HSGW Administration Guide, StarOS Release 21.16

First Published: 2019-11-15

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

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 2

CHAPTER 3

CHAPTER 4

About this Guide

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

HRPD Serving Gateway (HSGW) is a StarOS application that runs on Cisco ASR 5500. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	**Description**
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	**Description**
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.

Typeface Conventions	Description
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Supported Documents and Resources

Related Common Documentation

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

The following common documents are available:

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

Related Product Documentation

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

- *MME Administration Guide*
- *P-GW Administration Guide*
- *SAEGW Administration Guide*
- *S-GW Administration Guide*

Obtaining Documentation

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

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

Contacting Customer Support

Use the information in this section to contact customer support.

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

CHAPTER 1

HRPD Serving Gateway Overview

Cisco® HRPD Serving Gateway (HSGW) provides wireless carriers with a flexible solution in 3GPP2 evolved High Rate Packet Data (eHRPD) wireless data networks.

This overview provides general information about the HSGW including:

Product Description

The HSGW terminates the HRPD access network interface from the Evolved Access Network/Evolved Packet Core Function (eAN/ePCF) and routes UE-originated or terminated packet data traffic.

The HSGW functionality provides interworking of the AT with the 3GPP Evolved Packet System (EPS) architecture and protocols specified in 3GPP 23.402 (mobility, policy control (PCC), and roaming). It supports efficient (seamless) inter-technology mobility between Long Term Evolution (LTE) and HRPD with the following requirements:

- Sub 300ms bearer interruption
- Inter-technology handoff between 3GPP Enhanced UMTS Terrestrial Radio Access Network (E-UTRAN) and HRPD
- Intra-technology handoff between an HSGW and an existing PDSN
- Support for inter-HSGW fast handoff via Proxy Mobile IPv6 (PMIPv6) Binding Update

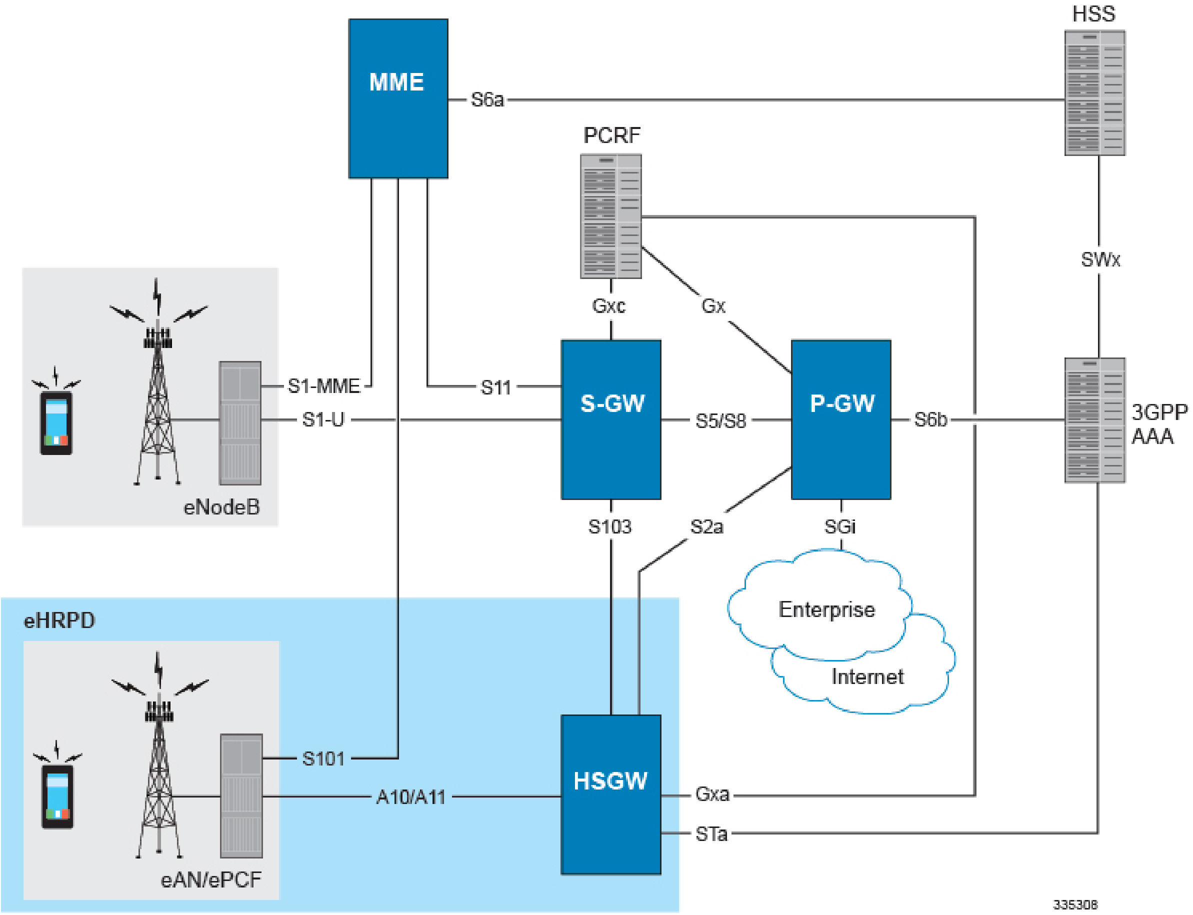
The HSGW provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE (4G System Architecture Evolution) core network and performs the following functions:

- 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
- 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 Features and Functionality - Base Software, on page 9 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:

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

For more information on QoS features, refer to the Features and Functionality - Base Software, on page 9 in this overview.

AAA, Policy and Charging

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

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

For more information on policy and charging features, refer to the Features and Functionality - Base Software, on page 9 in this overview.

