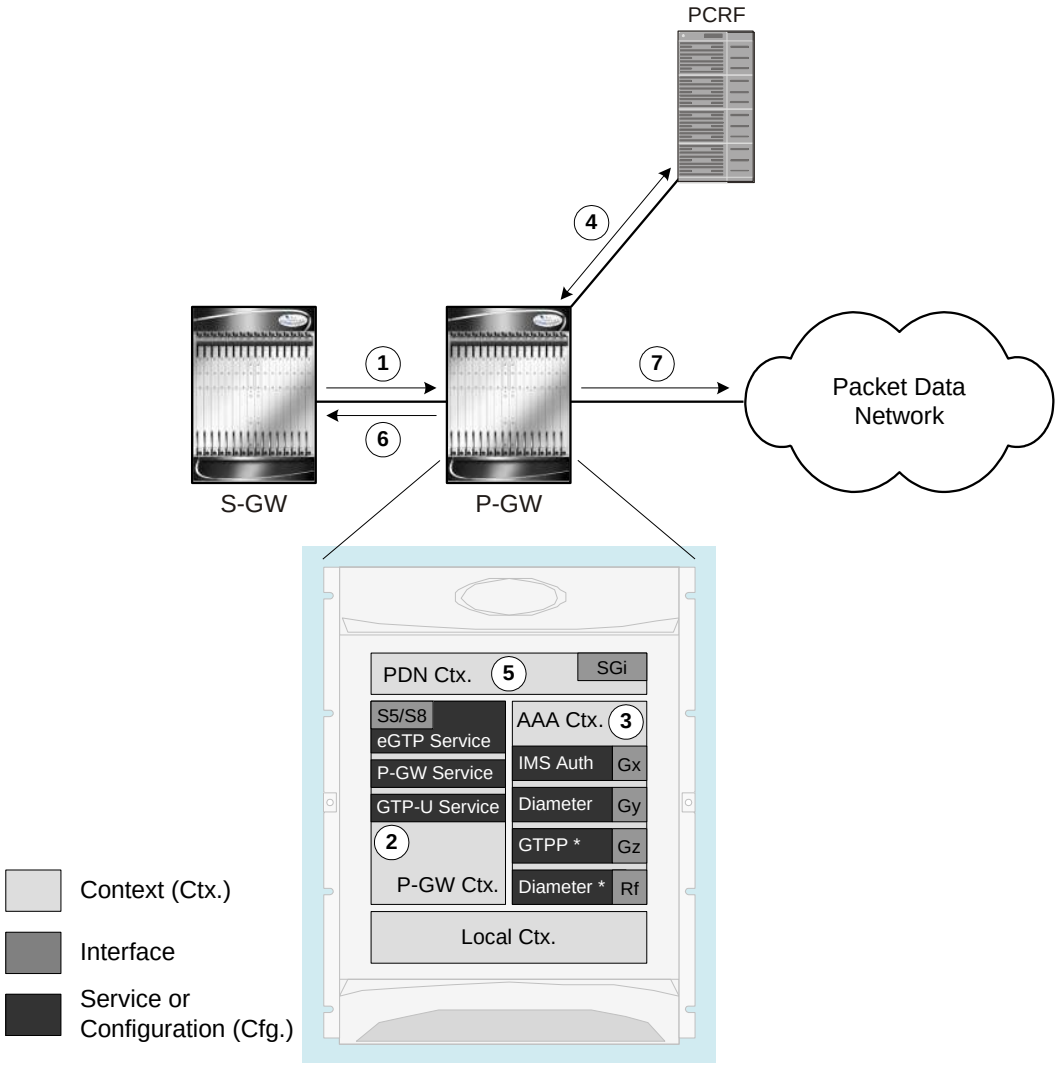
Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	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.
Gy Interface Configuration (to on-line charging server)	

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 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.
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)	

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 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

