Cisco ASR 5000 Series HRPD Serving Gateway Administration Guide

Version 10.0

Last Updated August 6, 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-22984-01

Cisco ASR 5000 Series HRPD Serving Gateway Administration Guide

CONTENTS

About this Guide vii
Conventions Used viii
Contacting Customer Support x
HRPD Serving Gateway Overview 11
eHRPD Network Summary 12
eHRPD Network Components 13
Evolved Access Network (eAN) 13
Evolved Packet Control Function (ePCF) 13
HRPD Serving Gateway (HSGW) 13
E-UTRAN EPC Network Components 14
eNodeB 14
Mobility Management Entity (MME) 14
Serving Gateway (S-GW) 15
PDN Gateway (P-GW) 15
Product Description 17
Basic Features 18
Authentication 18
IP Address Allocation 19
Quality of Service 19
AAA, Policy and Charging 20
Product Specifications 21
Licenses 21
Hardware Requirements 21
Platforms 21
Components 21
Operating System Requirements 22
Network Deployment(s) 23
HRPD Serving Gateway in an eHRPD Network 23
Supported Logical Network Interfaces (Reference Points) 24
Features and Functionality - Base Software 28
Subscriber Session Management Features 28
Proxy Mobile IPv6 (S2a) 28
Mobile IP Registration Revocation 29
Session Recovery Support 29
Non-Optimized Inter-HSGW Session Handover 30
Quality of Service Management Features 30
DSCP Marking 31
UE Initiated Dedicated Bearer Resource Establishment 31
Network Access and Charging Management Features 32
EAP Authentication (STa) 32
Rf Diameter Accounting 32
AAA Server Groups 33
Dynamic Policy and Charging: Gxa Reference Interface 33
Intelligent Traffic Control 34
Network Operation Management Functions 34
A10/A11 34

Multiple PDN Support 35
P-GW Selection (Discovery) 35
PPP VSNCP 36
Congestion Control 36
IP Access Control Lists 37
System Management Features 37
Management System 37
Bulk Statistics Support 39
Threshold Crossing Alerts (TCA) Support 40
ANSI T1.276 Compliance 41
Features and Functionality - External Application Support 42
Web Element Management System 42
Features and Functionality - Optional Enhanced Feature Software 44
IP Header Compression (RoHCv1 for IPv6) 44
IP Security (IPSec) 44
Traffic Policing and Shaping 45
Traffic Policing 45
Traffic Shaping 46
Layer 2 Traffic Management (VLANs) 46
Call/Session Procedure Flows 47
Initial Attach with IPv6/IPv4 Access 47
PMIPv6 Lifetime Extension without Handover 49
PDN Connection Release Initiated by UE 50
PDN Connection Release Initiated by HSGW 52
PDN Connection Release Initiated by P-GW 53
Supported Standards 56
3GPP References 56
3GPP2 References 56
IETF References 57
Object Management Group (OMG) Standards 57

HSGW Configuration 59

Configuring the System to Perform as a Standalone HSGW 60
Information Required 60
Required Local Context Configuration Information 60
Required HSGW Context Configuration Information 61
Required MAG Context Configuration Information 62
Required AAA Context Configuration Information 62
How This Configuration Works 64
Configuration 66
Initial Configuration 67
HSGW and MAG Service Configuration 71
AAA and Policy Configuration 72
Optional Header Compression Configuration 75
Verifying and Saving the Configuration 76

Verifying and Saving Your Configuration 77

Verifying the Configuration 78
Feature Configuration 78
Service Configuration 79
Context Configuration 80
System Configuration 80
Finding Configuration Errors 80
Saving the Configuration 82
Saving the Configuration on the Chassis 83

Monitoring the Service 85

Monitoring System Status and Performance 86
Clearing Statistics and Counters 88
HSGW Engineering Rules 89
Interface and Port Rules 90
A10/A11 Interface Rules 90
S2a Interface Rules 90
MAG to LMA Rules 90
HSGW Service Rules 92
HSGW Subscriber Rules 93
Sample Configuration Files 95
Standalone eHRPD Serving Gateway 96
Configuration Sample 96

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
HRPD Serving Gateway Overview

The ASR 5000 provides wireless carriers with a flexible solution that functions as an HRPD Serving Gateway (HSGW) in 3GPP2 evolved High Rate Packet Data (eHRPD) wireless data networks.

This overview provides general information about the HSGW including:

- eHRPD Network Summary
- Product Description
- Product Specifications
- Network Deployment(s)
- Features and Functionality - Base Software
- Features and Functionality - External Application Support
- Features and Functionality - Optional Enhanced Feature Software
- Call Session Procedure Flows
- Supported Standards

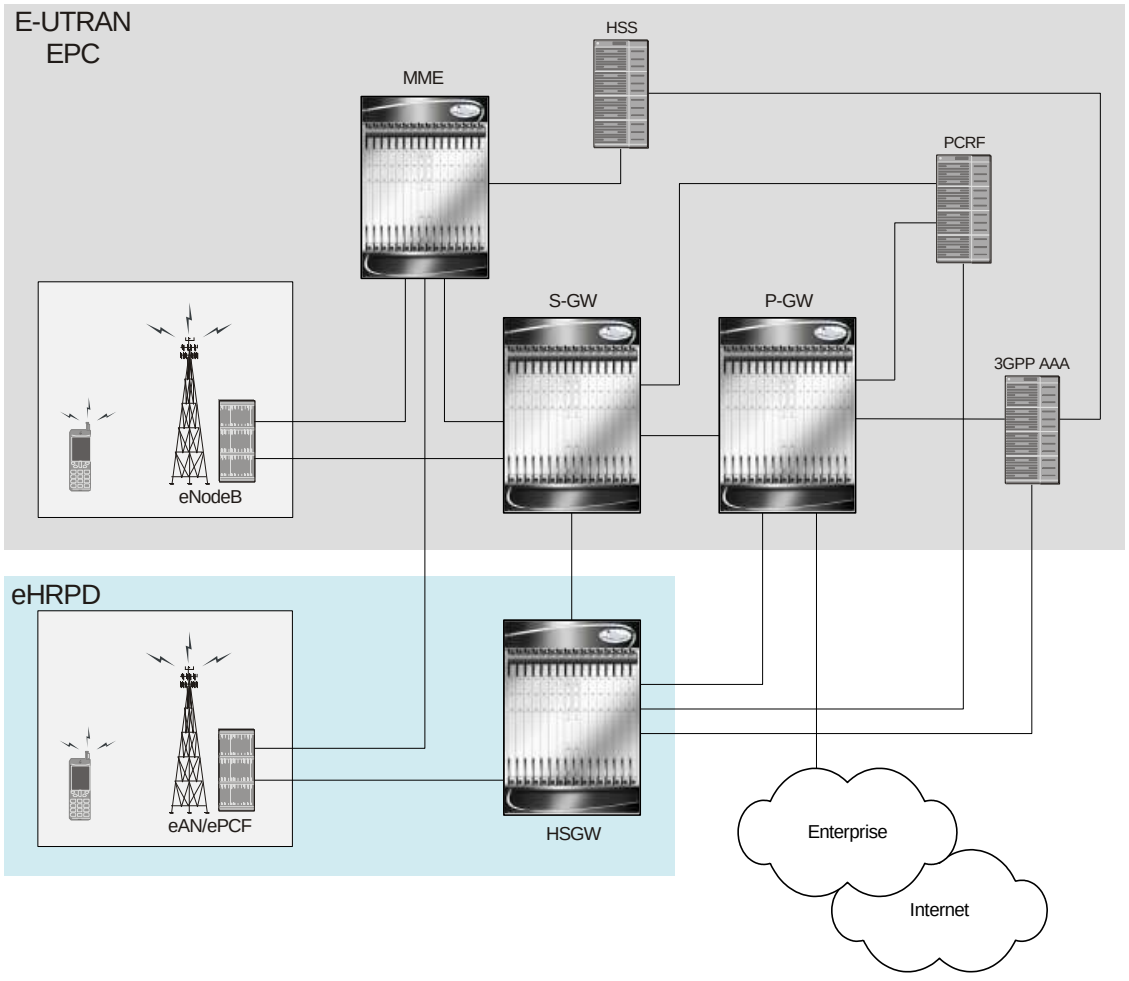
eHRPD Network Summary

In a High Rate Packet Data (HRPD) network, the method of 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).

The eHRPD network's main function is to provide interworking of the mobile node with the Evolved Packet System (EPS). The EPS is a 3GPP Enhanced UMTS Terrestrial Radio Access Network/Evolved Packet Core (E-UTRAN/EPC). The E-UTRAN/EPC is the core data network of the 4G System Architecture Evolution (SAE) network supporting the Long Term Evolution Radio Access Network (LTE RAN).

The following figure shows the physical relationship of the eHRPD network with the E-UTRAN/EPC.



The primary functions of the eHRPD network are:

- Connectivity to LTE core (EPC)

- Support for multiple PDN connections
- Leverage existing CDMA infrastructure
- Migration path to LTE
- Minimal changes to RAN infrastructure
- Support handoffs between LTE RAN(E-UTRAN) and eHRPD

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

E-UTRAN EPC Network Components

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

eNodeB

The eNodeB (eNB) is the LTE base station and is one of two nodes in the SAE Architecture user plane (the other is the S-GW). The eNB communicates with other eNBs via the X2 interface. The eNB 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 stream
- 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
- PGW and SGW 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 P-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 PMIP6

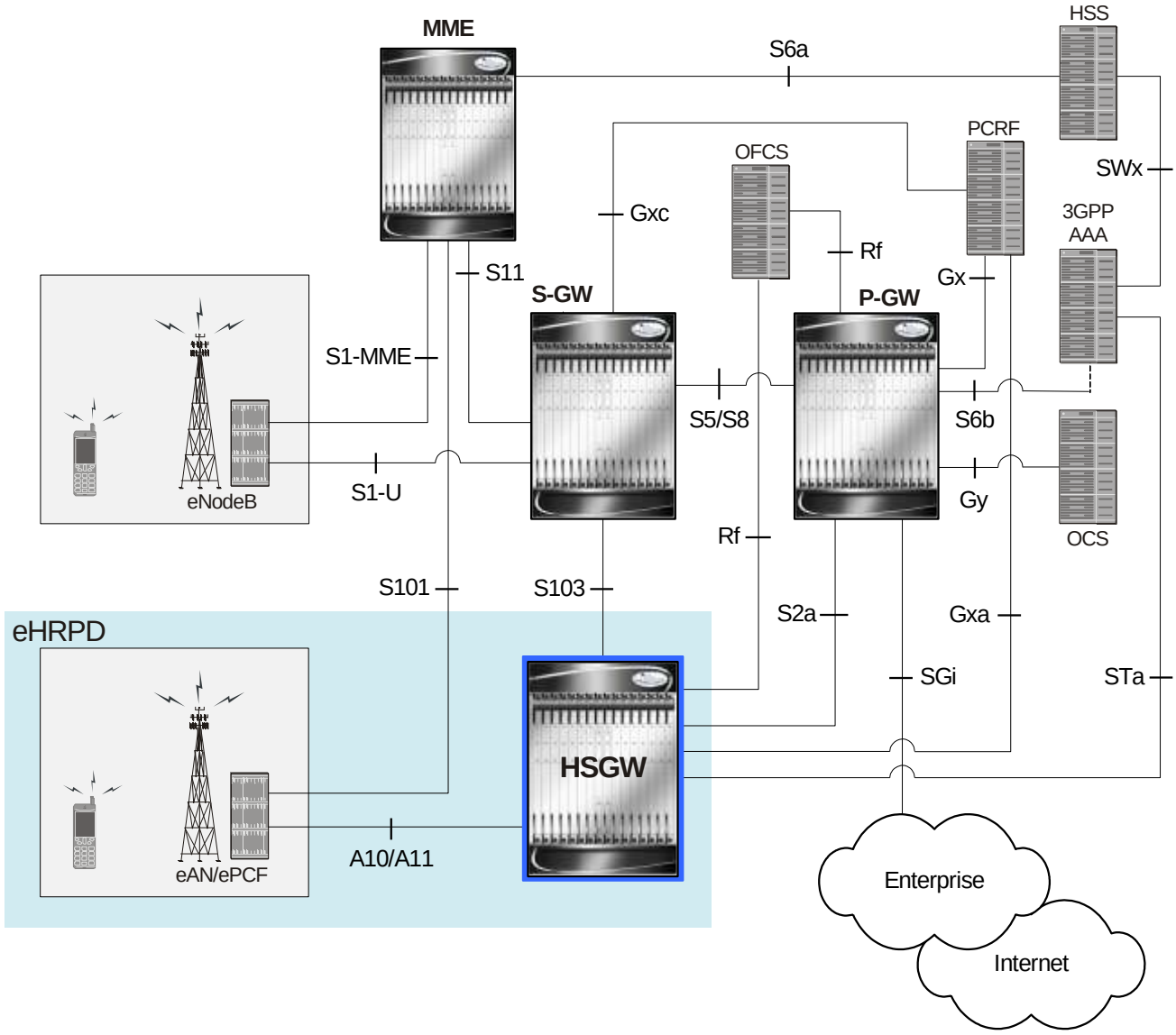
Product Description

The HSGW terminates the eHRPD access network interface from the Evolved Access Network/Evolved Packet Core Function (eAN/ePCF) and routes UE-originated or terminated packet data traffic. It provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE core network and performs the following functions:

- Mobility anchoring for inter-eAN handoffs
- Transport level packet marking in the uplink and the downlink, e.g., setting the DiffServ Code Point, based on the QCI of the associated EPS bearer
- Uplink and downlink charging per UE, PDN, and QCI
- Downlink bearer binding based on policy information
- Uplink bearer binding verification with packet dropping of UL traffic that does not comply with established uplink policy
- MAG functions for S2a mobility (i.e., Network-based mobility based on PMIPv6)
- Support for IPv4 and IPv6 address assignment
- EAP Authenticator function
- Policy enforcement functions defined for the Gxa interface
- Robust Header Compression (RoHC)
- Support for VSNCP and VSNP with UE
- Support for packet-based or HDLC-like framing on auxiliary connections
- IPv6 SLACC support, generating RAs responding to RSs

An HSGW also establishes, maintains and terminates link layer sessions to UEs. The HSGW functionality provides interworking of the UE with the 3GPP EPS architecture and protocols. This includes support for mobility, policy control and charging (PCC), access authentication, and roaming. The HSGW also manages inter-HSGW handoffs.

Figure 1. eHRPD Basic Network Topology



Basic Features

Authentication

The HSGW supports the following authentication features:

- EAP over PPP
- UE and HSGW negotiates EAP as the authentication protocol during LCP
- HSGW is the EAP authenticator
- EAP-AKA' (trusted non-3GPP access procedure) as specified in TS 33.402
- EAP is performed between UE and 3GPP AAA over PPP/STa

For more information on authentication features, refer to the Network Access and Charging Management Features section in this overview.

IP Address Allocation

The HSGW supports the following IP address allocation features:

- Support for IPv4 and IPv6 addressing
- Types of PDNs - IPv4, IPv6 or IPv4v6
- IPv6 addressing
  - Interface Identifier assigned during initial attach and used by UE to generate it's link local address
  - HSGW sends the assigned /64 bit prefix in RA to the UE
  - Configure the 128-bits IPv6 address using IPv6 SLAAC (RFC 4862)
  - Optional IPv6 parameter configuration via stateless DHCPv6(Not supported)
- IPv4 address
  - IPv4 address allocation during attach
  - Deferred address allocation using DHCPv4(Not supported)
  - Option IPv4 parameter configuration via stateless DHCPv4(Not supported)

Quality of Service

The HSGW supports the following QoS features:

- HRPD Profile ID to QCI Mapping
- DSCP Marking
- UE Initiated Dedicated Bearer Resource Establishment
- QCI to DSCP Mapping

For more information on QoS features, refer to the Quality of Service Management Features section in this overview.

AAA, Policy and Charging

The HSGW supports the following AAA, policy and charging features:

- EAP Authentication (STa)
- Rf Diameter Accounting
- AAA Server Groups
- Dynamic Policy and Charging: Gxa Reference Interface
- Intelligent Traffic Control

For more information on policy and charging features, refer to the Network Access and Charging Management Features section in this overview.

Product Specifications

The following information is located in this section:

- Licenses
- Hardware Requirements
- Operating System Requirements

Licenses

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

The following licenses are available for this product:

- HSGW Software License, 10k Sessions - 600-00-7641
- HSGW Software License, 1k Sessions - 600-00-7650

Hardware Requirements

Information in this section describes the hardware required to enable HSGW services.

Platforms

The HSGW service operates on the ASR 5000 platform.

Components

The following application and line cards are required to support HSGW functionality on an ASR 5000:

- **System Management Cards (SMCs)**: Provides full system control and management of all cards within the chassis. Up to two SMCs can be installed; one active, one redundant.
- **Packet Services Cards (PSCs)**: The PSCs provide high-speed, multi-threaded PDP context processing capabilities for HSGW services. Up to 14 PSCs 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 eHRPD data network. Up to 26 line cards can be installed for a fully loaded system with 13 active PSCs, 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 the HSGW or 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 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 *Cisco ASR 5000 Series Product Overview Guide*.

Operating System Requirements

The HSGW is available for all Cisco Systems ASR 5000 platforms running StarOS Release 9.0 or later.

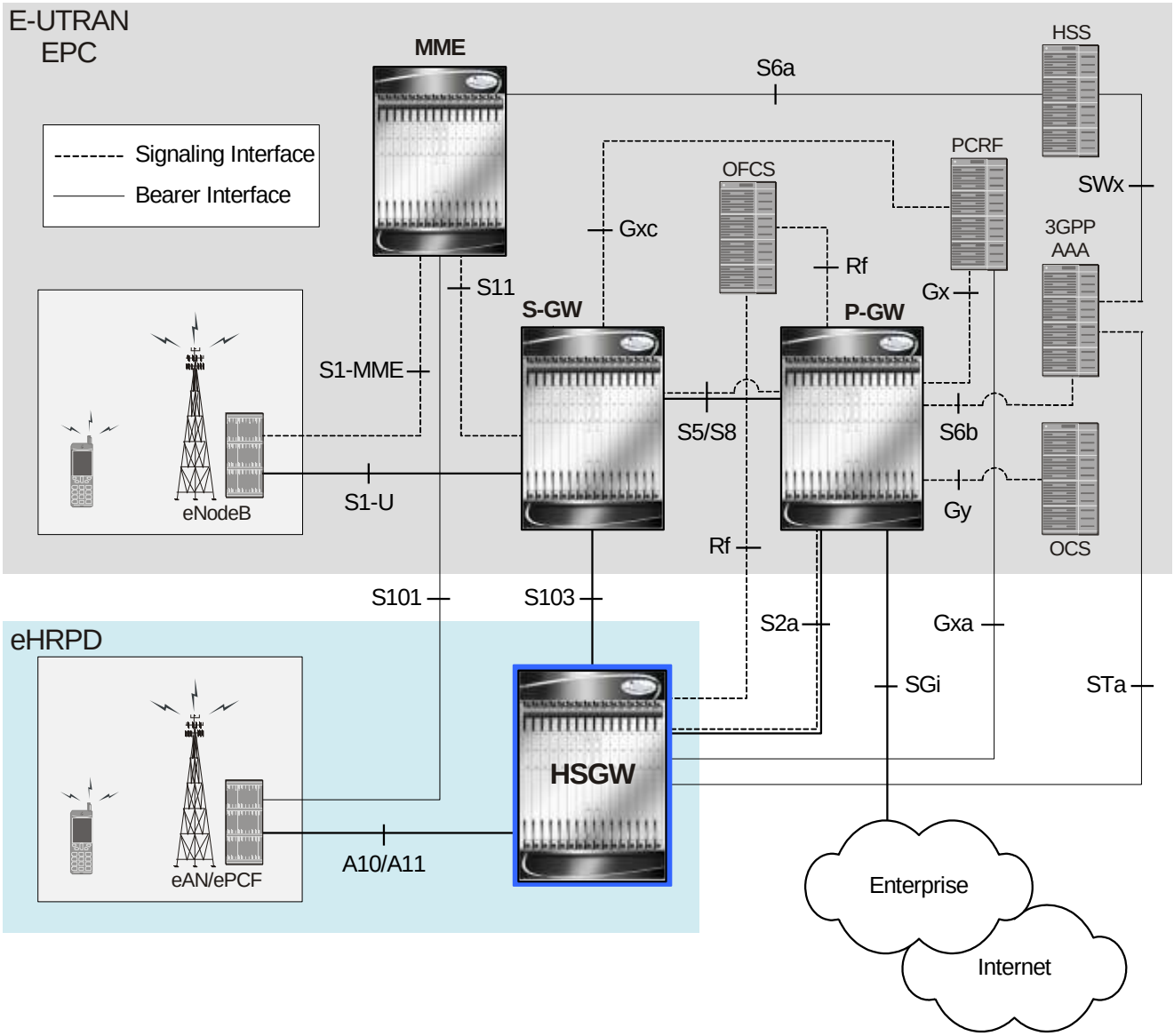
Network Deployment(s)

This section describes the supported interfaces and the deployment scenario of an HSGW in an eHRPD network.

HRPD Serving Gateway in an eHRPD Network

The following figure displays a simplified network view of the HSGW in an eHRPD network and how it interconnects with a 3GPP Evolved-UTRAN/Evolved Packet Core network. The interfaces shown in the following graphic are standards-based and are presented for informational purposes only. For information on interfaces supported by Cisco Systems' HSGW, refer to the next section,.

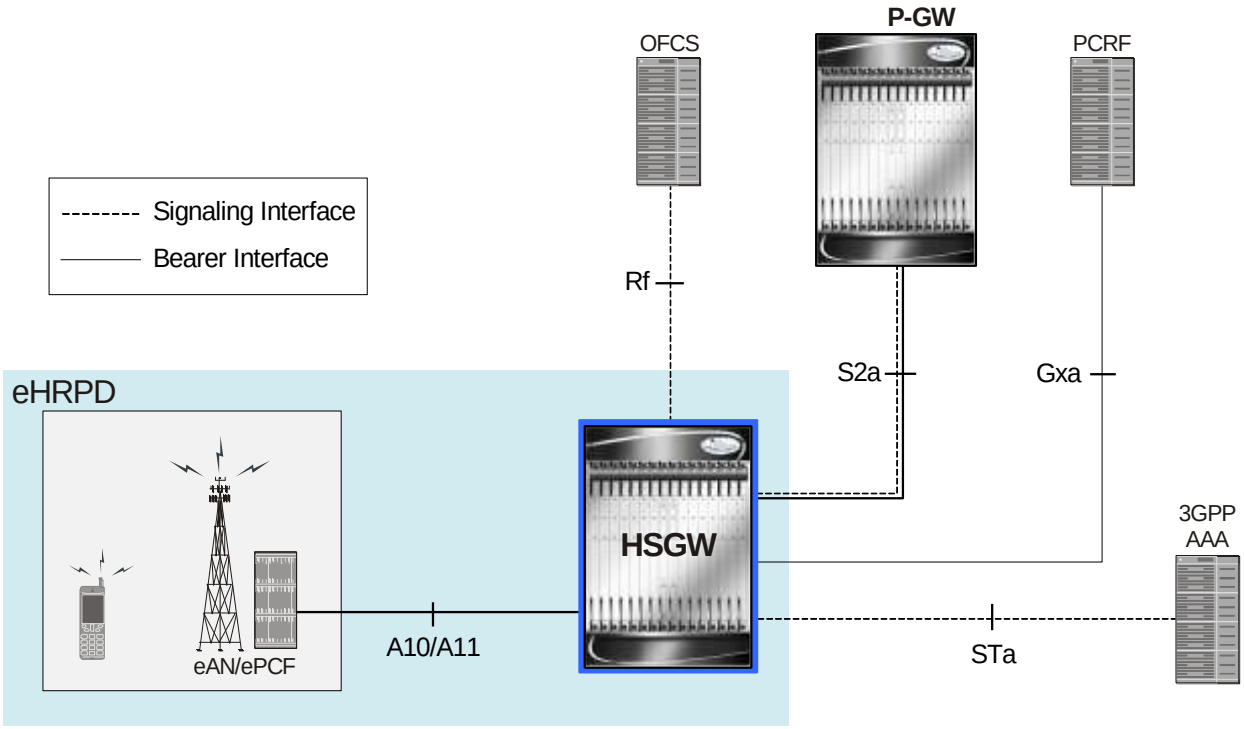
Figure 2. HSGW in an eHRPD Network Architecture



Supported Logical Network Interfaces (Reference Points)

The HSGW supports many of the standards-based logical network interfaces or reference points. The graphic below and following text define the supported interfaces. Basic protocol stacks are also included.