Platform Requirements

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

Licenses

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

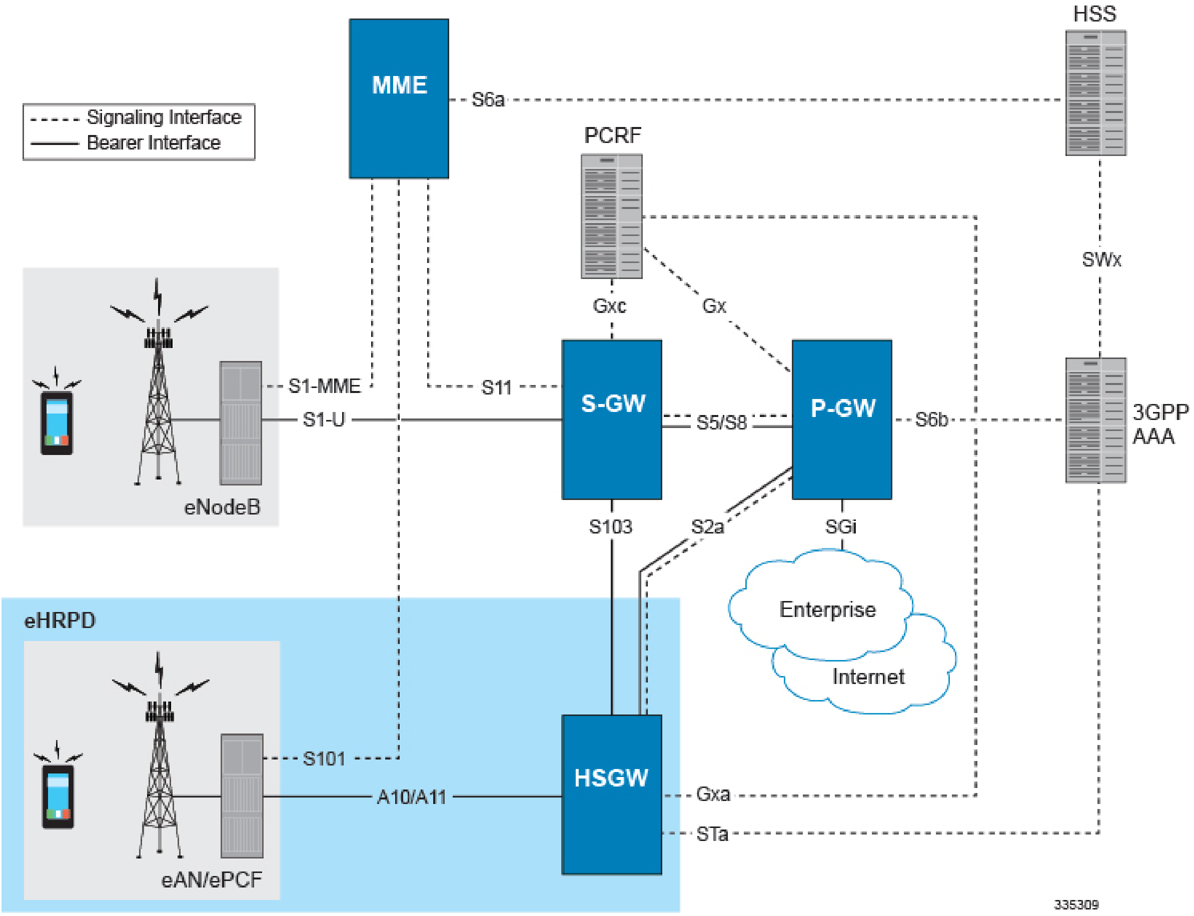
Network Deployment

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.

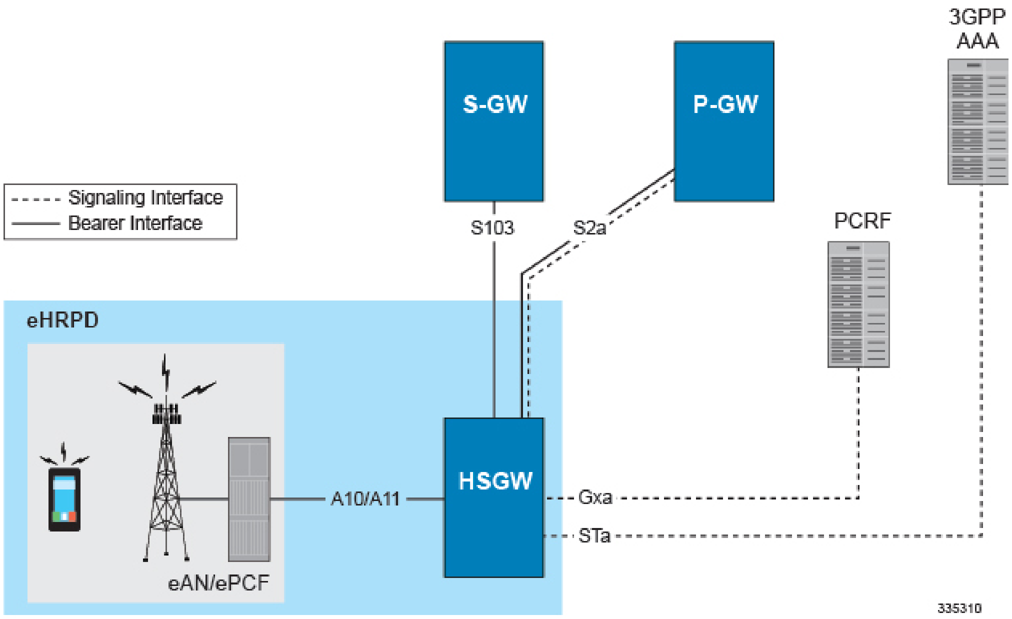
Figure 2: HSGW in an eHRPD Network Architecture



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.

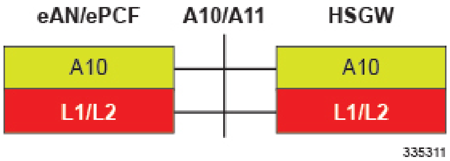
Figure 3: HSGW Supported Network Interfaces



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

A10/A11 Interface

This interface exists between the Evolved Access Network/Evolved Packet Control Function (eAN/ePCF) and the HSGW and implements the A10 (bearer) and A11 (signaling) protocols defined in 3GPP2 specifications.

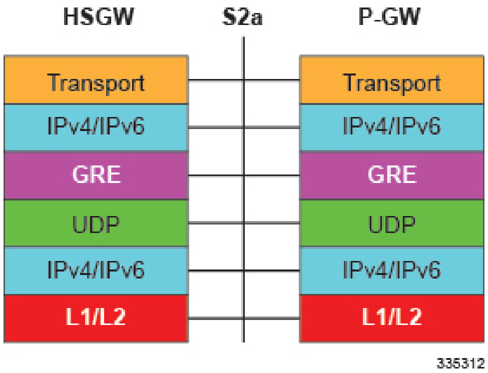


S2a Interface

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

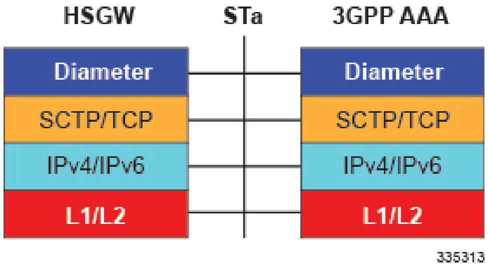


STa Interface

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

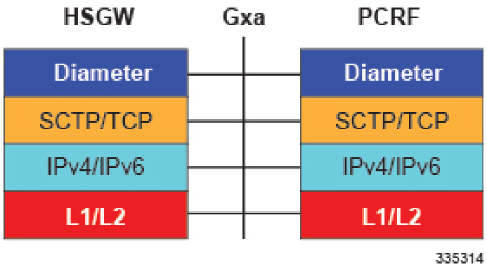


Gxa Interface

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.

Note To configure the basic service and functionality on the system for the HSGW service, refer to the configuration examples provided in the *HRPD Serving Gateway Administration Guide*.

The following features are supported and described in this section:

- A10/A11, on page 10
- AAA Server Groups, on page 10
- ANSI T1.276 Compliance, on page 10
- Bulk Statistics Support, on page 11
- Congestion Control, on page 12
- DSCP Marking, on page 12
- Dynamic Policy and Charging: Gxa Reference Interface, on page 13
- EAP Authentication (STa), on page 13
- Inter-user Best Effort Support Over eHRPD, on page 14
- IP Access Control Lists, on page 14
- Management System Overview, on page 15
- Mobile IP Registration Revocation, on page 16
- Multiple PDN Support, on page 17
- Network Initiated QoS, on page 17
- Non-Optimized Inter-HSGW Session Handover, on page 17
- P-GW Selection (Discovery), on page 18
- PMIPv6 Heartbeat, on page 19
- PPP VSNCP, on page 19
- Proxy Mobile IPv6 (S2a), on page 19
- Threshold Crossing Alerts (TCA) Support, on page 20
- UE Initiated Dedicated Bearer Resource Establishment, on page 21

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.

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.

ANSI T1.276 Compliance

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

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

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

These measures are applicable to the ASR 5500 and 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.