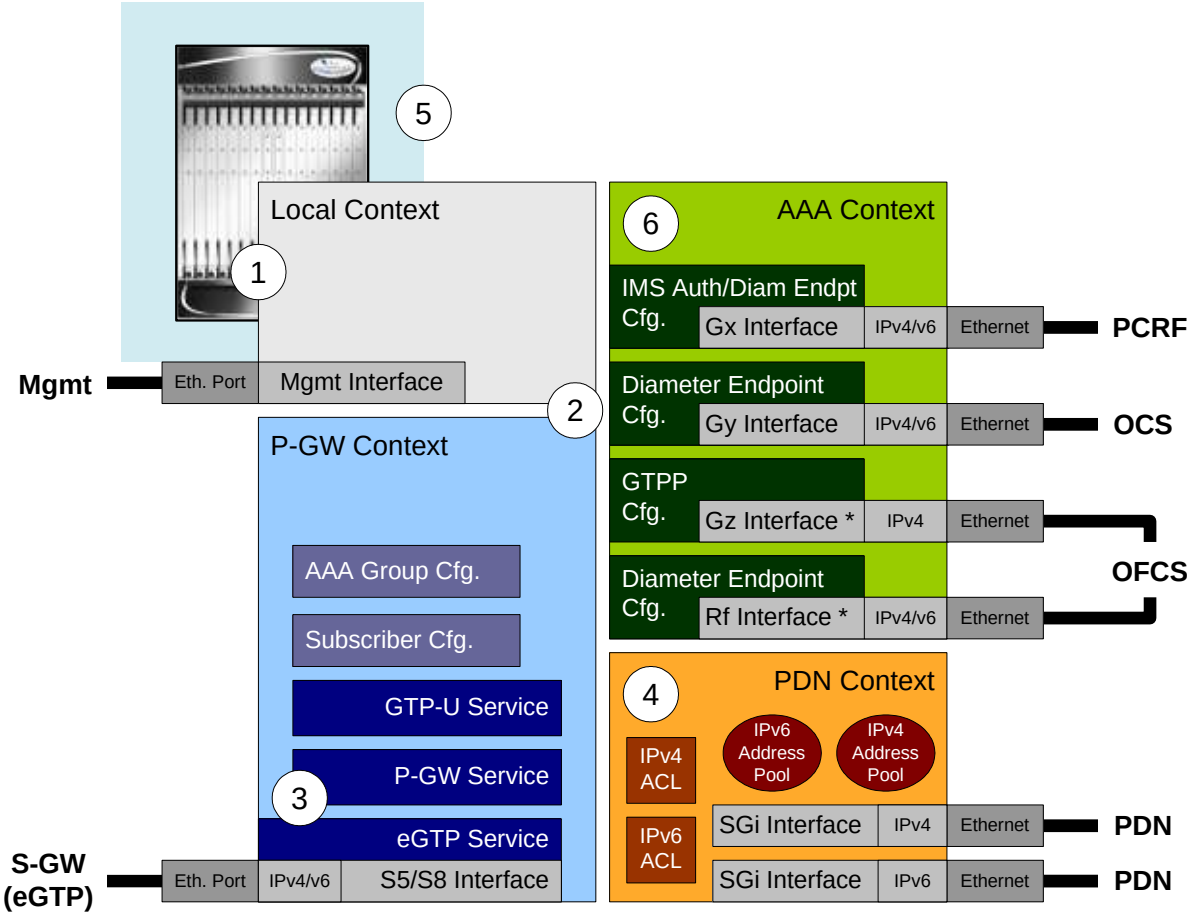
The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.



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:



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 section of this chapter.

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 section.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration section.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration section.

Step 6 Create a AAA context and configure parameters for policy by applying the example configuration in the Policy Configuration section.

Step 7 Verify and save the configuration by following the steps found in the Verifying and Saving the Configuration section.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in the Modifying the Local Context section.

Step 2 Create the context where the eGTP service will reside by applying the example configuration in the Creating and Configuring a P-MIP P-GW Context section.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in the Creating and Configuring APNs in the P-GW Context section.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in the Creating and Configuring AAA Groups in the P-GW Context section.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in the Creating and Configuring an eGTP Service section.

Step 6 Create and configure a GTP-U service within the P-GW context by applying the example configuration in the Creating and Configuring a GTP-U Service section.

Step 7 Create a context through which the interface to the PDN will reside by applying the example configuration in the Creating a P-GW PDN Context section.

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 section above.

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>
```

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
```

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

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service section.

Step 2 Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring a Static IP Route section.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-servers <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 section for more information.

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_definition>
               .
               .
         <rule_definition>
         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 egcdr
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft-packet-filter qci3
      exit
   charging-action static
      service-identifier <id>
      billing-action egcdr
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft-packet-filter qci3
      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 rule base 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 off-line charging. The **billing-records egcdr** command is required for Gz accounting. All other commands are optional.