Figure 3. HSGW Supported Network Interfaces

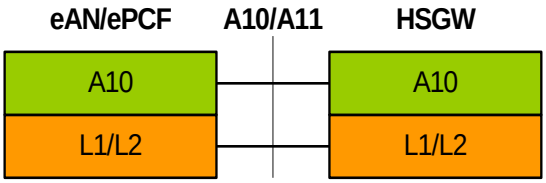


In support of both mobile and network originated subscriber PDP contexts, the HSGW provides the following network interfaces:

A10/A11

This interface exists between the Evolved Access Network/Evolved Packet Control

Function (eAN/ePCF) and the HSGW and implements the A10 (signaling) and A11 (bearer) protocols defined in 3GPP2 specifications.

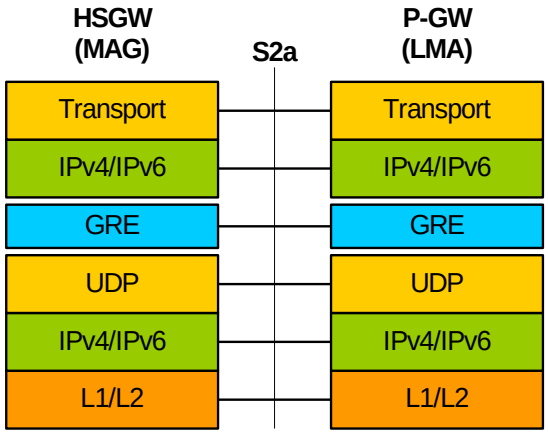


S2a Interface

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

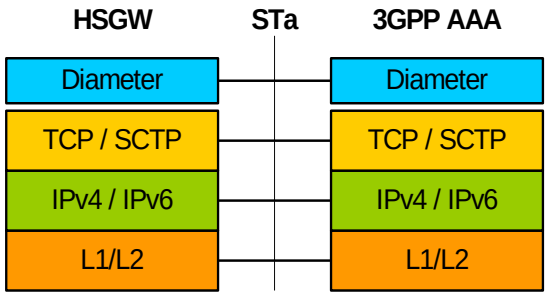


STa Interface

This signaling interface supports Diameter transactions between a 3GPP2 AAA proxy and a 3GPP AAA server. This interface is used for UE authentication and authorization.

Supported protocols:

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

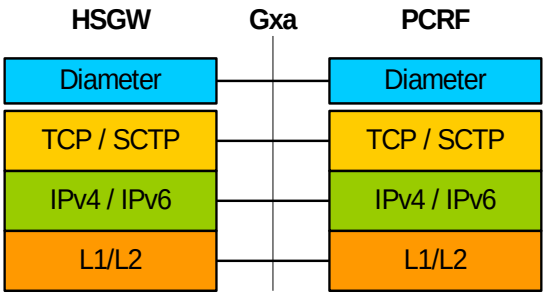


Gxa Interface

This signalling interface supports the transfer of policy control information (QoS) between the HSGW (BBERF) and a PCRF.

Supported protocols:

- Transport Layer: TCP, SCTP
- 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 HSGW 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 HSGW service, refer to the configuration examples provided in the HSGW Administration Guide.

The following features 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:

- Proxy Mobile IPv6 (S2a)
- Mobile IP Registration Revocation
- Session Recovery Support
- Non-Optimized Inter-HSGW Session Handover

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 PDN Gateway. 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 (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 PDN Gateway 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 PGW.

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

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. 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

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

This feature is also useful for Software Patch Upgrade activities. If session recovery feature is enabled during the software patch upgrading, it helps to permit preservation of existing sessions on the active PSC during the upgrade process.

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

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

The additional hardware resources required for session recovery include a standby system processor card (SPC) and a standby PSC.

There are two modes for Session Recovery.

- **Task recovery mode**: Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby PSC. In this mode, recovery is performed by using the mirrored "standby-mode" session manager task(s) running on active PSCs. The "standby-mode" task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full PSC recovery mode**: Used when a PSC hardware failure occurs, or when a PSC migration failure happens. In this mode, the standby PSC is made active and the "standby-mode" session manager and AAA manager tasks on the newly activated PSC perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different PSCs to ensure task recovery.

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

Non-Optimized Inter-HSGW Session Handover

Enables non-optimized roaming between two eHRPD access networks that lack a relationship of trust and when there are no SLAs in place for low latency hand-offs.

Inter-HSGW hand-overs without context transfers are designed for cases in which the user roams between two eHRPD networks where no established trust relationship exists between the serving and target operator networks. Additionally no H1/H2 optimized hand-over interface exists between the two networks and the Target HSGW requires the UE to perform new PPP LCP and attach procedures. Prior to the hand-off the UE has a complete data path with the remote host and can send and receive packets via the eHRPD access network and HSGW & PGW in the EPC core.

The UE eventually transitions between the Serving and Target access networks in active or dormant mode as identified via A16 or A13 signaling. The Target HSGW receives an A11 Registration Request with VSNCP set to "Hand-Off". The request includes the IP address of the Serving HSGW, the MSID of the UE and information concerning existing A10 connections. Since the Target HSGW lacks an authentication context for the UE, it sends the LCP config-request to trigger LCP negotiation and new EAP-AKA procedures via the STa reference interface. After EAP success, the UE sends its VSNCP Configure Request with Attach Type equal to "Hand-off". It also sets the IP address to the previously assigned address in the PDN Address Option. The HSGW initiates PMIPv6 binding update signaling via the S2a interface to the PGW and the PGW responds by sending a PMIPv6 Binding Revocation Indication to the Serving HSGW.

Quality of Service Management Features

This section describes the following features:

- DSCP Marking
- UE Initiated Dedicated Bearer Resource Establishment

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For Interactive Traffic class, the HSGW supports per-HSGW 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

UE Initiated Dedicated Bearer Resource Establishment

Enables a real-time procedure as applications are started, for the Access Terminal to request the appropriate end-to-end QoS and service treatment to satisfy the expected quality of user experience.

Existing HRPD applications use UE/AT initiated bearer setup procedures. As a migration step toward the EUTRAN-based LTE-SAE network model, the e-HRPD architecture has been designed to support two approaches to resource allocation that include network initiated and UE initiated dedicated bearer establishment. In the StarOS 9.0 release, the HSGW will support only UE initiated bearer creation with negotiated QoS and flow mapping procedures.

After the initial establishment of the e-HRPD radio connection, the UE/AT uses the A11' signaling to establish the default PDN connection with the HSGW. As in the existing EV-DO Rev A network, the UE uses RSVP setup procedures to trigger bearer resource allocation for each additional dedicated EPC bearer. The UE includes the PDN-ID, ProfileID, UL/DL TFT, and ReqID in the reservation.

Each Traffic Flow Template (referred to as Service Data Flow Template in the LTE terminology) consists of an aggregate of one or more packet filters. Each dedicated bearer can contain multiple IP data flows that utilize a common QoS scheduling treatment and reservation priority. If different scheduling classes are needed to optimize the quality of user experience for any service data flows, it is best to provision additional dedicated bearers. The UE maps each TFT packet filter to a Reservation Label/FlowID. The UE sends the TFT to the HSGW to bind the DL SDF IP flows to a FlowID that is in turn mapped to an A10 tunnel toward the RAN. The HSGW uses the RSVP signaling as an event trigger to request Policy Charging and Control (PCC) rules from the PCRF. The HSGW maps the provisioned QoS PCC rules and authorized QCI service class to ProfileID's in the RSVP response to the UE. At the final stage the UE

establishes the auxiliary RLP and A10' connection to the HSGW. Once that is accomplished traffic can begin flowing across the dedicated bearer.

Network Access and Charging Management Features

This section describes the following features:

- EAP Authentication (STa)
- Rf Diameter Accounting
- AAA Server Groups
- Dynamic Policy and Charging: Gxa Reference Interface
- Intelligent Traffic Control

EAP Authentication (STa)

Enables secure user and device level authentication with a 3GPP AAA server or via 3GPP2 AAA proxy and the authenticator in the HSGW.

In an evolved HRPD access network, the HSGW uses the Diameter based STa interface to authenticate subscriber traffic with the 3GPP AAA server. Following completion of the PPP LCP procedures between the UE and HSGW, the HSGW selects EAP-AKA as the method for authenticating the subscriber session. EAP-AKA uses symmetric cryptography and pre-shared keys to derive the security keys between the UE and EAP server. EAP-AKA user identity information (NAI=IMSI) is conveyed over EAP-PPP between the UE and HSGW.

The HSGW represents the EAP authenticator and triggers the identity challenge-response signaling between the UE and back-end 3GPP AAA server. On successful verification of user credentials the 3GPP AAA server obtains the Cipher Key and Integrity Key from the HSS. It uses these keys to derive the Master Session Keys (MSK) that are returned on EAP-Success to the HSGW. The HSGW uses the MSK to derive the Pair-wise Mobility Keys (PMK) that are returned in the Main A10' connection to the e-PCF. The RAN uses these keys to secure traffic transmitted over the wireless access network to the UE.

After the user credentials are verified by the 3GPP AAA and HSS the HSGW returns the PDN address in the VSNCP signaling to the UE. In the e-HRPD connection establishment procedures the PDN address is triggered based on subscription information conveyed over the STa reference interface. Based on the subscription information and requested PDN-Type signaled by the UE, the HSGW informs the PDN GW of the type of required address (v6 HNP and/or IPv4 Home Address Option for dual IPv4/v6 PDNs).

Rf Diameter Accounting

Provides the framework for offline charging in a packet switched domain. The gateway support nodes use the Rf interface to convey session related, bearer related or service specific charging records to the CGF and billing domain for enabling charging plans.

The Rf reference interface enables offline accounting functions on the HSGW in accordance with 3GPP Release 8 specifications. In an LTE application the same reference interface is also supported on the S-GW and PDN Gateway

platforms. The systems use the Charging Trigger Function (CTF) to transfer offline accounting records via a Diameter interface to an adjunct Charging Data Function (CDF) / Charging Gateway Function (CGF). The HSGW and Serving Gateway collect charging information for each mobile subscriber UE pertaining to the radio network usage while the P-GW collects charging information for each mobile subscriber related to the external data network usage.

The ASR 5000 Charging Trigger Function features dual redundant 140GB RAID hard drives and up to 100GB of capacity on each drive is reserved for writing charging records (CDRs, UDRs, and FDRs) to local file directories with non-volatile persistent memory. The CTF periodically uses the sFTP protocol to push charging files to the CDF/CGF. It is also possible for the CDF/CGF to pull offline accounting records at various intervals or times of the day.

The HSGW, SGW and PGW collect information per-user, per IP CAN bearer or per service. Bearer charging is used to collect charging information related to data volumes sent to and received from the UE and categorized by QoS traffic class. Users can be identified by MSISDN or IMSI. Flow Data Records (FDRs) are used to correlate application charging data with EPC bearer usage information. The FDRs contain application level charging information like service identifiers, rating groups, IMS charging identifiers that can be used to identify the application. The FDRs also contain the authorized QoS information (QCI) that was assigned to a given flow. This information is used correlate charging records with EPC bearers.

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 and Charging: Gxa Reference Interface

Enables network initiated policy based usage controls for such functions as service data flow authorization for EPS bearers, QCI mapping, modified QoS treatments and per-APN AMBR bandwidth rate enforcement.

As referenced in Figure 1 below, in an e-HRPD application the Gxa reference point is defined to transfer QoS policy information between the PCRF and Bearer Binding Event Reporting Function (BBERF) on the HSGW. In contrast with an S5/S8 GTP network model where the sole policy enforcement point resides on the PGW, the S2a model introduces the additional BBERF function to map EPS bearers to the main and auxiliary A10 connections. Gxa is sometimes referred to as an off-path signaling interface because no in-band procedure is defined to convey PCC rules via the PMIPv6 S2a reference interface. Gxa is a Diameter based policy signaling interface.