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 list of supported schemas for HSGW:

- **Card**: Provides card-level statistics
- **Context**: Provides context-level statistics
- **Diameter-acct**: Provides Diameter Accounting statistics
- **Diameter-auth**: Provides Diameter Authentication statistics
- **ECS**: Provides Enhanced Charging Service statistics
- **HSGW**: Provides HSGW statistics
- **IMSA**: Provides IMS Authorization statistics
- **IP Pool**: Provides IP pool statistics
- **MAG**: Provides Mobile Access Gateway statistics
- **Port**: Provides port-level statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **RP**: Provides RP statistics
- **System**: Provides system-level statistics

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

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

When 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*.

Congestion Control

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

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

Congestion control operation is based on configuring the following:

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

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

  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

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

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

In addition, the HSGW allows configuration of diameter packets with DSCP values.

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.

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

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).

Inter-user Best Effort Support Over eHRPD

The HSGW supports mapping of QoS parameters between 3GPP and 3GPP2 networks using QCI to flow profile-ID mapping, in accordance with 3GPP2 X.S0057. The HSGW supports the IUP VSA (26/139) to the eHRPD RAN. The non-GBR QCI is mapped to EV-DO Best Effort IUP class (0-7).

In addition, the HSGW is able to receive per-subscriber QoS instructions via the Gxa interface from PCRF to differentiate non-GBR best effort type flows.

IP Access Control Lists

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

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

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

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

Management System Overview

The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (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.

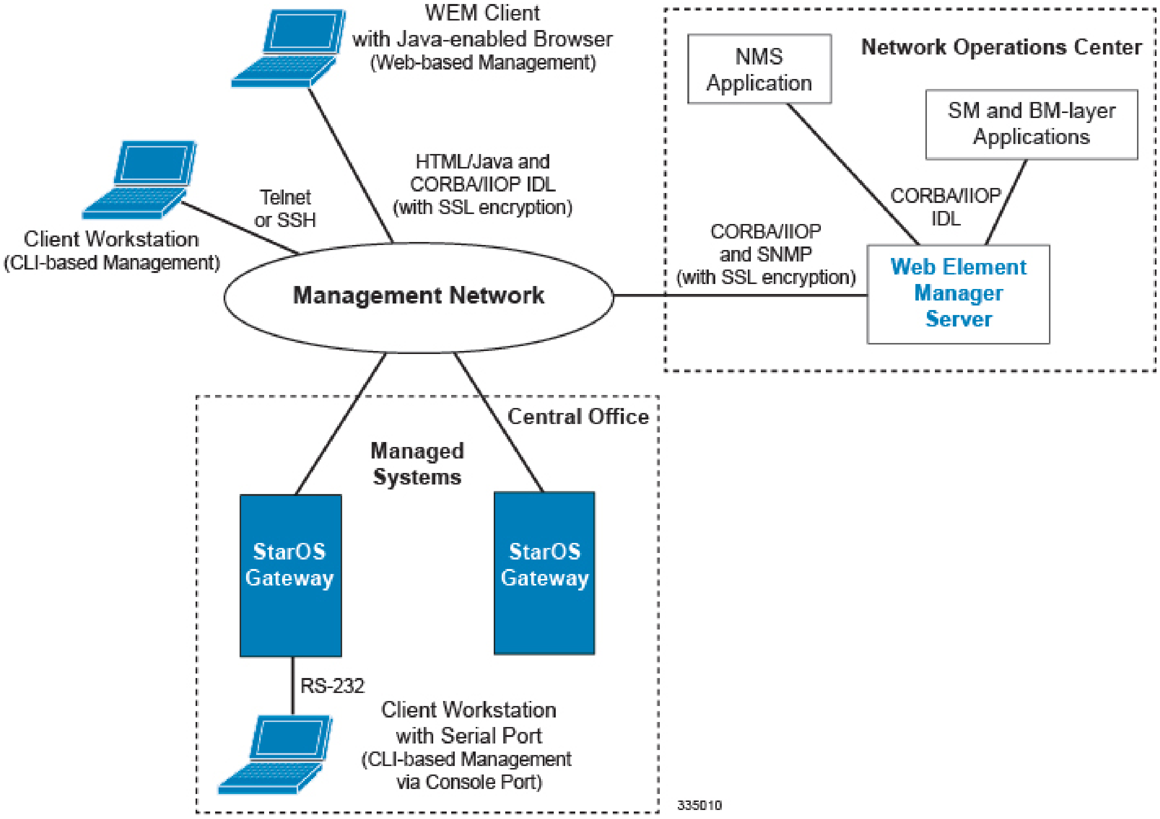
Cisco Systems' O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

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 HSGW 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*.

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)

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, you may configure a maximum of 14 PDN connections per user session. By default, up to three PDN connections per user session are supported.

Network Initiated QoS

The Network Initiated QoS control is a set of signaling procedures for managing bearers and controlling their QoS assigned by the network. This gives network operators full control over the QoS provided for its offered services for each of its subscriber groups.

If the UE supports Network Initiated QoS, then the UE shall include the MS Support of Network Requested Bearer Control indicator (BCM) parameter in the additional parameter list of the PCO option when sent in the vendor specific network control protocol (VSNCP) Configure-Request from the UE to the HSGW. Otherwise, the UE shall not include the MS Support of Network Requested Bearer Control indicator (BCM) parameter.

For Network Initiated QOS, three types of operations are permitted:

- Initiate flow request
- Deletion of packet filters for the specified traffic flow template (TFT)
- Modifications of packet filters for the specified TFT

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 and 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.

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.

Important P-GW load balancing using DNS SRV lookup can be enabled by defining P-GW DNS selection criteria in the HSGW service.

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:

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

During dynamic P-GW node selection by HSGW, if the selected P-GW is unreachable, HSGW selects the next P-GW entry from the P-GW candidate list returned during the S-NAPTR procedure to set up the PDN connection. For example, when an eHRPD PDN comes up, PMIPv6 session is tried with first P-GW selected if no reply is received for max-retransmission, HSGW tries with another P-GW if available based on DNS resolution results by starting with initial retransmission timeout as configured. There is no limit on the number of P-GW fallback attempts per PDN and HSGW will keep trying fallback as long as alternate P-GWs are available. The session may, however, get dropped if session-timeout gets triggered, in which case PMIPv6 PDN will also get deleted.

PMIPv6 Heartbeat

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

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

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

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

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.

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

Threshold Crossing Alerts (TCA) Support

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

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

The following thresholding models are supported by the system:

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

Thresholding reports conditions using one of the following mechanisms:

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

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

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

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

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

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

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

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.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the HSGW service.

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

Intelligent Traffic Control

The feature use license for Intelligent Traffic Control on the HSGW is included in the HSGW session use license.

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.

Important For more information on ITC, refer to the *Intelligent Traffic Control* chapter in this guide.

IP Security (IPSec)

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

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)

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 Reference Guide*.

Lawful Intercept

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

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

Layer 2 Traffic Management (VLANs)

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

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

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

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

Session Recovery Support

The feature use license for Session Recovery on the HSGW is included in the HSGW session use license.

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

Session recovery is performed by mirroring key software processes (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 Administration Guide*.