Policy Configuration

Step 1 Configure the policy and accounting interfaces by applying the example configuration in the Creating and Configuring the AAA Context section.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping 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 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>
      exit
```

Notes:

- QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203. Values 10 through 32 can be configured for non-standard use.
- 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

Refer to the Verifying and Saving Your Configuration chapter to verify and save your P-GW configuration.

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
- How This Configuration Works
- P-MIP P-GW (eHRPD) Configuration

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.

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 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 that will be used to access the system such as telnetd, sshd, and/or ftpd.

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.
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.

Required Information	Description
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).
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 15. 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.

Required Information	Description
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.
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

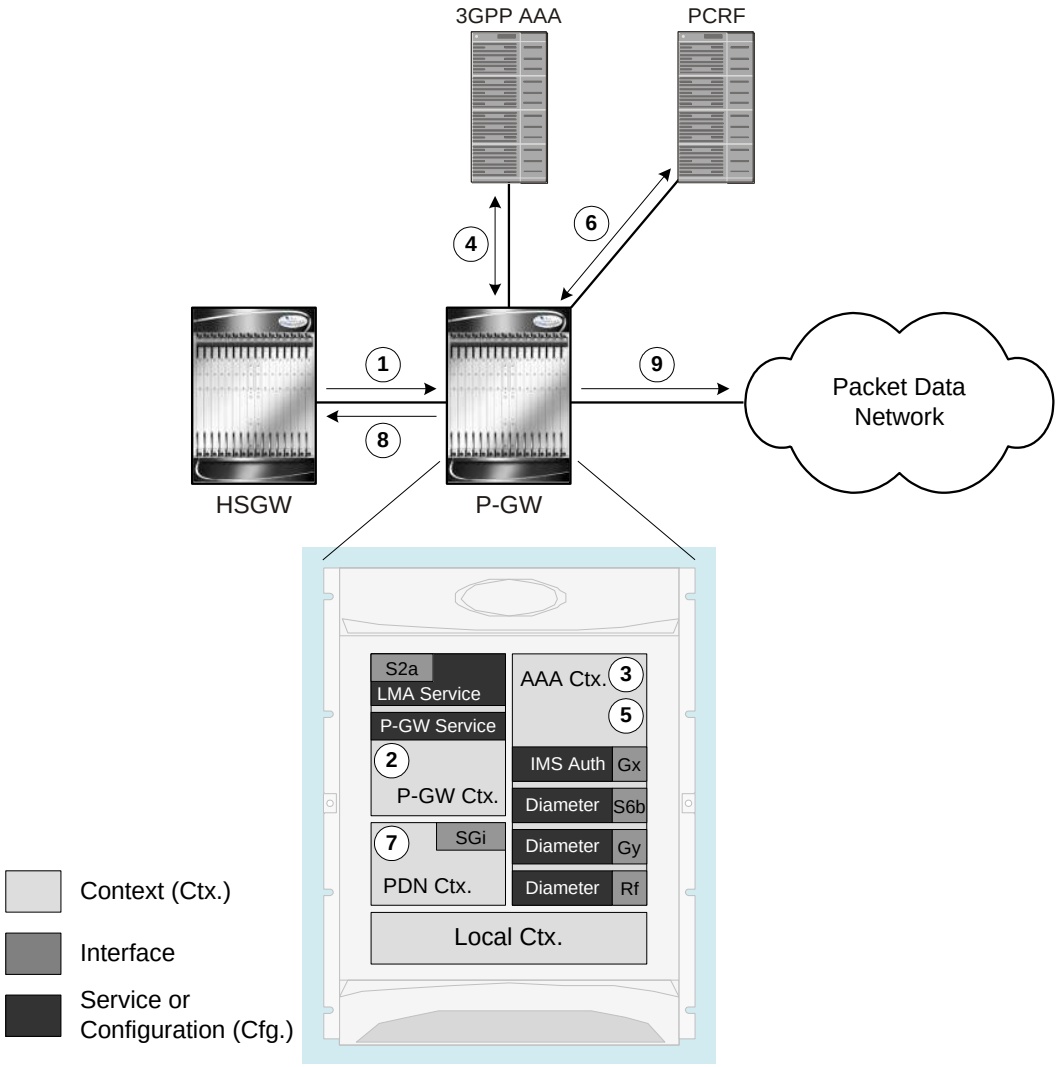
Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	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.
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.
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.
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.

Required Information	Description
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.
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.

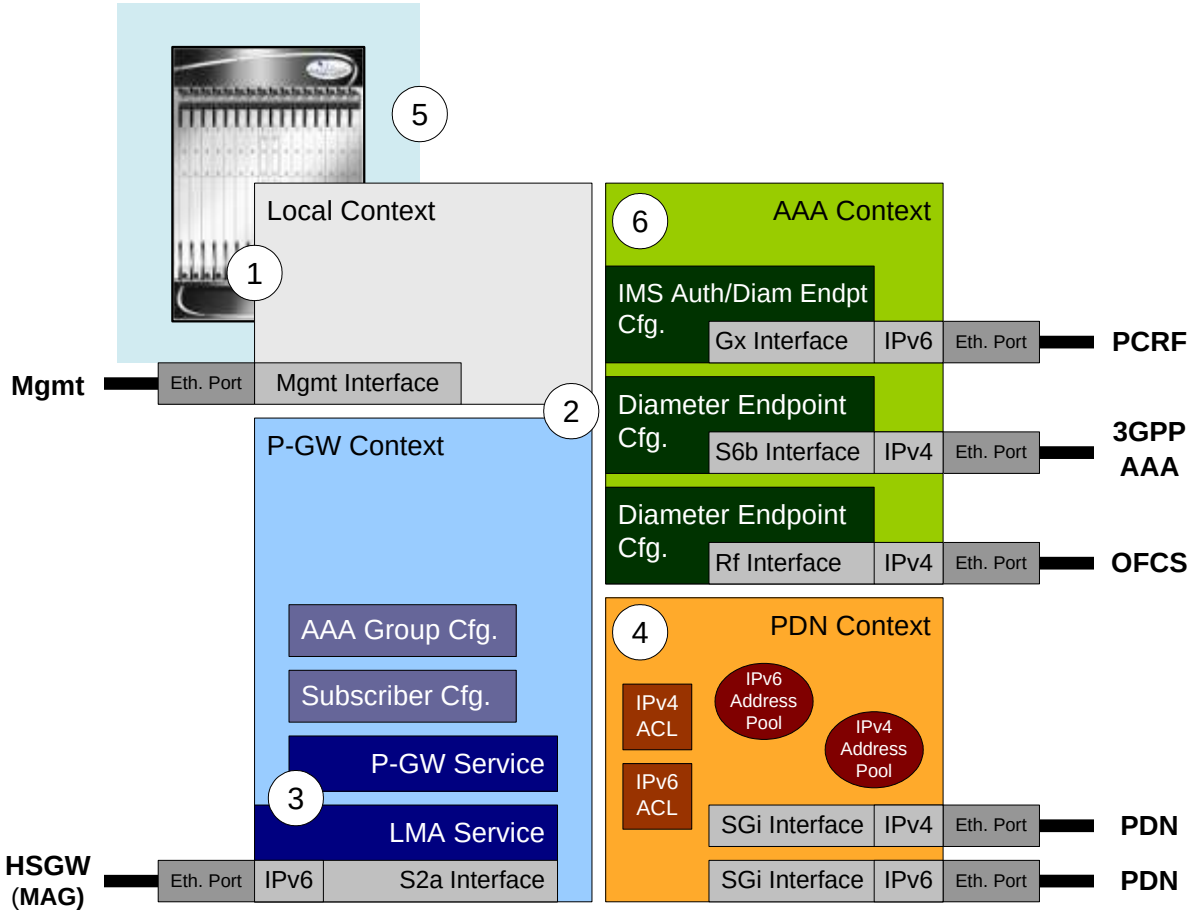


1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts 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.



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 section of this chapter.

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 the P-GW Service Configuration section.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration section.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration section.

Step 6 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in the AAA and Policy Configuration section.

Step 7 Verify and save the configuration by following the instruction in the Verifying and Saving the Configuration section.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in the Modifying the Local Context section.

Step 2 Create the context where the P-GW service will reside by applying the example configuration in the Creating and Configuring a P-MIP P-GW Context section.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in the Creating and Configuring APNs in the P-GW Context section.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in the Creating and Configuring AAA Groups in the P-GW Context section.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in the Creating and Configuring an LMA Service section.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in the Creating a P-GW PDN Context section.

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>
```