Gxa signaling is used for bearer binding and reporting of events. It provides control over the user plane traffic handling and encompasses the following functionality:

- Provisioning, update and removal of QoS rules from PCRF to BBERF.
- Bearer binding: Associates Policy Charging and Control (PCC) rules with default or dedicated EPS bearers. For a service data flow that is under QoS control, the Bearer Binding Function (BBF) within the HSGW ensures that the service data flow is carried over the bearer with the appropriate QoS service class.

- Bearer retention and teardown procedures
- Event reporting: Transmission of traffic plane events from BBERF to PCRF.
- Service data flow detection for tunneled and un-tunneled service data flows: The HSGW uses service data flow filters received from the PCRF for service data flow detection.
- QoS interworking/mapping between 3GPP QoS (QCI, GBR, MBR) and 3GPP2 ProfileID's

Intelligent Traffic Control

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

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

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

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

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

Network Operation Management Functions

This section describes the following features:

- A10A11
- Multiple PDN Support
- P-GW Selection (Discovery)
- PPP VSNCP
- Congestion Control
- IP Access Control Lists

A10/A11

Provides a lighter weight PPP network control protocol designed to reduce connection set-up latency for delay sensitive multimedia services. Also provides a mechanism to allow user devices in an evolved HRPD network to request one or more PDN connections to an external network.

The HRPD Serving Gateway connects the evolved HRPD access network with the Evolved Packet Core (EPC) as a trusted non-3GPP access network. In an e-HRPD network the A10'/A11' reference interfaces are functionally equivalent to the comparable HRPD interfaces. They are used for connection and bearer establishment procedures. In contrast to the conventional client-based mobility in an HRPD network, mobility management in the e-HRPD application is network based using Proxy Mobile IPv6 call anchoring between the MAG function on HSGW and LMA on PDN GW. Connections between the UE and HSGW are based on Simple IPv6. A11' signaling carries the IMSI based user identity.

The main A10' connection (SO59) carries PPP traffic including EAP-over-PPP for network authentication. The UE performs LCP negotiation with the HSGW over the main A10' connection. The interface between the e-PCF and HSGW uses GRE encapsulation for A10's. HDLC framing is used on the Main A10 and SO64 auxiliary A10's while SO67 A10 connections use packet based framing. After successful authentication, the HSGW retrieves the QoS profile from the 3GPP HSS and transfers this information via A11' signaling to the e-PCF.

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 HSGW 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 PDN 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 PDN GW LMA's. The PDN 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.

Performance: In the current release, each HSGW maintains a limit of up to three PDN connections per user session.

P-GW Selection (Discovery)

Supports the allocation of a P-GW used to provide PDN access to the subscriber. Subscriber information is used via the STa interface from the 3GPP AAA server, which receives subscriber information from the HSS.

The HSGW uses subscriber information provided by the 3GPP AAA server for P-GW selection. PDN subscription contexts provided by the 3GPP AAA server may contain:

1. the IP address of a P-GW

   If the 3GPP AAA server provides the IP address of a P-GW, no further P-GW selection functionality is performed.

2. the identity of a P-GW

   If the P-GW identity is a fully qualified domain name (FQDN) instead of an IP address, the P-GW address is derived by using the Domain Name Service (DNS) function.

3. the identity of an APN

   If only an APN is provided, an APN FQDN constructed for the APN is used to derive the P-GW address through the DNS function. If the DNS function provides a list of P-GW addresses, one P-GW address is selected from this list using the following criteria:

   - topology matching (if enabled)
   - P-GW priority (as configured in DNS records)

PPP VSNCP

VSNCP offers streamlined PPP signaling with fewer messages to reduce connection set-up latency for VoIP services (VORA). VSNCP also includes PDN connection request messages for signaling EPC attachments to external networks.

Vendor Specific Network Control Protocol (VSNCP) provides a PPP vendor protocol in accordance with IETF RFC 3772 that is designed for PDN establishment and is used to encapsulate user datagrams sent over the main A10' connection between the UE and HSGW. The UE uses the VSNCP signaling to request access to a PDN from the HSGW. It encodes one or more PDN-ID's to create multiple VSNCP instances within a PPP connection. Additionally, all PDN connection requests include the requested Access Point Name (APN), PDN Type (IPv4, IPv6 or IPv4/v6) and the PDN address. The UE can also include the Protocol Configuration Options (PCO) in the VSNCP signaling and the HSGW can encode this attribute with information such as primary/secondary DNS server or P-CSCF addresses in the Configuration Acknowledgement response message.

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 this 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
- Bulk Statistics Support
- Threshold Crossing Alerts (TCA) Support
- ANSI T1.276 Compliance

Management System

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 (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 Systems' 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.

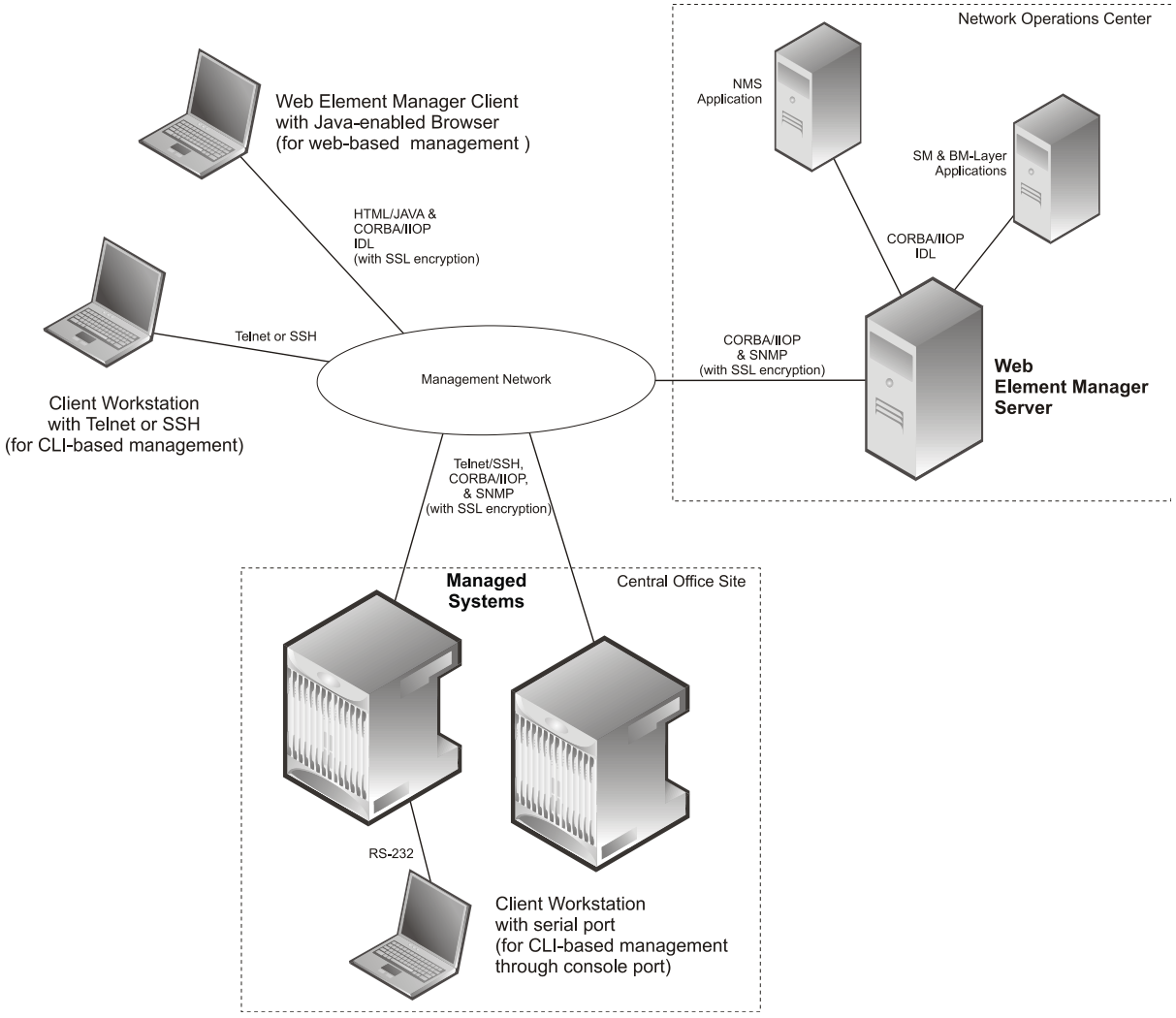
These include:

- 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 4. 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. For more information on command line interface based management, refer to the Command Line Interface Reference and P-GW Administration Guide.

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
- **Context**: Provides context-level statistics
- **IP Pool**: Provides IP pool statistics
- **MAG**: Provides Mobile Access Gateway statistics
- **ECS**: Provides Enhanced Charging Service statistics
- **RADIUS**: Provides AAA RADIUS 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 chassis 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, chassis host name, chassis 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 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 - External Application Support

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

- Web Element Management System

Web Element Management System

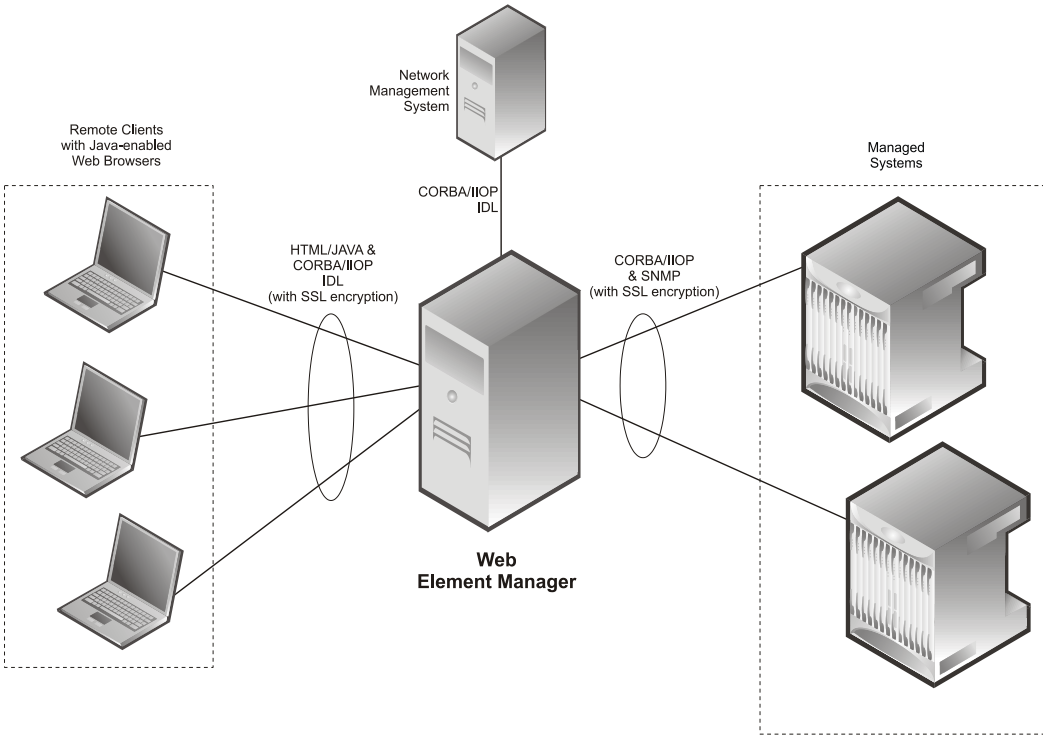
Provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management for the ASR 5000.

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 Web Element Manager and other network components.

Figure 5. Web Element Manager Network Interfaces



License Keys: A license key is required in order to use the Web Element Manager application. Please contact your local Sales or Support representative for more information.

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 S-GW service.

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

This section describes following features:

- IP Header Compression (RoHCv1 for IPv6)
- IP Security (IPSec)
- Traffic Policing and Shaping
- Layer 2 Traffic Management (VLANs)

IP Header Compression (RoHCv1 for IPv6)

Dynamic header compression contexts enable more efficient memory utilization by allocating and deleting header compression contexts based on the presence/absence of traffic flowing over an S067 A10 bearer connection.