Traffic Policing and Shaping

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

Traffic policing 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 this 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 IPv6/IPv4 Access, on page 25
- PMIPv6 Lifetime Extension without Handover, on page 27
- PDN Connection Release Initiated by UE, on page 28
- PDN Connection Release Initiated by HSGW, on page 30
- PDN Connection Release Initiated by P-GW, on page 31

Initial Attach with IPv6/IPv4 Access

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

Figure 5: Initial Attach with IPv6/IPv4 Access Call Flow

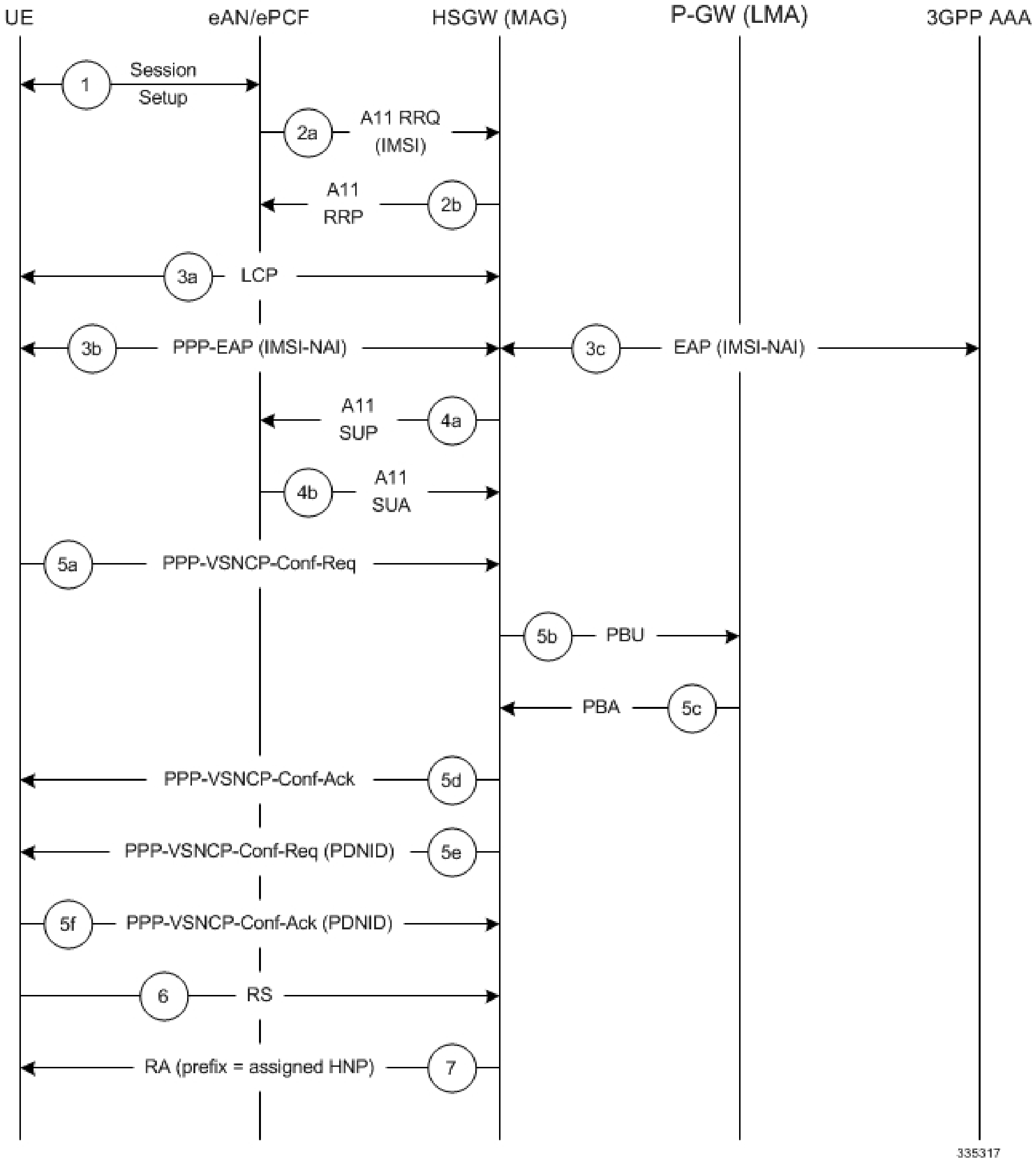


Table 2: Initial Attach with IPv6/IPv4 Access Call Flow Description

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.

Step	Description
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 6: PMIPv6 Lifetime Extension (without handover) Call Flow

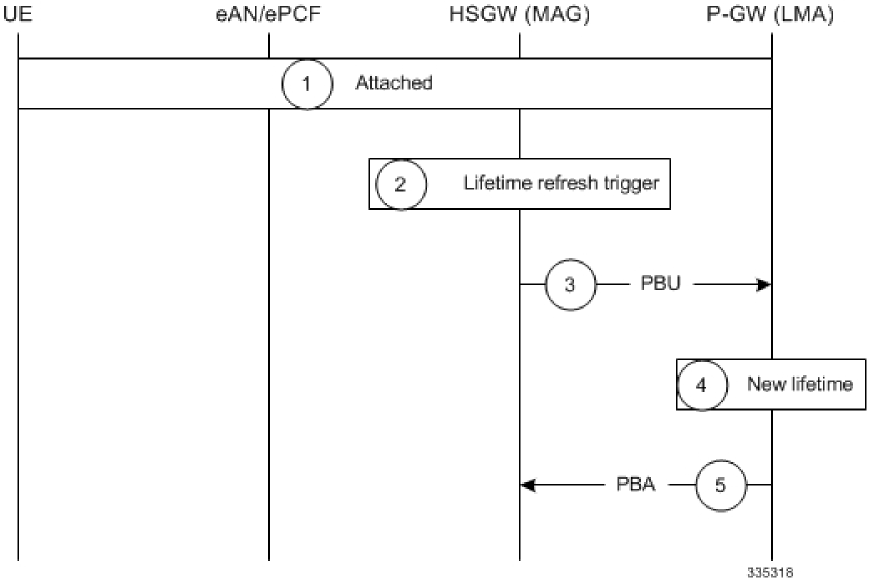


Table 3: PMIPv6 Lifetime Extension (without handover) Call Flow Description

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 7: PDN Connection Release by the UE Call Flow

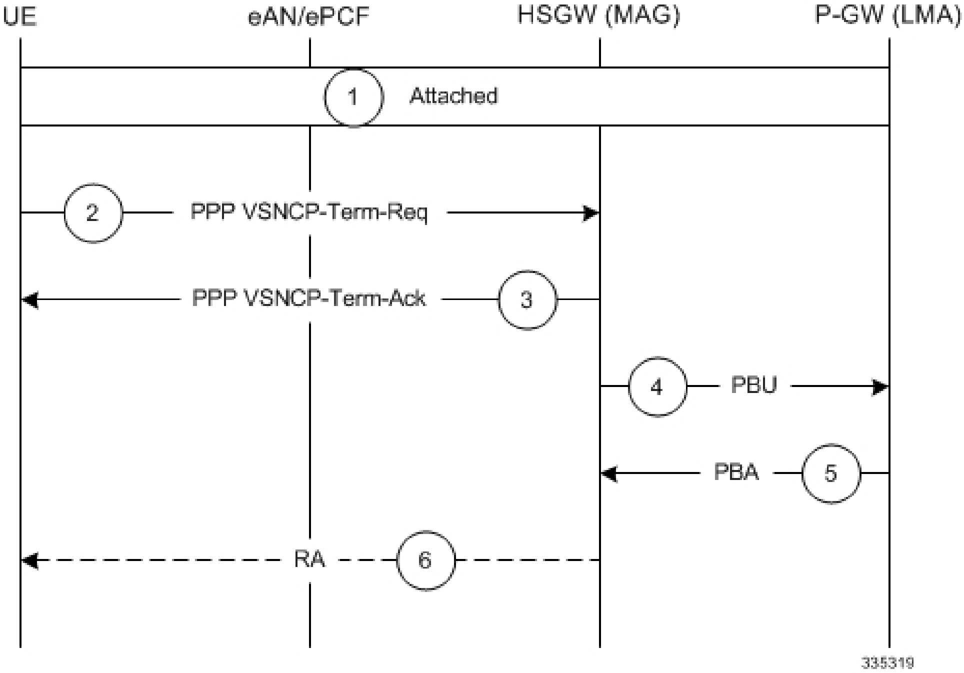


Table 4: PDN Connection Release by the UE Call Flow Description

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 8: PDN Connection Release by the HSGW Call Flow