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 a P-MIP P-GW Context section above.

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

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service section.

Step 2 Specify an IP route to the HRPD Serving Gateway by applying the example configuration in the Configuring a Static IP Route section.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-servers <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 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 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
    rulebase default
        exit
    rulebase <name>
        <rule_base>
            .
            .
        <rule_base>
        end
```

Notes:

- 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.
- A rule base is a collection of rule definitions and associated charging actions.

AAA and Policy Configuration

Step 1 Configure AAA and policy interfaces by applying the example configuration in the Creating and Configuring the AAA Context section.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping 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>
      exit
```

Notes:

- QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203. Values 10 through 32 can be configured for non-standard use.
- 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

Refer to the Verifying and Saving Your Configuration chapter to verify and save your P-GW configuration.

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

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

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

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

show ip pool

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

```
context : isp1:

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

 | (S) - Static (E) - Resource

 |

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

 ||

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

 ||||

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

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

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

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

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

Important: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

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

show *<service_type> <service_name>*

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

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

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

show context name *<name>*

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

```
Context Name     ContextID     State

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

test1            2          Active
```

System Configuration

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

show configuration

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

Finding Configuration Errors

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

show configuration errors

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

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

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

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

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

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

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

Saving the Configuration

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

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

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

```
[local]host_name#
```

To save your current configuration, enter the following command:

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

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

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

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

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

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

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

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

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

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

Chapter 4
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.

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 17. 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**
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**
Verify BGP neighbors on ingress P-GW context	**context** *ingress_pgw_context_name* **show ip bgp summary**
Display IP Connectivity State	
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**

To do this:	Enter this command:
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.	
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]**

To do this:	Enter this command:
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	
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**

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.

Chapter 5
Configuring Subscriber Session Tracing

This chapter provides information on subscriber session trace functionality to allow an operator to trace subscriber activity at various points in the network and at various level of details in EPS network. 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 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.