In order to provision VoIP services over an e-HRPD network the StarOS 9.0 release adds support for ROHC compression contexts over IPv6 datagrams using the RTP profile over S067 auxiliary A10' connections. The e-HRPD application uses pre-established SO67 A10' connections for VoIP bearers. A header compression context is allocated for the first time when a new SO67 A10' connection request comes with negotiated ROHC parameters.

In order to optimize memory allocation and system performance, the HSGW uses configured inactivity time of traffic over the bearer to dynamically determine when the ROHC compression context should be removed. This feature is also useful for preserving compression contexts on intra-HSGW call hand-offs. The dynamic header compression context parameters are configured in the ROHC profile that is associated with the subscriber session.

Important: For more information on IP header compression support, refer IP Header Compression chapter in System Enhanced Feature Configuration Guide.

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)

- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)

In order to provision VoIP services over an e-HRPD network the StarOS 9.0 release adds support for ROHC compression contexts over IPv6 datagrams using the RTP profile over S067 auxiliary A10' connections. The e-HRPD application uses pre-established SO67 A10' connections for VoIP bearers. A header compression context is allocated for the first time when a new SO67 A10' connection request comes with negotiated ROHC parameters.

In order to optimize memory allocation and system performance, the HSGW uses configured inactivity time of traffic over the bearer to dynamically determine when the ROHC compression context should be removed. This feature is also useful for preserving compression contexts on intra-HSGW call hand-offs. The dynamic header compression context parameters are configured in the ROHC profile that is associated with the subscriber session.

Important: For more information on IP header compression support, refer IP Header Compression chapter in 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.

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. For IPv4, IKEv1 is used and for IPv6, IKEv2 is supported. IPSec can be implemented on the system for the following applications:

- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.

Important: Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

Important: For more information on IPSec support, refer to the IP Security chapter in the System Enhanced Feature Configuration Guide.

Call/Session Procedure Flows

This section provides information on the function of the HSGW in an eHRPD network and presents call procedure flows for different stages of session setup.

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 6. Initial Attach with IPv6/IPv4 Access Call Flow

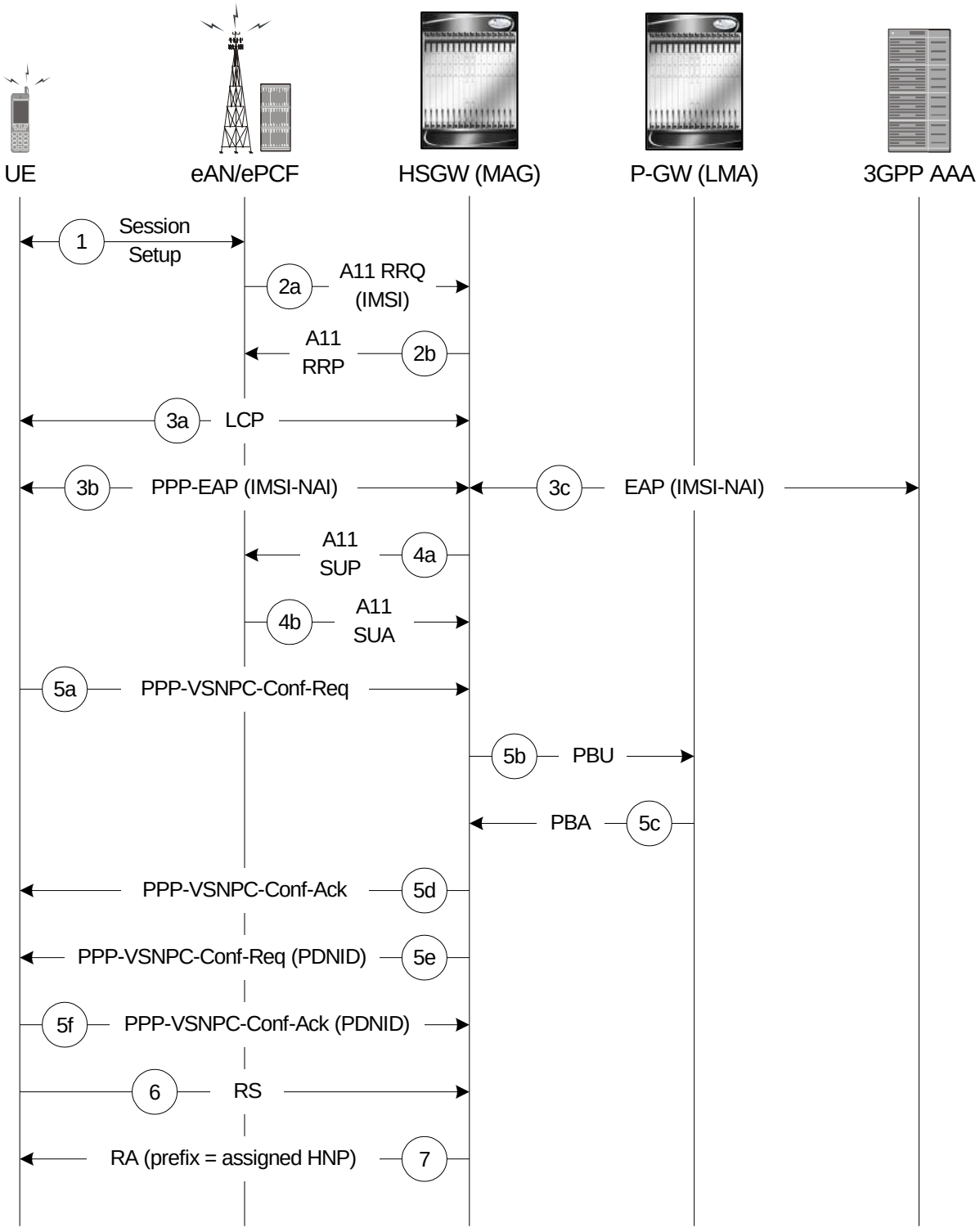


Table 2. Initial Attach with IPv6/IPv4 Access Call Flow Description

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 7. PMIPv6 Lifetime Extension (without handover) Call Flow

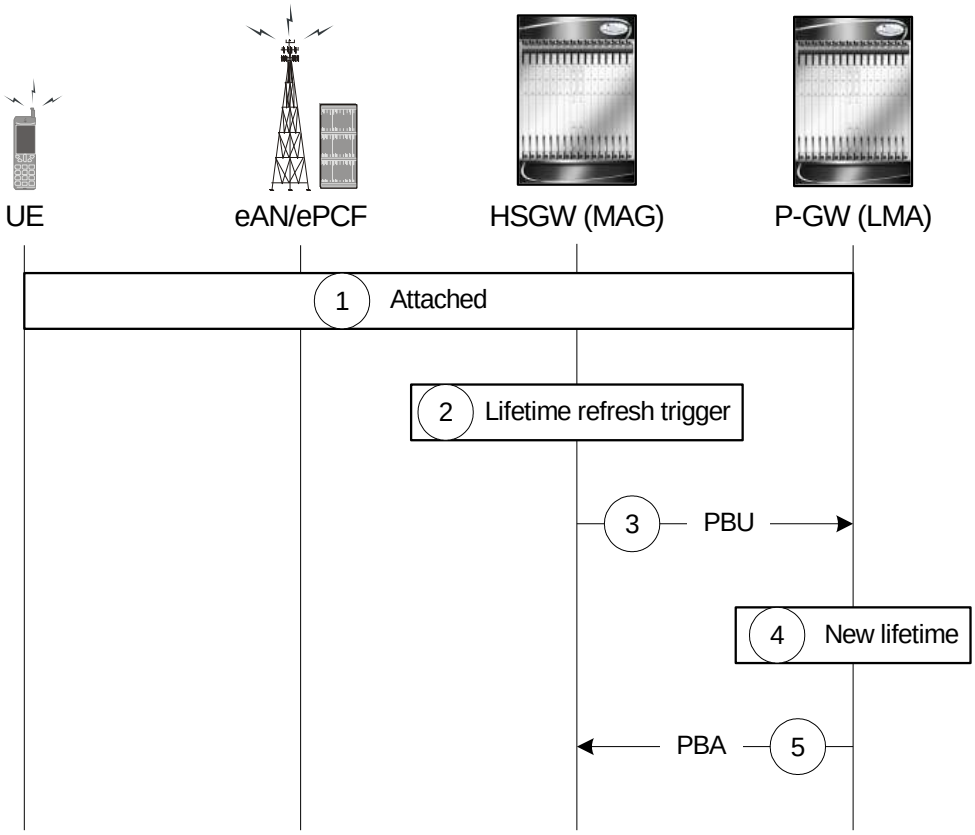


Table 3. PMIPv6 Lifetime Extension (without handover) Call Flow Description

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 8. PDN Connection Release by the UE Call Flow

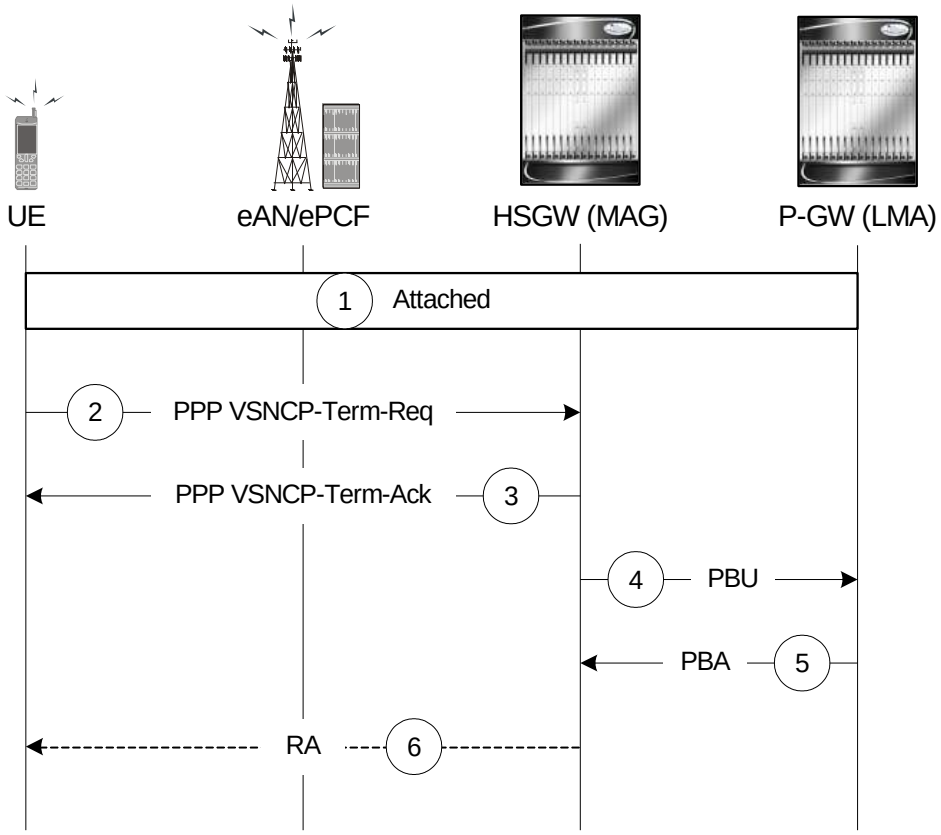


Table 4. PDN Connection Release by the UE Call Flow Description

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 9. PDN Connection Release by the HSGW Call Flow