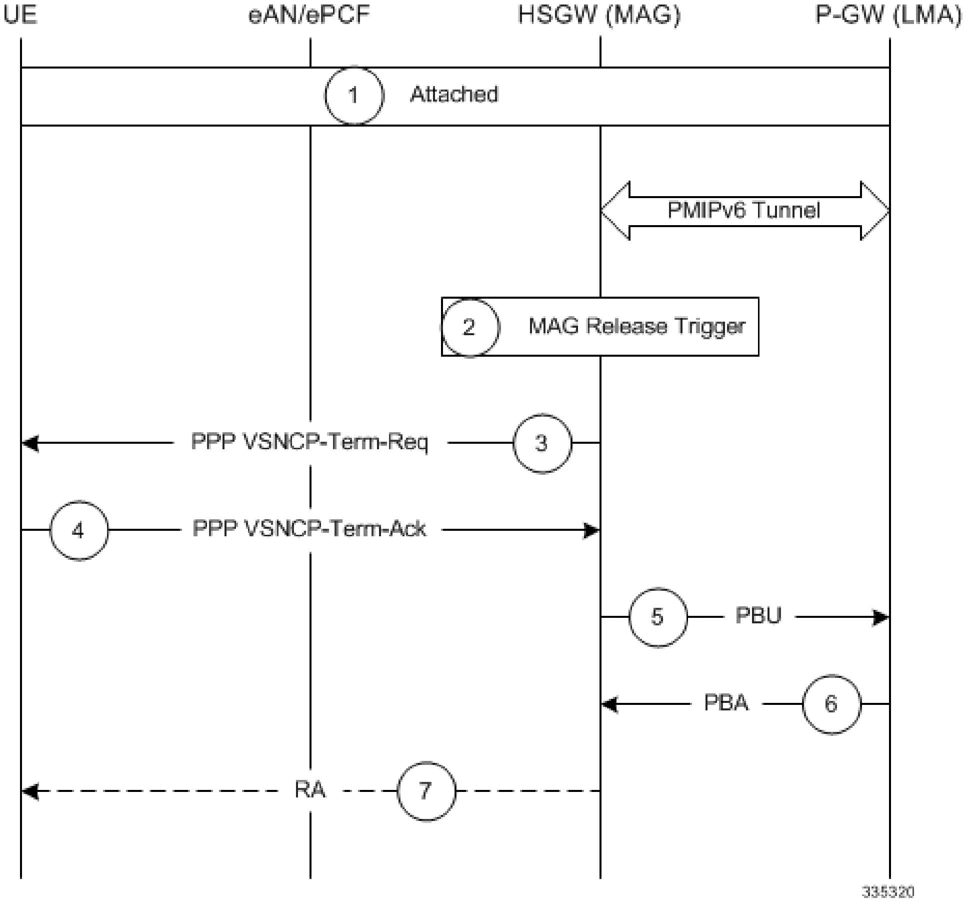


Table 5: PDN Connection Release by the HSGW Call Flow Description

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

Step	Description
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 9: PDN Connection Release by the P-GW Call Flow

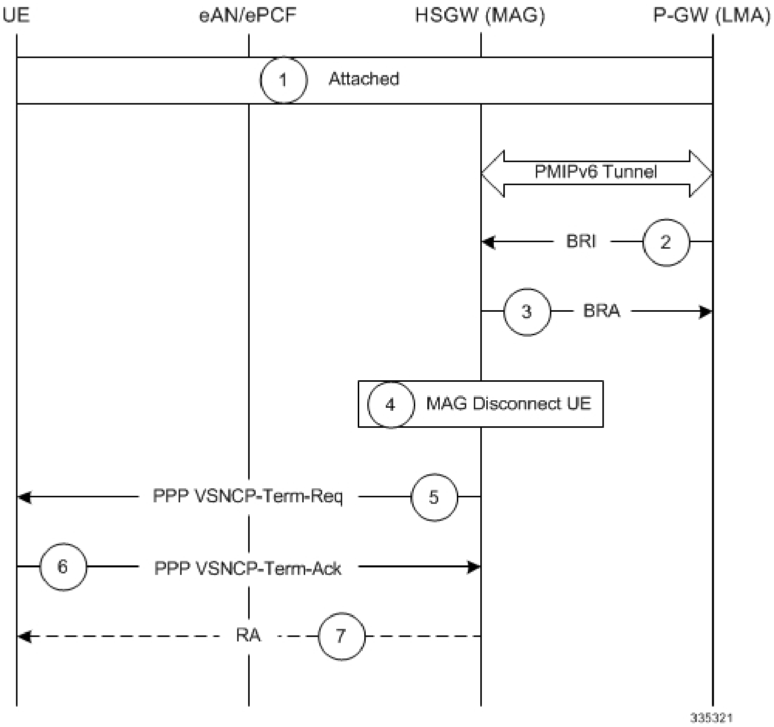


Table 6: PDN Connection Release by the P-GW Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	A 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).
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:

- Release 9 3GPP References, on page 32
- Release 8 3GPP References, on page 33
- 3GPP2 References, on page 33
- IETF References, on page 34
- Object Management Group (OMG) Standards, on page 34

Release 9 3GPP References

Important The HSGW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402. Architecture enhancements for non-3GPP accesses

- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.275 Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols Stage 3

Release 8 3GPP References

Important The HSGW currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.203: Policy and charging control architecture
- 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 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.210. Charging rule provisioning over Gx interface
- 3GPP TS 29.273 Evolved Packet System (EPS)3GPP EPS AAA interfaces
- 3GPP TS 32.299 Rf Offline Accounting Interface

3GPP2 References

- 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.S0017-D v1.0: Interoperability Specification (IOS) for cdma2000 Access Network Interfaces - Part 7 (A10 and A11 Interfaces), June, 2007.
- A.S0022-0 v1.0: E-UTRAN - HRPD Connectivity and Interworking: Access Network Aspects (E-UTRAN HRPD IOS), March 2009.
- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects
- X.S0011-001-D v1.0: cdma2000 Wireless IP Network Standard: Introduction, February, 2006.
- X.S0011-005-D v1.0: cdma2000 Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs, February, 2006.