This chapter discusses following topics for feature support of Subscriber Session Tracing in LTE service:

- Introduction
- Supported Standards
- Supported Networks and Platforms
- Licenses
- Subscriber Session Tracing Functional Description
- Subscriber Session Trace Configuration
- Verifying Your Configuration

Introduction

The 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.

In general, 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 UE connects to the access network.

The EPC network entities like MME, S-GW, P-GW support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. 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

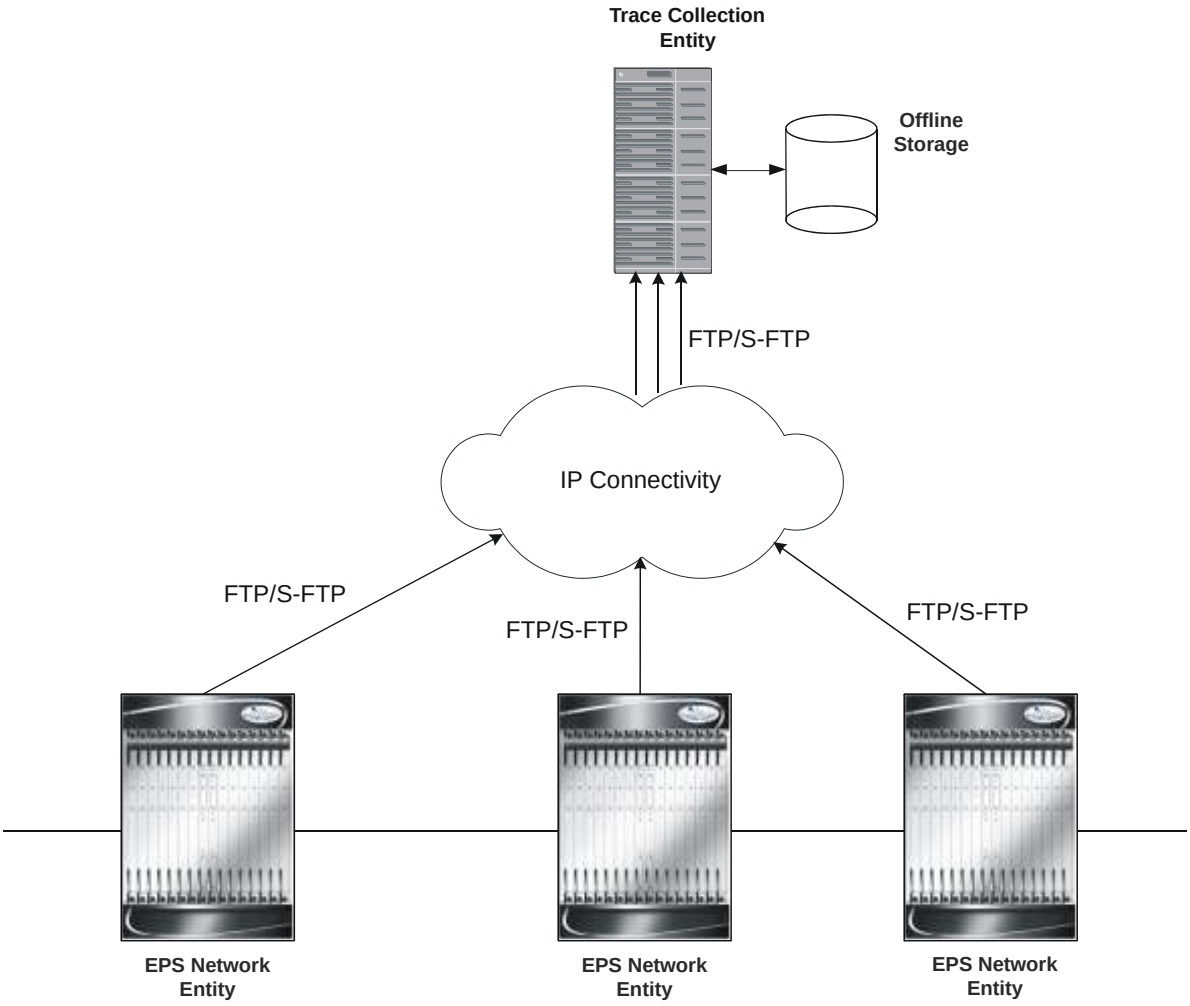
Important: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

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 5000 platforms. 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.

Important: Only Maximum Trace Depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 15. Session Trace Function and Interfaces



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.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Supported Functions

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)

- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity
    - Support up to 32 simultaneous session traces per NE
    - Capacity to activate/deactivate TBD trace sessions per second
    - Each NE can buffer TBD bytes of trace data locally
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
    - MME: S1, S3, S6a, S10, S11
    - S-GW: S4, S5, S8, S11, Gxc
    - PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Collection Entity (TCE) Support
    - Active pushing of files to the TCE
    - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 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)

Supported Networks and Platforms

This feature supports all ASR 5000 Series Platforms with StarOS Release 9.0 or later running MME/S-GW/P-GW service(s) for the core LTE network functions.

Licenses

This is a base feature and available for configuration with default LTE component license(s) on the system:

Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session on EPC nodes:

Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

Trace Session

A trace session is the time between trace activation and trace de-activation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently subscriber session trace is not supported for co-located network elements in EPC network.

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, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

Management Activation

With a management-initiated activation, the WEM sends an activation request directly to the NE where the trace is to be initiated. The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

Signaling Activation

With a signaling based activation, the trace session is indicated to the NE 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).

Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

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 a 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.

Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Data Collection and Reporting

Subscriber session trace functionality supprots data collection and reporting system to provide historical usage adn event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09)

Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages (specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Note: Only Maximum Trace Depth is supported in the current release.

Trace Scope

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

Network Element Details

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

MME

The MME support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1a	eNodeB	N	Y
S3	SGSN	Y	Y
S6a	HSS	Y	N

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S10	MME	Y	Y
S11	S-GW	N	Y

S-GW

The S-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S4	SGSN	N	N
S3	P-GW (Intra-PLMN)	N	Y
S6a	P-GW (Inter-PLMN)	N	N
S11	MME	Y	N

P-GW

The PDN-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S2abc	Various NEs	N	N
S5	S-GW (Intra-PLMN)	Y	N
S6b	AAA Server/Proxy	Y	N
S8	S-GW (Inter-PLMN)	N	N
Gx	Policy Server	Y	N
SGi	IMS	Y	N

Subscriber Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements s in LTE/EPC networks.

Important: This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC networks. Commands that configure additional function 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 the *System Administration Guide* and specific product Administration Guide.

To configure the system to support subscriber session trace collection and trace file transport on a system:

Step 1 Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC Network Element* section.

Step 2 Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.

Step 3 Save the changes to system configuration by applying the example configuration found in *Verifying and Saving Your Configuration* chapter.

Step 4 Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

Enabling Subscriber Session Trace on EPC Network Element

This section provides the configuration example to enable the subscriber session trace on a system at the Exec mode:

```
session trace subscriber network-element {mme | pgw | sgw} {imei
<imei_id>} {imsi <imsi_id>} {interface {all | <interface>}} trace-ref
<trace_ref_id> collection-entity <ip_address>
```

Notes:

- *<interface>* is the name of the interfaces applicable for specific NE on which subscriber session traces have to be collected. For more information, refer **`session trace subscriber`** command in the *Command Line Interface Reference*.
- *<trace_ref_id>* is the configured Trace Id to be used for this trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- *<ip_address>* is the IP address of Trace collection Entity in IPv4 notation.

Trace File Collection Configuration

This section provides the configuration example to configure the trace file collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

```
configure

   session trace [ collection-timer <dur> ] [ network-element { all | mme
| pgw | sgw } ] [ retry-timer <dur> ] [ tce-mode { none | push transport
{ ftp | sftp } path <string> username <name> { encrypted password
<enc_pw> | password <password> } } ]

   end
```

Notes:

- *<string>* is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer **session trace** command in the *Command Line Interface Reference*.

Verifying Your Configuration

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

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

These instructions are used to verify the Subscriber Session Trace configuration.

Step 1 Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:

```
show session trace statistics
```

The output of this command displays the statistics of the session trace instance.

```
Num current trace sessions: 5

Total trace sessions activated: 15

Total Number of trace session activation failures: 2

Total Number of trace recording sessions triggered: 15

Total Number of messages traced: 123

Number of current TCE connections: 2

Total number of TCE connections: 3

Total number of files uploaded to all TCEs: 34
```

Step 2 View the session trace references active for various network elements in an EPC network by entering the following command in Exec Mode:

```
show session trace trace-summary
```

The output of this command displays the summary of trace references for all network elements:

```
MME

  Trace Reference: 310012012345

  Trace Reference: 310012012346

SGW

  Trace Reference: 310012012345
```

```
  Trace Reference: 310012012346
PGW
  Trace Reference: 310012012347
```

Appendix A
Sample Configuration Files

This appendix contains sample configuration files for the P-GW. The following configurations are supported:

- Standalone eGTP PDN Gateway
- Standalone PMIPv6 PDN Gateway Supporting an eHRPD Network

In each configuration example, commented lines are labeled with the number symbol (#) and variables are identified using italics within brackets (<*variable*>).

Standalone eGTP PDN Gateway

Configuration Sample

```
# Configuration file for an ASR 5000 in an eGTP P-GW role
#
# Send P-GW licenses
configure /flash/flashconfig/<pgw_license_name>.cfg
end
#
# Set system to not require confirmation when creating new contexts
and/or services. Config file must end with "no autoconfirm" to return the
CLI to its default setting.
#
configure
   autoconfirm
#
# Configure ASR 5000 cards
#
# Activate the PSCs
   card <slot_number>
      mode active psc
      exit
   card <slot_number>
      mode active psc
      exit
```

```
# Repeat for the number of PSCs in the system
   end
#
# Modify the local context for local system management
config
   context local
      interface <name>
         ip address <address> <mask>
         exit
      server ftpd
         exit
      ssh key <key> length <bytes>
      server sshd
         subsystem sftp
         exit
      server telnetd
         exit
      subscriber default
         exit
      administrator <name> encrypted password <password> ftp
      aaa group 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
      exit
```

```
   ntp
      enable
      server <ip_address>
      exit
   snmp engine-id local <id>
   snmp notif-threshold <count> low <low_count> period <seconds>
   snmp authentication-failure-trap
   snmp heartbeat interval <minutes>
   snmp community <string> read-write
   snmp target <name> <ip_address>
   system contact <string>
   system location <string>
# P-GW context configuration
   gtpp single-source
   context <pgw_context_name>
      interface <s5s8_interface_name>
         ip address <ipv4_address>
# note alternative IPv6 address:
         ipv6 address <address>
         exit
      gtpp group default
         gtpp charging-agent address <gx_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 trigger egcdr max-losdv
         gtpp egcdr losdv-max-containers <number>
```

```
    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>
    exit
subscriber default
    exit
apn <rf_acct_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>
    exit
aaa group <gz_acct_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>
            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>
            exit
        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_ip_address>
            exit
        gtpu-service <gtpu_service_name>
            bind ipv4-address <s5s8_interface_ip_address>
    # note alternative IPv6 address:
            bind ipv6-address <s5s8_interface_ip_address>
            exit
```

```
      pgw-servers <pgw_service_name> -noconfirm
         associate egtp-service <egtp_service_name>
         associate qci-qos-mapping <name>
         fqdn host <domain_name> realm <realm_name>
         plmn id mcc <id> mnc <id>
         exit
      ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <s5s8_interface_name> <pgw_context_name>
      exit
# PDN context configuration
   context <pdn_context_name> -noconfirm
      interface <pdn_sgi_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <pdn_sgi_ipv6_interface_name>
         ipv6 address <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>
         exit
   # Enabling active charging
      require active-charging optimized-mode
      active-charging service <name>
         ruledef <name>
            <rule_definition>
                  .
                  .
            <rule_definition>
            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 egcdr
   qos-class-identifier <id>
   allocation-retention-priority <priority>
   tft-packet-filter qci3
   exit
charging-action static
   service-identifier <id>
   billing-action egcdr
   qos-class-identifier <id>
   allocation-retention-priority <priority>
   tft-packet-filter qci3
   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>
         exit
      exit
# AAA and policy
   context <aaa_context_name> -noconfirm
      interface <gx_interface_name>
         ipv6 address <address>
# note alternative IPv4 address:
         ip address <ipv4_address>
         exit
      interface <gy_interface_name>
         ipv6 address <address>
```

```
# note alternative IPv4 address:
        ip address <ipv4_address>
        exit
      interface <gz_interface_name>
        ip address <ipv4_address>
        exit
      interface <rf_interface_name>
        ip address <ipv4_address>
# note alternative IPv6 address:
        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_ipv6_adr>
# note alternative IPv4 address:
        p-cscf table <#> row-precedence <#> ip-address <pcrf_ipv4_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_context_ip_address>
        peer <gx_cfg_name> realm <name> address <pcrf_ip_addr>
```

```
        route-entry peer <gx_cfg_name>
        exit
    diameter endpoint <gy_cfg_name>
        origin realm <realm_name>
        origin host <name> address <aaa_context_ip_address>
        peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
        route-entry peer <gy_cfg_name>
        exit
    diameter endpoint <rf_cfg_name>
        origin realm <realm_name>
        origin host <name> address <aaa_context_ip_address>
        peer <rf_cfg_name> realm <name> address <ofcs_ip_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>
      exit
# QCI-QoS mapping
   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
```

Standalone PMIPv6 PDN Gateway Supporting an eHRPD Network

Configuration Sample