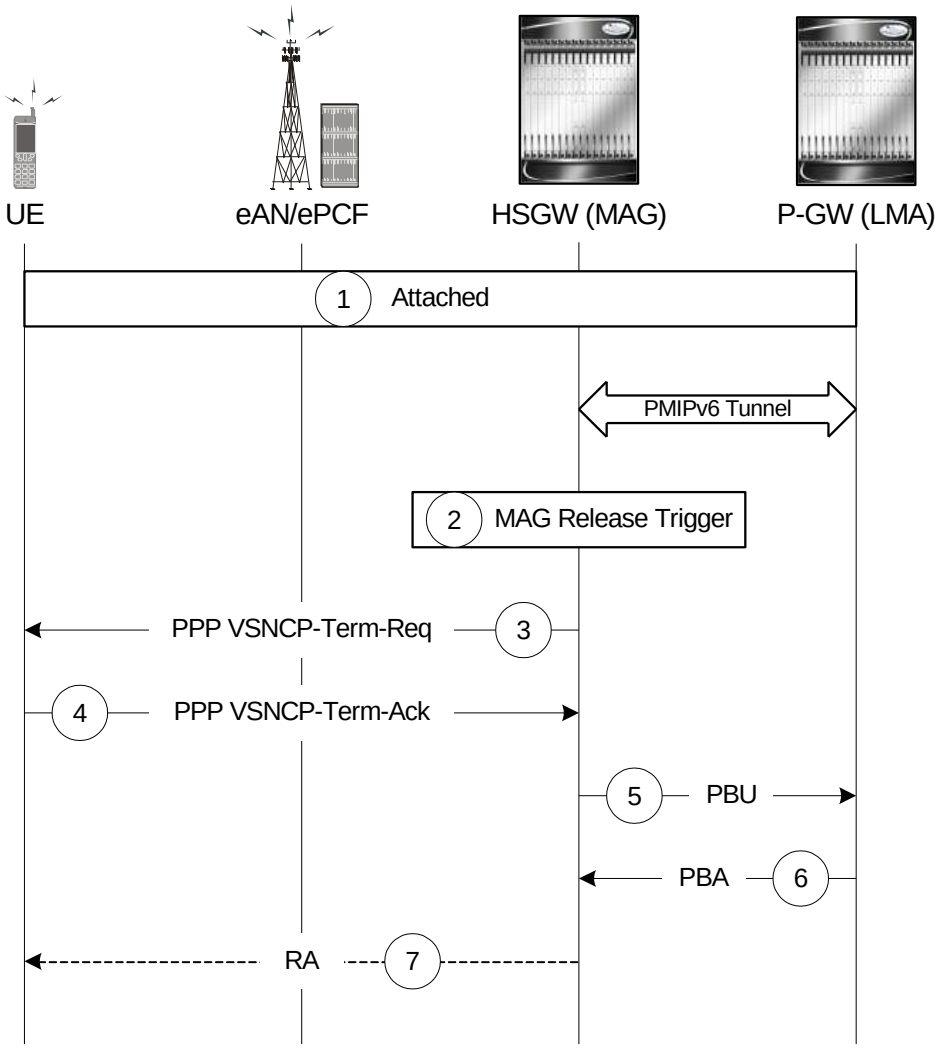


Table 5. PDN Connection Release by the HSGW Call Flow Description

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.
3	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.

Step	Description
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 10. PDN Connection Release by the HSGW Call Flow

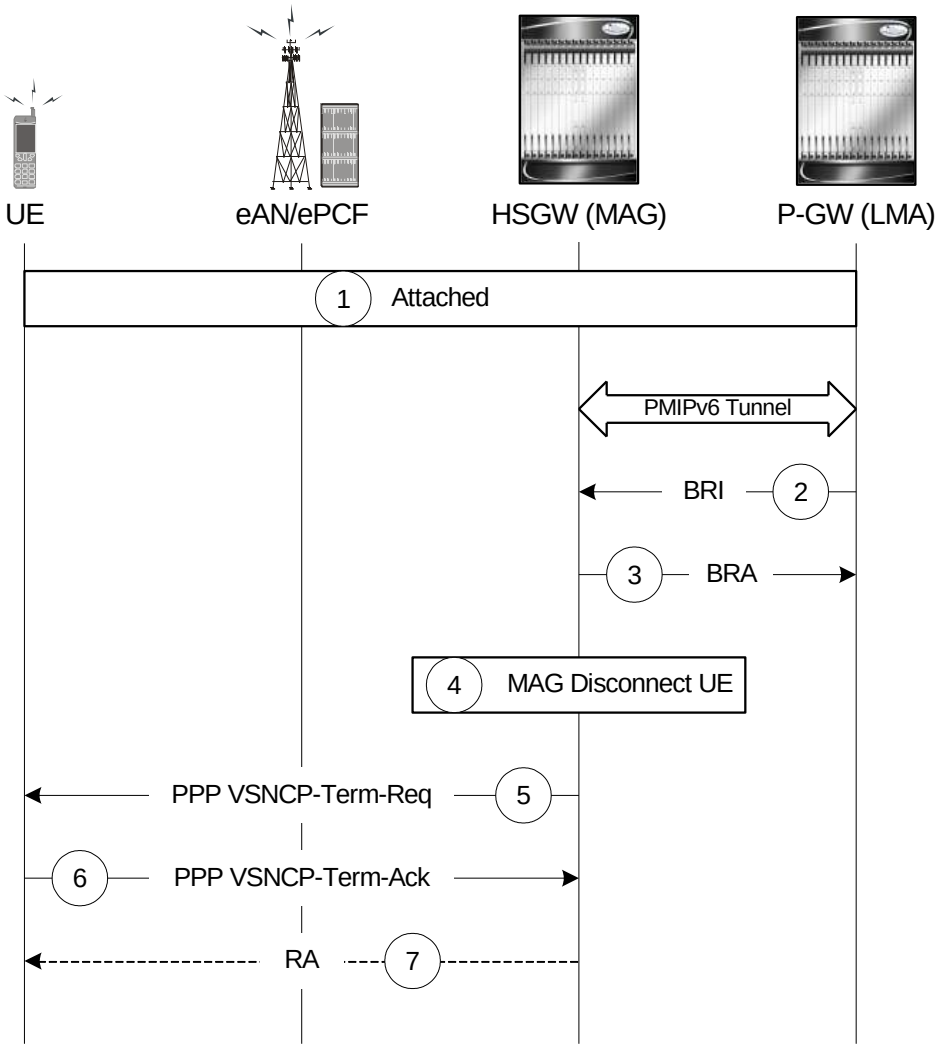


Table 6. PDN Connection Release by the HSGW Call Flow Description

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.
6	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).

Step	Description
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

Supported Standards

The HSGW complies with the following standards.

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

3GPP References

- 3GPP TR 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402 Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.273 Evolved Packet System (EPS);3GPP EPS AAA interfaces
- 3GPP TS 29.275 Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 32.299 Rf Offline Accounting Interface

3GPP2 References

- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects
- X.S0057-0 v1.0: “E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects”
- A.S0008-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, August 2007. (HRPD IOS)
- A.S0009-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function, August 2007. (HRPD IOS)
- A.S0022-0 v1.0: E-UTRAN - HRPD Connectivity and Interworking: Access Network Aspects (E-UTRAN – HRPD IOS), March 2009.
- A.S0017-D v1.0: Interoperability Specification (IOS) for cdma2000 Access Network Interfaces - Part 7 (A10 and A11 Interfaces), June, 2007.
- X.S0011-D v1.0: cdma2000 Wireless IP Network Standard, March 2006.

IETF References

- RFC 1661 (July 1994): The Point-to-Point Protocol (PPP)
- RFC 2205 (September 1997): Resource Reservation Protocol (RSVP)
- RFC 2473 (December 1998): Generic Packet Tunneling in IPv6 Specification
- RFC 3095 (July 2001): RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed
- RFC 3748 (June 2004): Extensible Authentication Protocol (EAP)
- RFC 3772 (May 2004): PPP Vendor Protocol
- RFC 3775 (June 2004): Mobility Support in IPv6
- RFC 4283 (November 2005): Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 5094 (February 2008): Service Selection for Mobile IPv6
- RFC 5149 (December 2007): Mobile IPv6 Vendor Specific Option
- RFC 5213 (August 2008): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-09.txt): IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-grekey-option-06.txt): GRE Key Option for Proxy Mobile IPv6
- Internet-Draft (draft-meghana-netlmm-pmipv6-mipv4-00): Proxy Mobile IPv6 and Mobile IPv4 interworking
- Internet-Draft (draft-ietf-mip6-nemo-v4traversal-06.txt): Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft arkko-eap-aka-kdf): Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- Internet-Draft (draft-muhanna-mext-binding-revocation-01): Binding Revocation for IPv6 Mobility

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

Chapter 2
HSGW Configuration

This chapter provides configuration information for the HRPD Serving Gateway (HSGW).

Important: Information about all commands in this chapter can be found in the ST-series Multimedia Core Platforms 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 HSGW product are located in the ST-series Multimedia Core Platforms Command Line Interface Reference.

The following information is provided in this chapter:

- Configuring the System to Perform as a Standalone HSGW

Configuring the System to Perform as a Standalone HSGW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an HSGW in a test environment. For a more robust configuration example, refer to the Sample Configuration Files appendix. Information provided in this section includes the following:

- Information Required
- How This Configuration Works
- Configuration

Information Required

The following sections describe the minimum amount of information required to configure and make the HSGW 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 HSGW 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 HSGW.

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface.Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.

Required Information	Description
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

Required HSGW Context Configuration Information

The following table lists the information that is required to configure the HSGW context on an HSGW.

Required Information	Description
HSGW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the HSGW context is recognized by the system.
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication.
Diameter endpoint name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Diameter endpoint is recognized by the system.The Diameter endpoint name identifies the configuration used to communicate with the 3GPP AAA server in the AAA context.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy is recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
A10/A11 Interface Configuration (To/from eAN/ePCF)	
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 management interface(s) to a specific network.
HSGW Service Configuration	
HSGW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HSGW service is recognized by the system.Multiple names are needed if multiple HSGW services will be used.

Required Information	Description
Security Parameter Index Remote Address	**eAN/ePCF IP address:**Specifies the IP address of the eAN/ePCF. The HSGW service allows the creation of a security profile associated with a particular eAN/ePCF.
	SPI number: Specifies the SPI (number) which indicates a security context between the eAN/ePCF and the HSGW.
	Encrypted secret: Configures the shared-secret between the HSGW service and the eAN/ePCF. This command can also be non-encrypted.

Required MAG Context Configuration Information

The following table lists the information that is required to configure the MAG context on an HSGW.

Required Information	Description
MAG context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the MAG context is recognized by the system.
S2a Interface Configuration (To/from P-GW LMA)	
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 address 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.
MAG Service Configuration	
MAG Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the MAG service is recognized by the system.