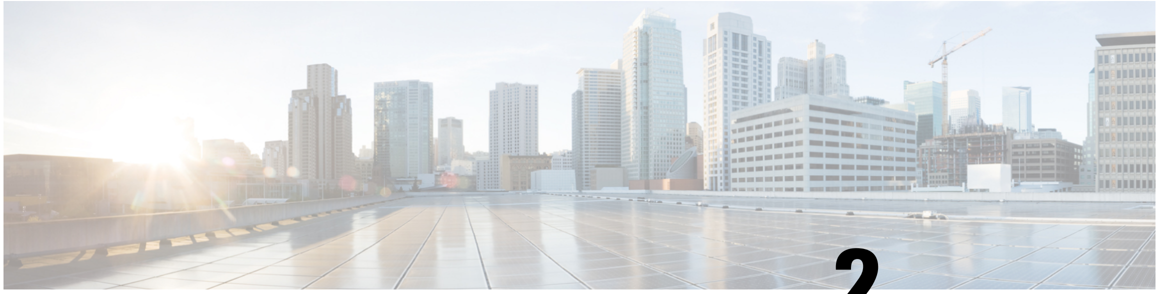
- X.S0057-0 v3.0: E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects, September 17, 2010

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 3588: (September 2003) Diameter Base Protocol
- RFC 3748 (June 2004): Extensible Authentication Protocol (EAP)
- RFC 3772 (May 2004): PPP Vendor Protocol
- RFC 3775 (June 2004): Mobility Support in IPv6
- RFC 4005: (August 2005) Diameter Network Access Server Application
- RFC 4006: (August 2005) Diameter Credit-Control Application
- RFC 4072: (August 2005) Diameter Extensible Authentication Protocol (EAP) Application
- RFC 4283 (November 2005): Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 5094 (December 2007): Mobile IPv6 Vendor Specific Option
- RFC 5149 (February 2008): Service Selection for Mobile IPv6
- RFC 5213 (August 2008): Proxy Mobile IPv6
- RFC 5847 (June 2010): Heartbeat Mechanism for 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 *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 *Command Line Interface Reference*.

The following information is provided in this chapter:

- Configuring the System to Perform as a Standalone HSGW, on page 35
- Configuring Optional Features on the HSGW, on page 49

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, on page 35
- How This Configuration Works, on page 41
- Configuration, on page 42

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.
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.

Required Information	Description
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.
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.
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.

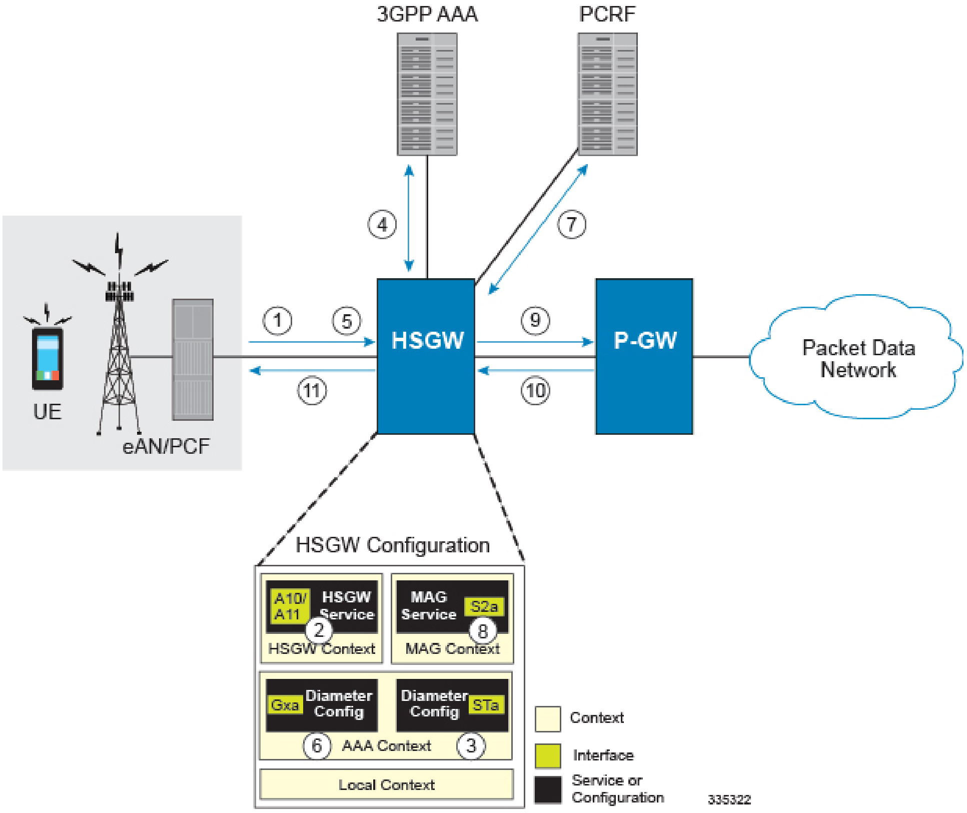
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Gxa Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gxa Diameter endpoint 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.

Required Information	Description
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.
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.

Required Information	Description
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.

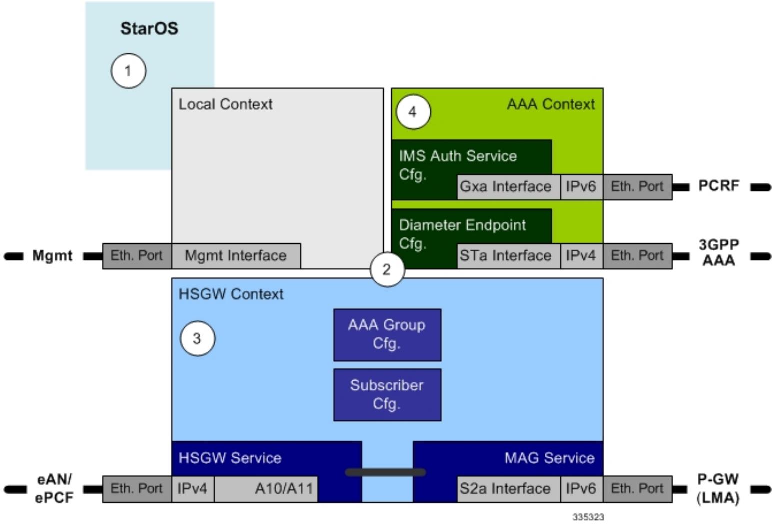
Step 9 The HSGW establishes the S2a connection by sending a PMIP Proxy Binding Update (PBU) to the P-GW including the NAI and APN. The PBU also includes the home network prefix and/or IPv4 home address option based on the subscriber\'s APN profile and UE IP version capability.

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 Initial Configuration, on page 43.

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 HSGW and MAG Service Configuration, on page 45.

Step 4 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in AAA and Policy Configuration, on page 47.

Step 5 Verify and save the configuration by following the instruction in Verifying and Saving the Configuration, on page 49.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 43.

Step 2 Create the context where the HSGW service will reside by applying the example configuration in Creating and Configuring an HSGW Context, on page 44.

Step 3 Specify static IP routes to the eAN/ePCF and/or PDN gateway by applying the example configuration in Configuring Static IP Routes, on page 44.

Step 4 Create an HSGW service within the newly created HSGW context by applying the example configuration in Creating an HSGW Service, on page 45.

Step 5 Create the context where the MAG service will reside by applying the example configuration in Creating and Configuring MAG Context, on page 45.

Step 6 Create a MAG service within the newly created MAG context by applying the example configuration in Creating a MAG Service, on page 45.

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 server 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 Configuring the HSGW Service, on page 46 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 Configuring the HSGW Service, on page 46.

Step 2 Configure the MAG service by applying the example configuration in Configuring the MAG Service, on page 46.

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>

               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, on page 44 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 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, on page 44 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, on page 44 section.

AAA and Policy Configuration

Step 1 Configure AAA and policy interfaces by applying the example configuration in Creating and Configuring the AAA Context, on page 47.