```
# Configuration file for an ASR 5000 in a PMIPv6 P-GW role supporting an eHRPD
network
#
# Send P-GW licenses
configure /flash/flashconfig/<pgw_license_name>.cfg
end
#
# Set system to not require confirmation when creating new contexts
and/or services. Config file must end with "no autoconfirm" to return the
CLI to its default setting.
#
configure
   autoconfirm
#
# Configure ASR 5000 cards
#
# Activate the PSCs
   card <slot_number>
      mode active psc
      exit
   card <slot_number>
```

```
      mode active psc
      exit
# Repeat for the number of PSCs in the system
   end
#
# Modify the local context for local system management
config
   context local
      interface <name>
         ip address <address> <mask>
         exit
      server ftpd
         exit
      ssh key <key> length <bytes>
      server sshd
         subsystem sftp
         exit
      server telnetd
         exit
      subscriber default
         exit
      administrator <name> encrypted password <password> ftp
      aaa group 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
      exit
   ntp
      enable
      server <ip_address>
      exit
   snmp engine-id local <id>
   snmp notif-threshold <count> low <low_count> period <seconds>
   snmp authentication-failure-trap
   snmp heartbeat interval <minutes>
   snmp community <string> read-write
   snmp target <name> <ip_address>
   system contact <string>
   system location <string>
# P-GW context configuration
   context <pgw_context_name>
      interface <s2a_interface_name>
         ipv6 address <ipv6_address>
            tunnel-mode ipv6ip
               source interface <name>
               destination address <ipv4_or_ipv6_address>
               exit
            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
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>
   exit
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>
         exit
      lma-service <lma_service_name> -noconfirm
         no aaa accounting
         revocation enable
         bind address <s2a_interface_ipv6_address>
         exit
      pgw-service <pgw_service_name>
         associate lma-service <lma_service_name>
         associate qci-qos-mapping <name>
         authorize external
         plmn id mcc <id> mnc <id>
         exit
      ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <s2a8_interface_name> <pgw_context_name>
      exit
# PDN context configuration
```

```
context <pdn_context_name> -noconfirm
   interface <pdn_sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
   interface <pdn_sgi_ipv6_interface_name>
      ipv6 address <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 <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>
```

```
      exit
# Enabling active charging
   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
      rulebase default
```

```
            exit
         rulebase <name>
            <rule_base>
               .
               .
            <rule_base>
            exit
         exit
   # AAA and policy
      context <aaa_context_name> -noconfirm
         interface <gx_interface_name>
            ipv6 address <address>
   # note alternative IPv4 address:
            ip address <ipv4_address>
            exit
         interface <gy_interface_name>
            ipv6 address <address>
   # note alternative IPv4 address:
            ip address <ipv4_address>
            exit
         interface <s6b_interface_name>
            ip address <ipv4_address>
   # note alternative IPv6 address:
            ipv6 address <address>
            exit
         interface <rf_interface_name>
            ip address <ipv4_address>
   # note alternative IPv6 address:
            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_ipv6_adr>
   # note alternative IPv4 address:
            p-cscf table <#> row-precedence <#> ip-address <pcrf_ipv4_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_context_ip_address>
            peer <gx_cfg_name> realm <name> address <pcrf_ip_addr>
            route-entry peer <gx_cfg_name>
            exit
         diameter endpoint <gy_cfg_name>
            origin realm <realm_name>
            origin host <name> address <aaa_context_ip_address>
            peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
            route-entry peer <gy_cfg_name>
            exit
         diameter endpoint <s6b_cfg_name>
            origin realm <realm_name>
```

```
            origin host <name> address <aaa_context_ip_address>
            peer <s6b_cfg_name> realm <name> address <3gpp_aaa_ip_addr>
            route-entry peer <s6b_cfg_name>
            exit
         diameter endpoint <rf_cfg_name>
            origin realm <realm_name>
            origin host <name> address <aaa_context_ip_address>
            peer <rf_cfg_name> realm <name> address <ofcs_ip_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 <s6b_interface_name> <aaa_context_name>
         exit
      port ethernet <slot_number/port_number>
         no shutdown
         bind interface <rf_interface_name> <aaa_context_name>
         exit
   # QCI-QoS mapping
      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
```

Appendix B
P-GW Engineering Rules

This appendix provides PDN Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5000 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 rules are covered in this appendix:

- Interface and Port Rules
- P-GW Context and Service Rules
- P-GW Subscriber Rules

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.

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 HSGWs or S-GWs addresses per P-GW.
    - The system maintains statistics for a maximum of 8192 peer HSGWs or S-GWs per P-GW service.
    - If more than 8192 HSGWs or S-GWs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 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.