Required AAA Context Configuration Information

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

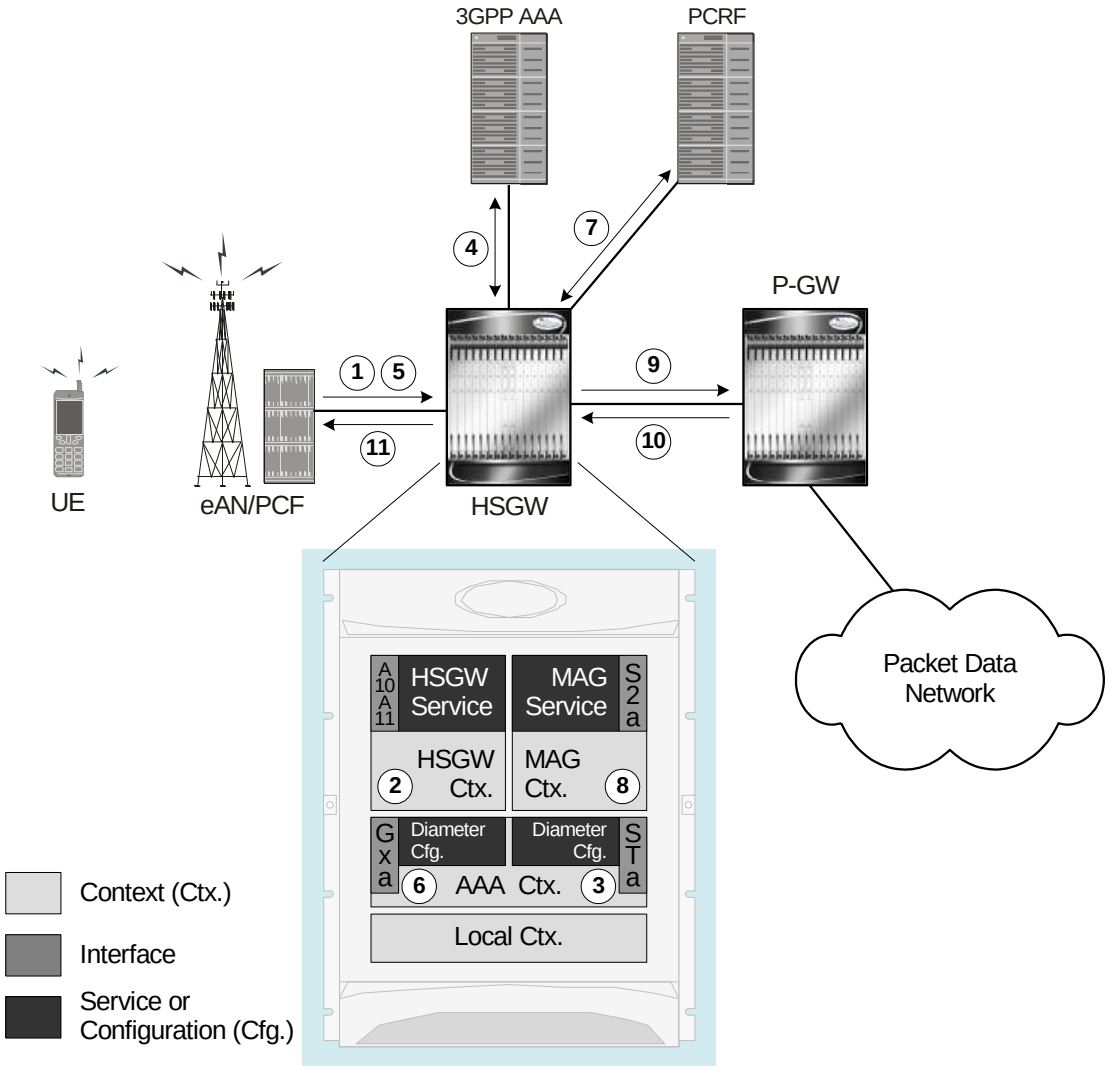
Required Information	Description
Gxa Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	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.
Gxa Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gxa 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 Gxa origin host is recognized by the system.
Origin host address	The IPv6 address of the Gxa interface.
Peer name	The Gxa endpoint name described above.
Peer realm name	The Gxa origin realm name described above.
Peer address and port number	The IPv6 address and port number of the PCRF.
Route-entry peer	The Gxa endpoint name described above.
STa 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 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.
STa Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the STa 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 STa origin host is recognized by the system.

Required Information	Description
Origin host address	The IPv6 address of the STa interface.
Peer name	The STa endpoint name described above.
Peer realm name	The STa origin realm name described above.
Peer address and port number	The IPv6 address and port number of the PCRF.
Route-entry peer	The STa 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 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.
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 IPv6 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 IPv6 address and port number of the PCRF.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a PMIP call originating in the eHRPD network.



Step 1 A subscriber session from the eAN/PCF is received by the HSGW service over the A10/A11 interface.

Step 2 The HSGW 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.

Step 3 The AAA group is configured with the Diameter endpoint for the STa interface to the AAA server which is used to authenticate and authorize the subscriber and session.

Step 4 The system completes the Diameter EAP interactions with the AAA server and receives the subscriber profile on successful authentication. The subscriber profile contains Access Point Name (APN) profiles that include APNs the subscriber is authorized to connect to and the P-GW identity/FQDN that serves the APN.

Step 5 Upon successful authentication, the UE begins establishment of PDN connection by sending a Vendor Specific Network Control Protocol (VSNCP) configuration request including the APN and the IP version capability of the UE.

Step 6 The HSGW uses the configured Gxa Diameter endpoint under the IMS Auth service to establish the gateway control session for this PDN.

Step 7 As part of the gateway control session establishment, the HSGW sends a CC-Request (CCR) message to the PCRF and the PCRF acknowledges establishment by responding back with CC-Answer (CCA) message.

Step 8 HSGW uses the configured MAG context to determine the MAG service to use for the outgoing S2a connection.

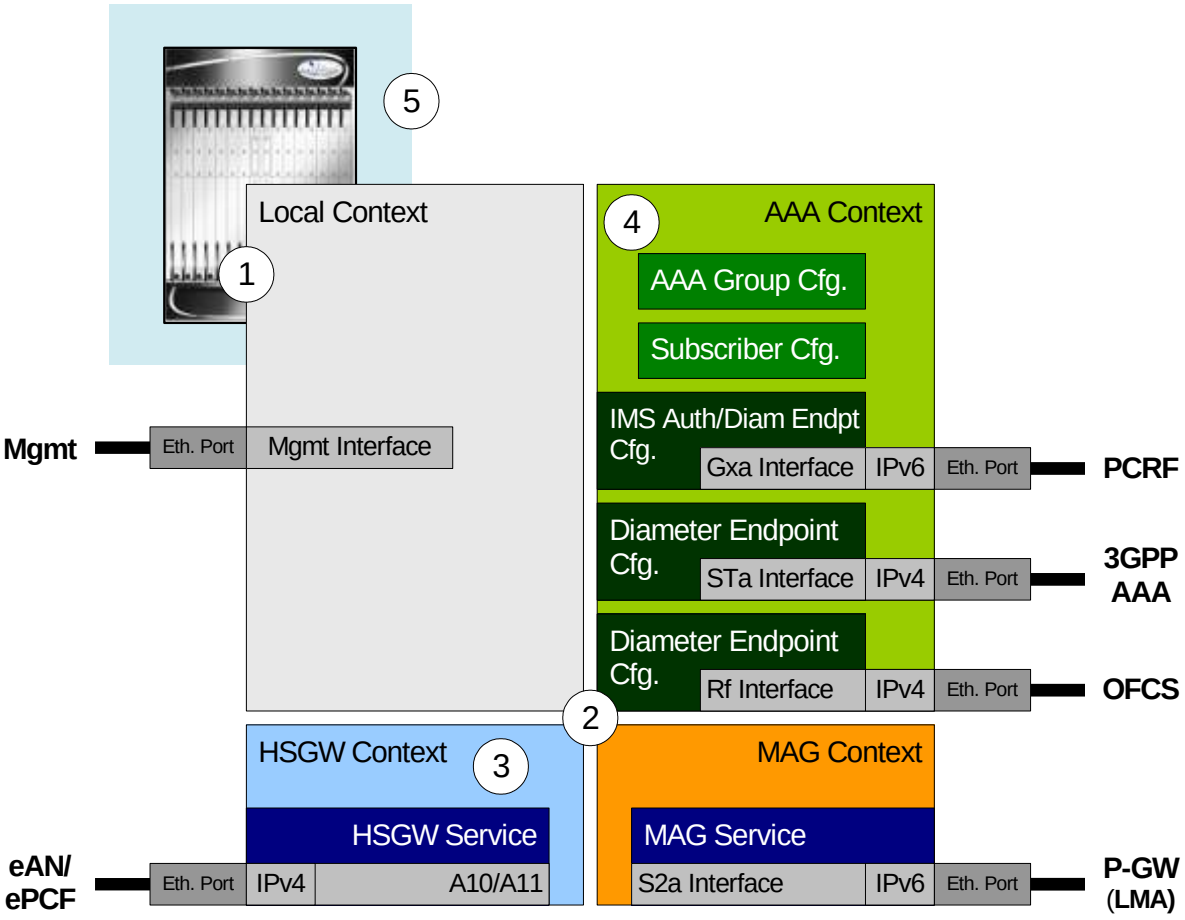
Step 9 The HSGW establishes the S2a connection by sending a PMIP Proxy Binding Update (PBU) to the P-GW including the NAI and APN. The PBU also includes the home network prefix and/or IPv4 home address option based on the subscriber's APN profile and UE IP version capability.

Step 10 The P-GW responds with a Proxy Binding Acknowledgement (PBA) that includes the assigned IPv6 home network prefix and interface identifier and/or IPv4 home address acknowledgement option based on the PBU.

Step 11 The HSGW conveys the assigned IP information to the UE in a VSNCP configuration acknowledgement message. Additionally, if an IPv6 address is assign to the UE, the HSGW sends a router advertisement message to the UE including the assigned home network prefix.

Configuration

To configure the system to perform as a standalone HSGW 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 an HSGW and set basic parameters such as interfaces and an IP route by applying the example configurations presented in the HSGW and MAG Service Configuration section.

Step 4 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in the AAA and Policy Configuration section.

Step 5 Optionally configure a Robust Header Compression (RoHC) profile by following the steps found in the Optional Header Compression Configuration section.

Step 6 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 HSGW service will reside by applying the example configuration in the Creating and Configuring an HSGW Context section.

Step 3 Specify static IP routes to the eAN/ePCF and/or PDN gateway by applying the example configuration in the Configuring Static IP Routes section.

Step 4 Create an HSGW service within the newly created HSGW context by applying the example configuration in the Creating an HSGW Service section.

Step 5 Create the context where the MAG service will reside by applying the example configuration in the Creating and Configuring MAG Context section.

Step 6 Create a MAG service within the newly created MAG context by applying the example configuration in the Creating a MAG Service 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 <server-type>
```

```
            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
```

Notes:

- This configuration is provided as a sample for a configuration file. It is the same configuration that is provided in the "Using the CLI for Initial Configuration" procedure in the Getting Started chapter of the System Administration Guide.
- Remote access is configured using the command as shown in the local context above. Multiple server types are available. For more information on remote access server types, refer to the Configuring the System for Remote Access section in the Getting Started chapter of the System Administration Guide and the Context Configuration Mode Commands chapter in the Command Line Interface Reference.

Creating and Configuring an HSGW Context

Use the following example to create an HSGW context and Ethernet interfaces, and bind the interfaces to configured Ethernet ports. The interfaces created in this configuration support the A10/A11 connection to the eAN/ePCF and the connection to the P-GW.

```
configure
   context <hsgw_context_name> -noconfirm
      interface <a10-a11_interface_name>
         ip address <ipv4_address>
         exit
      policy accounting <rf_acct_policy_name> -noconfirm
         accounting-level {type}
         operator-string <string>
         exit
```

```
ip domain-lookup

ip name-servers <ipv4_or_ipv6_address>

dns-client <name>

port ethernet <slot_number/port_number>

   no shutdown

   bind interface <a10-a11_interface_name> <hsgw_context_name>

   end
```

Notes:

- The HSGW-to-ePCF (A10/A11) interface must be an IPv4 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types supported by the HSGW are: 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.
- The **ip domain-lookup**, **ip name-servers**, and **dns-client** commands are used during P-GW FQDN discovery.

Configuring Static IP Routes

Use the following example to configure static IP routes for data traffic between the HSGW and the eAN/ePCF and/or P-GW:

```
configure

   context <hsgw_context_name>

      ip route <addr/mask> next-hop <epcf_addr> <hsgw_epcf_intrfc_name>

      ipv6 route <ipv6_addr/prefix> next-hop <pgw_addr> interface
<s2a_intrfc_name>

      end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

Creating an HSGW Service

Use the following configuration example to create the HSGW service:

```
configure

   context <hsgw_context_name> -noconfirm

      hsgw-service <hsgw_service_name> -noconfirm

         end
```

Creating and Configuring MAG Context

Use the following example to create a MAG context and Ethernet interface, and bind the interface to configured Ethernet ports. The interface created in this configuration supports the S2a connection to the P-GW.

```
configure
   context <mag_context_name> -noconfirm
      interface <s2a_interface_name>
         ip address <ipv6_address>
         exit
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <s2a_interface_name> <mag_context_name>
      end
```

Notes:

- The HSGW-to-PGW (S2a) interface must be an IPv6 address.

Creating a MAG Service

Use the following configuration example to create the MAG service:

```
configure
   context <mag_context_name> -noconfirm
      mag-service <mag_service_name> -noconfirm
         end
```

Notes:

- A separate MAG context with a MAG service can be created to segregate the HSGW network from the MAG network. Refer to the Configuring the HSGW Service section for additional information on using a MAG service in a separate context.

HSGW and MAG Service Configuration

Step 1 Configure HSGW service settings by applying the example configuration in the Configuring the HSGW Service section.

Step 2 Configure the MAG service by applying the example configuration in the Configuring the MAG Service section.

Configuring the HSGW Service

Use the following configuration example to set parameters including binding the HSGW-eAN/ePCF interface to this service and configuring the SPI between the HSGW and eAN/ePCF:

```
configure

   context <hsgw_context_name> -noconfirm

      hsgw-service <hsgw_service_name> -noconfirm

         mobile-access-gateway context <mag_context_name> mag-service
<mag_service_name>

         associate accounting-policy <rf_name>

         spi remote-address <epcf_address> spi-number <num> encrypted secret
<secret>

         plmn id mcc <number> mnc <number>

         fqdn <domain_name>

         gre sequence-mode recorder

         gre flow-control action resume-session timeout <msecs>

         gre segmentation

         unauthorized-flows qos-update wait-timeout <seconds>

         ip header-compression rohc

         bind address <a10-a11_interface_address>

         end
```

Notes:

- The accounting policy is configured in the HSGW context using the **policy accounting** command. This is the pointer to the accounting policy configuration for the Rf (off-line charging) interface. Refer to Creating and Configuring an HSGW Context for more information.
- The **plmn id** command configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.

- The Fully Qualified Domain Name (FQDN) command is used to identify the HSGW to a P-GW during HSGW selection. The FQDN is included in an APN on the P-GW.
- The **gre** commands are used to configure Generic Routing Encapsulation (GRE) parameters for the A10 protocol.
- The **dns-pgw context** command can be used if the DNS client is configured in a different context from the HSGW service.
- The IP header compression command is optional and enables, in this service, the RoHC profile configuration created in the Global Configuration Mode. Refer to the Optional Header Compression Configuration section for more information.
- The address used in the binding entry must be the IP address configured as the HSGW-to-ePCF A10/A11 interface in the Creating and Configuring an HSGW Context section.
- The HSGW defaults to a MAG service configured in the same context unless the mobile-access-gateway context *<mag_context_name>* mag-service *<name>* command is used as defined above.

Configuring the MAG Service

Use the following example to configure the MAG service:

```
configure
   context <mag_context_name> -noconfirm
      mag-servics <mag_service_name> -noconfirm
         information-element-set custom1
         bind address <s2a_interface_address>
         end
```

Notes:

- The information element set is used to identify mobility options sent in PBUs from the MAG to the LMA. “custom1” is custom set of option specific to a Starent customer. The default setting is “standard”.
- The address used in the binding entry must be the IP address configured as the HSGW-to-PGW S2a interface in the Creating and Configuring an HSGW Context section.

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 Configure the default subscriber for the AAA context by applying the example configuration in the Modifying the Default Subscriber section.

Step 3 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 and a AAA server and PCRF:

```
configure
   context <aaa_context_name> -noconfirm
      interface <aaa_sta_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <pcrf_gxa_ipv6_interface_name>
         ip address <ipv6_address>
         exit
      interface <ocs_rf_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      subscriber default
         exit
      aaa group default
         diameter accounting endpoint <rf_ofcs_server>
         diameter authentication endpoint <sta_cfg_name>
         diameter accounting server <rf_ofcs_server> priority <num>
         diameter authentication server <3gpp_aaa_server> priority <num>
         exit
      ims-auth-service <gxa_ims_service_name>
         policy-control
            diameter origin endpoint <gxa_cfg_name>
            diameter dictionary <gxa_dictionry_name>
            diameter host-select table <#> algorithm round-robin
```

```
            diameter host-select row-precedence <#> table <#> host
<gxa_cfg_name>
            exit
         exit
      aaa group default
         diameter authentication dictionary <name>
         diameter authentication endpoint <sta_cfg_name>
         diameter authentication server <sta_cfg_name> priority <#>
         exit
      diameter endpoint <sta_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv4_address>
         peer <sta_cfg_name> realm <name> address <aaa_ipv4_address>
         route-entry peer <sta_cfg_name>
         exit
      diameter endpoint <gxa_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv6_address>
         peer <gxa_cfg_name> realm <name> address <pcrf_ip_addr> port <#>
         route-entry peer <gxa_cfg_name>
         end
      diameter endpoint <rf_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv4_address>
         peer <rf_cfg_name> realm <name> address <ocs_ip_addr> port <#>
         route-entry peer <rf_cfg_name>
         end
```

Modifying the Default Subscriber

Use the following example to modify the default subscriber configuration in the AAA context:

```
configure
   context <aaa_context_name> -noconfirm
      subscriber default
         ims-auth-service <gxa_ims_service_name>
         rohc-profile-name <name>
         end
```

Notes:

- The IMS Auth Service is also crested and configured in the AAA context.
- A RoHC profile name is optional and dependant on if RoHC is being configured for this HSGW. RoHC profiles are configured through the Global Configuration Mode. Refer to the Optional Header Compression Configuration section for the RoHC profile configuration and the Command Line Interface Reference for detailed information about RoHC profile commands.

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 configuration example shown above 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.

Optional Header Compression Configuration

Use the following example to configure a Robust Header Compression profile:

```
configure
   rohc-profile profile-name <name>
      common-options
         delay-release-hc-context-timer <seconds>
         inactive-traffic-release-hc-context-timer <seconds>
```

Verifying and Saving the Configuration

Refer to the Verifying and Saving Your Configuration chapter to verify and save your HSGW 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 Guide for a detailed listing of these traps.

Monitoring System Status and Performance

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

To do this:	Enter this command:
View Congestion-Control Information	
View Congestion-Control Statistics	
View Congestion-Control Statistics	**show congestion-control statistics { a11mgr | ipsecmgr }**
View Subscriber Information	
Display Session Resource Status	
View session resource status	**show resources session**
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**
View Statistics for Subscribers using HSGW Services on the System	
View statistics for subscribers using any HSGW service on the system	**show subscribers hsgw-only full**
View statistics for subscribers using a specific HSGW service on the system	**show subscribers hsgw-service** *service_name*
View Statistics for Subscribers using MAG Services on the System	
View statistics for subscribers using any MAG service on the system	**show subscribers mag-only full**
View statistics for subscribers using a specific MAG service on the system	**show subscribers mag-service** *service_name*
View Session Subsystem and Task Information	
Display Session Subsystem and Task StatisticsRefer 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**

To do this:	Enter this command:
View Session Manager statistics	**show session subsystem facility sessmgr all**
View MAG Manager statistics	**show session subsystem facility magmgr all**
View Session Recovery Information	
View session recovery status	**show session recovery status [verbose]**
View Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View HSGW Service Information	
View HSGW service statistics	**show hsgw-service statistics all**
View MAG Service Information	
View MAG service statistics for a specific service	**show mag-service statistics name** *service_name*
View Robust Header Compression Information	
View RoHC statistics	**show rohc statistics**
View QoS/QCI Information	
View RAN Profile ID to QoS Class Index mapping tables	**show profile-id-qci-mapping table all**
View QoS Class Index to QoS mapping tables	**show qci-qos-mapping table all**

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 Command Line Reference for detailed information on using this command.

Appendix A
HSGW Engineering Rules

This appendix provides HRPD Serving Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ST40 Intelligent Mobile Gateway for your network deployment. General and network-specific rules are located in the appendix of the System Administration Guide for the specific network type.

The following rules are covered in this appendix:

- Interface and Port Rules
- HSGW Service Rules
- HSGW 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.

A10/A11 Interface Rules

The following engineering rules apply to the A10/A11 interface:

- An A10/A11 interface is created once the IP address of a logical interface is bound to an HSGW service.
- The logical interface(s) that will be used to facilitate the A10/A11 interface(s) must be configured within an "ingress" context.
- HSGW services must be configured within an "ingress" context.
- At least one HSGW service must be bound to each interface; however, multiple HSGW services can be bound to a single interface if secondary addresses are assigned to the interface.
- Each HSGW service must be configured with the Security Parameter Index (SPI) of the Evolved Packet Control Function (ePCF) that it will be communicating with over the A10/A11 interface.
- Multiple SPIs can be configured within the HSGW service to allow communications with multiple ePCFs over the A10/A11 interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the A10/A11 interface can be limited.

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.

MAG to LMA Rules

The following engineering rules apply to the S2a interface from the MAG service to the LMA service residing on the P-GW:

- An S2a interface is created once the IP address of a logical interface is bound to an MAG service.
- The logical interface(s) that will be used to facilitate the S2a interface(s) must be configured within the egress context.
- MAG services must be configured within the egress context.

- MAG services must be associated with an HSGW service.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S2a interface can be limited.

HSGW 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.

- Up to 2,048 Security Parameter Indices (SPIs) can be configured for a single HSGW service.
- Up to 2,048 MAG-LMA SPIs can be supported for a single HSGW service.
- The system maintains statistics for a maximum of 4096 peer LMAs per MAG service.
- The total number of entries per table and per chassis is limited to 256.
- Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty troubleshooting problems, and make it difficulty understanding outputs of show commands.

HSGW Subscriber Rules

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

- A maximum of 2,048 local subscribers can be configured per context.
- Default subscriber templates may be configured on a per HSGW or MAG service.

Appendix B
Sample Configuration Files

This appendix contains sample configuration files for the HSGW. The following configurations are supported:

- Standalone eHRPD Serving Gateway

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

Standalone eHRPD Serving Gateway

The configuration sample contained in this section contains example configurations described in the System Administration Guide and the eHRPD Serving Gateway Administration Guide. Descriptions of all commands contained herein can be found in the Command Line Interface Reference.

Configuration Sample

```
# Configuration file for ST40 in HSGW role
#
# Send HSGW licenses
configure /flash/flashconfig/<hsgw_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 ST40 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 10.2.10.2
       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>
    rohc-profile profile-name <name>
       common-options
          delay-release-hc-context-timer <seconds>
          inactive-traffic-release-hc-context-timer <seconds>
          exit
       exit
# HSGW context
    context <hsgw_context_name>
       interface <a10-a11_interface_name>
          ip address <ip_address>
          exit
       ip domain-lookup
       ip name-servers <ipv4_or_ipv6_address>
       dns-client <name>
       policy accounting <rf_acct_policy_name>
          accounting-level {type}
          operator-string <string>
```

```
            exit
         hsgw-service <hsgw_service_name>
            associate accounting-policy <acct_policy_name>
            spi remote-address <ip_address> spi-number <num> encrypted secret
<secret>
            plmn id mcc <number> mnc <number>
            fqdn <domain_name>
            gre sequence-mode recorder
            gre flow-control action resume-session timeout <msecs>
            gre segmentation
            unauthorized-flows qos-update wait-timeout <seconds>
            ip header-compression rohc
            bind address <a10-a11_interface_address>
            exit
         exit
# MAG context
   context <hsgw_context_name>
      interface <s2a_interface_name>
         ip address <ipv6_address>
         exit
      mag-servics <mag_service_name> -noconfirm
         information-element-set custom1
         bind address <s2a_interface_address>
         exit
      exit
# AAA and policy
   context <aaa_context_name>
      interface <aaa_sta_ipv4_interface_name>
         ip address <ipv4_address>
```

```
      exit
    interface <pcrf_gxa_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    interface <ocs_rf_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    subscriber default
    ims-auth-service <gxa_ims_service_name>
    rohc-profile-name <name>
      exit
    aaa group default
      radius accounting interim interval <seconds>
      diameter accounting dictionary <name>
      diameter authentication dictionary <name>
      diameter accounting endpoint <rf_ofcs_server>
      diameter authentication endpoint <sta_cfg_name>
      diameter accounting server <rf_ofcs_server> priority <num>
      diameter authentication server <sta_cfg_name> priority <num>
      exit
    ims-auth-service <gxa_ims_service_name>
      policy-control
        diameter origin endpoint <gxa_cfg_name>
        diameter dictionary <gxa_dictionry_name>
        diameter host-select table <#> algorithm round-robin
        diameter host-select row-precedence <#> table <#> host
<gxa_cfg_name>
        exit
      exit
```

```
      diameter endpoint <sta_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv4_address>
         peer <sta_cfg_name> realm <name> address <aaa_ipv4_address>
         route-entry peer <sta_cfg_name>
         exit
      diameter endpoint <gxa_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv6_address>
         peer <gxa_cfg_name> realm <name> address <pcrf_ip_addr> port <#>
         route-entry peer <gxa_cfg_name>
         end
      diameter endpoint <rf_cfg_name>
         origin realm <realm_name>
         origin host <name> address <aaa_ctx_ipv4_address>
         peer <rf_cfg_name> realm <name> address <ocs_ip_addr> port <#>
         route-entry peer <rf_cfg_name>
         exit
      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
```