Step 2 Configure the default subscriber for the AAA context by applying the example configuration in Modifying the Default Subscriber, on page 48.

Step 3 Create and configure QCI to QoS mapping by applying the example configuration in Configuring QCI-QoS Mapping, on page 48.

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>
```

Notes:

- The IMS Auth Service is also crested and configured in the AAA context.

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.

Verifying and Saving the Configuration

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

Configuring Optional Features on the HSGW

The configuration examples in this section are optional and provided to cover the most common uses of the HSGW in a live network. The intent of these examples is to provide a base configuration for testing.

Configuring Network Initiated QoS

The configuration example in this section enables the ability to use network initiated QoS functionality.

In HSGW Service Configuration Mode, configure network initiated QoS as follows:

```
configure
     context <hsgw_context_name> -noconfirm
          hsgw-service <hsgw_service_name> -noconfirm
               network-initiated-qos
               rsvp max-retransmissions <count>
               rsvp retransmission-timeout <seconds>
               end
```

Notes:

- The **rsvp max-retransmissions** command specifies the maximum retransmission count of RP control packets. <*count*> must be an integer value between 1 and 1000000. Default count is 5.
- The **rsvp retransmission-timeout** command specifies the maximum amount of time, in seconds, to allow for retransmission of RP control packets. <*seconds*> must be an integer value between 1 and 1000000. Default is 3 seconds.

CHAPTER 3

Monitoring the Service

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

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

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

- Monitoring System Status and Performance, on page 51
- Clearing Statistics and Counters, on page 53

Monitoring System Status and Performance

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	

To do this:	Enter this command:
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**
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 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.

CHAPTER 4

Intelligent Traffic Control

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

This chapter contains the following topics:

Overview

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

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

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

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

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

ITC and EV-DO Rev A in 3GPP2 Networks

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

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

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

Bandwidth Control and Limiting

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

Licensing

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

How it Works

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

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

Traffic policing can be generally defined as

policy: condition >> action

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

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

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

Configuring Flow-based Traffic Policing

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

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

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

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

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

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

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

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

1. Configure the traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Class Maps, on page 58.
2. Configure the policy maps with traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Maps, on page 58.
3. Configure the policy group with policy maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Groups, on page 59.

4. Associate the subscriber profile with policy group to enable flow-based traffic policing for subscriber by applying the example configuration in Configuring a Subscriber for Flow-based Traffic Policing, on page 60.

5. Verify your flow-based traffic policing configuration by following the steps in Verifying Flow-based Traffic Policing Configuration, on page 60.

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

Configuring Class Maps

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

Important

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

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

Notes:

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

Configuring Policy Maps

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

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

Notes:

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

Configuring Policy Groups

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

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

Notes:

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

Configuring a Subscriber for Flow-based Traffic Policing

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

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

Notes:

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

Verifying Flow-based Traffic Policing Configuration

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

show subscribers access-flows full

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

CHAPTER 5

IP Header Compression

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

Important RoHC header compression is not applicable for SGSN and GGSN services.

Overview

The system supports IP header compression on the PPP tunnels established over the EVDO-RevA A10 links and also over the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67).

By default IP header compression using the VJ algorithm is enabled for subscribers using PPP.

Note that you can use the default VJ header compression algorithm alone, configure the use of RoHC header compression only, or use both VJ and RoHC IP header compression.

- **Van Jacobsen (VJ) -** The RFC 1144 (CTCP) header compression standard was developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

- **RObust Header Compression (RoHC)** - The RFC 3095 (RoHC) standard was developed in 2001. This standard can compress IP/UDP/RTP headers to just over one byte, even in the presence of severe channel impairments. This compression scheme can also compress IP/UDP and IP/ESP packet flows. RoHC is intended for use in wireless radio network equipment and mobile terminals to decrease header overhead, reduce packet loss, improve interactive response, and increase security over low-speed, noisy wireless links.

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

In addition, you can configure RoHC profiles that define RoHC Compressor and Decompressor parameters. These RoHC profiles can be applied to subscribers.

You can also turn off all IP header compression for a subscriber.

The procedures in this chapter describe how to configure the IP header compression methods used, but for RoHC over PPP the Internet Protocol Control Protocol (IPCP) negotiations determine when they are used.

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead.
- Reduces packet loss rate over lossy links.

Configuring VJ Header Compression for PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

Note that procedure described in this section is applicable only when VJ header compression is disabled.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* .

To configure the system to enable VJ header compression to IP headers:

Step 1 Enable VJ header compression by applying the example configuration in Enabling VJ Header Compression, on page 63.

Step 2 Verify your VJ header compression configuration by following the steps in Verifying the VJ Header Compression Configuration, on page 71.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling VJ Header Compression

Use the following example to enable the VJ header compression over PPP:

```
configure
     context <ctxt_name>
          subscriber name <subs_name>
               ip header-compression vj
               end
```

Notes:

- <*ctxt_name*> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <*subs_name*> is the name of the subscriber in the current context that you want to enable VJ IP header compression for.

Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring RoHC Header Compression for PPP

RoHC IP header compression can be configured for all IP traffic, uplink traffic only, or downlink traffic only. When RoHC is configured for all traffic, you can specify the mode in which RoHC is applied.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to enable RoHC header compression to IP headers:

- Enable RoHC header compression by applying the example configuration in Enabling RoHC Header Compression for PPP, on page 64.

- Verify your RoHC header compression configuration by following the steps in Verifying the Header Compression Configuration, on page 64.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling RoHC Header Compression for PPP

Use the following example to enable the RoHC over PPP:

```
configure
     context <ctxt_name>
          subscriber name <subs_name>
               ip header-compression RoHC [ any [ mode { optimistic |
reliable | unidirectional } ] | cid-mode { { large | small } [
marked-flows-only | max-cid | max-hdr <value> | mrru <value> ] } | marked
flows-only | max-hdr <value> | mrru <value> | downlink | uplink ] }+
               end
```

Notes:

- <*ctxt_name*> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <*subs_name*> is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring Both RoHC and VJ Header Compression

You can configure the system to use both VJ and RoHC IP header compression. When both VJ and RoHC are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

Important If both RoHC and VJ header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in th *Command Line Interface Reference*.

To configure the system to enable both RoHC and VJ header compression to IP headers:

- Enable the RoHC and VJ header compression by applying the example configuration in Enabling RoHC and VJ Header Compression for PPP, on page 65.
- Verify your RoHC and VJ header compression configuration by following the steps in Verifying the Header Compression Configuration, on page 65.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling RoHC and VJ Header Compression for PPP

Use the following example to enable the header compression over PPP:

```
configure
     context <ctxt_name>
          subscriber name <subs_name>
               ip header-compression vj RoHC [ any [ mode { optimistic |
reliable | unidirectional } ] | cid-mode { { large | small } [
marked-flows-only | max-cid | max-hdr <value> | mrru <value> ] } | marked
flows-only | max-hdr <value> | mrru <value> | downlink | uplink ] }+
               end
```

Notes:

- <*ctxt_name*> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <*subs_name*> is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- Refer to the Subscriber Configuration Mode Commands chapter in Command Line Interface Reference for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring RoHC for Use with SO67 in PDSN or HSGW Service

This section explains how to set RoHC settings in the PDSN or HSGW Service configuration mode. These settings are transferred to the PCF during the initial A11 setup and are used for the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67). RoHC is enabled through an auxiliary SO67 A10 connection and the PCF signals this information when the auxiliary A10 is connected.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer P*DSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to enable the RoHC header compression feature at the PDSN or HSGW Service over SO67:

Step 1 Enable header compression by applying the example configuration in Enabling RoHC Header Compression with PDSN, on page 66 or Enabling ROHC Header Compression with HSGW section.

Step 2 Verify your RoHC configuration by following the steps in Verifying the Header Compression Configuration, on page 67.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling RoHC Header Compression with PDSN

Use the following example to enable the RoHC header compression with PDSN over SO67:

```
configure
     context <ctxt_name>
          pdsn-service <svc_name>
               ip header-compression rohc
               cid-mode {large | small} max-cid integer
               mrru <num_octets>
               profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }
               end
```

Notes:

- *<ctxt_name>* is the system context in which PDSN service is configured and you wish to configure the service profile.

- <*svc_name*> is the name of the PDSN service in which you want to enable RoHC over SO67.
- Refer to the *PDSN Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Enabling RoHC Header Compression with HSGW

Use the following example to enable the RoHC header compression with HSGW over SO67:

```
configure
     context <ctxt_name>
          hsgw-service <svc_name>
               ip header-compression rohc
                    cid-mode {large | small} max-cid integer
                    mrru <num_octets>
                 profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip]
 }
                    end
```

Notes:

- <*ctxt_name*> is the system context in which HSGW service is configured and you wish to configure the service profile.
- <*svc_name*> is the name of the HSGW service in which you want to enable RoHC over SO67.
- Refer to the *HSGW Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context ctxt_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Using an RoHC Profile for Subscriber Sessions

You can configure RoHC profiles that specify numerous compressor and decompressor settings. These profiles can in turn be applied to a specific subscriber or the default subscriber. RoHC profiles are used for both RoHC over PPP and for RoHC over SO67.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to apply RoHC profile to a subscriber session:

Step 1 Create RoHC profile using decompression mode or decompression mode. If you want to use compression mode go to step a else follow step b:

a) Configure RoHC profile by applying the example configuration in the Creating RoHC Profile for Subscriber using Compression Mode, on page 68 using compression mode.

b) Alternatively configure RoHC profile by applying the example configuration in the Creating RoHC Profile for Subscriber using Decompression Mode, on page 69 using compression mode.

Step 2 Apply existing RoHC profile to a subscriber by applying the example configuration in the Applying RoHC Profile to a Subscriber, on page 69.

Step 3 Verify your RoHC header compression configuration by following the steps in the Verifying the Header Compression Configuration, on page 70.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Creating RoHC Profile for Subscriber using Compression Mode

Use the following example to create RoHC profile for a subscriber using compression mode:

```
configure
     RoHC-profile profile-name <RoHC_comp_profile_name>
          decompression-options
               [no] multiple-ts-stride
               rtp-sn-p <p_value>
               [no] use-ipid-override
               [no] use-optimized-talkspurt
               [no] use-optimized-transience
               [no] use-timer-based-compression
               end
```

Notes:

- *<RoHC_comp_profile_name>* is the name of the RoHC profile with compression mode which you want to apply to a subscriber.
- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Compression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

Creating RoHC Profile for Subscriber using Decompression Mode

Use the following example to create RoHC profile for a subscriber using decompression mode:

```
configure
     RoHC-profile profile-name <RoHC_decomp_profile_name>
          decompression-options
               context-timeout <dur>
               max-jitter-cd <dur_ms>
               nak-limit <limit>
               optimistic-mode-ack
               optimistic-mode-ack-limit <num_pkts>
               piggyback-wait-time <dur_ms>
               preferred-feedback-mode { bidirectional-optimistic |
bidirectional-reliable | unidirectional }
               rtp-sn-p <p_value>
               [no] rtp-sn-p-override
               [no] use-clock-option
               [no] use-crc-option
               [no] use-feedback
               [no] use-jitter-option
               [no] use-reject-option
               [no] use-sn-option
               end
```

Notes:

- <*RoHC_profile_name*> is the name of the RoHC profile with decompression mode which you want to apply to a subscriber.
- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Decompression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

Applying RoHC Profile to a Subscriber

Once an RoHC profile has been created that profile can be specified to be used for a specific subscribers. Use the following example to apply the RoHC profile to a subscriber:

```
configure
     context <ctxt_name>
          subscriber name <subs_name>
               RoHC-profile-name <RoHC_profile_name>
               end
```

Notes:

- <*ctxt_name*> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <*subs_name*> is the name of the subscriber in the current context that you want to enable RoHC header compression for.

- *<RoHC_profile_name>* is the name of the existing RoHC profile (created with compressed or decompressed mode) which you want to apply to a subscriber in the current context.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Disabling VJ Header Compression Over PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

If you do not want to apply compression to any IP headers for a subscriber session you can disable the IP header compression feature.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable VJ header compression to IP headers:

Step 1 Disable header compression by appling the example configuration in Disabling VJ Header Compression, on page 70.

Step 2 Verify your VJ header compression configuration by following the steps in Verifying the VJ Header Compression Configuration, on page 71.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Disabling VJ Header Compression

Use the following example to disable the VJ header compression over PPP:

```
configure
     context <ctxt_name>
          subscriber name <subs_name>
              no ip header-compression
              end
```

Notes:

- *<ctxt_name>* is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- *<subs_name>* is the name of the subscriber in the current context that you want to disable IP header compression for.

Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username <subs_name>
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Disabling RoHC Header Compression Over SO67

If you do not want to apply compression to any IP headers for a subscriber sessions using the EVDO-RevA SO67 feature, you can disable the IP header compression feature at the PDSN or HSGW Service.

Important This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *PDSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable the IP header compression feature at the PDSN or HSGW Service:

Step 1 Disable header compression by applying the example configuration in Disabling RoHC Header Compression, on page 72.

Step 2 Verify your RoHC configuration by following the steps in Verifying the Header Compression Configuration, on page 72.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Disabling RoHC Header Compression

Use the following example to disable the header compression over SO67:

```
configure
     context <ctxt_name>
          pdsn/hsgw-service <svc_name>
               no ip header-compression RoHC
               end
```

Notes:

- <*ctxt_name*> is the system context in which PDSN or HSGW service is configured and you wish to configure the service profile.
- <*svc_name*> is the name of the PDSN or HSGW service in which you want to disable RoHC over SO67.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context <ctxt_name>
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Checking IP Header Compression Statistics

This section commands to use to retrieve statistics that include IP header compression information.

The following Exec mode commands can be used to retrieve IP header compression statistics:

- monitor protocol ppp
- show ppp
- show ppp statistics
- show RoHC statistics
- show RoHC statistics pdsn-service
- show subscriber full username

For more information on these commands, refer to the *Command Line Interface Reference*.

RADIUS Attributes for IP Header Compression

This section lists the names of the RADIUS attributes to use for RoHC header compression. For more information on these attributes, refer to the AAA Interface Administration and Reference.

One of the following attributes can be used to specify the name of the RoHC profile to use for the subscriber session:

- SN-RoHC-Profile-Name
- SN1-RoHC-Profile-Name

Any RoHC parameters not specified in the RoHC profile are set to their default values.

CHAPTER 6

Mobile IP Registration Revocation

This chapter describes Registration Revocation for Mobile-IP and Proxy Mobile-IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in this administration guide before using the procedures in this chapter.

Important This license is enabled by default; however, not all features are supported on all platforms and other licenses may be required for full functionality as described in this chapter.

This chapter includes the following topics:

Overview

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring Registration Revocation

Support for MIP Registration Revocation requires the following configurations:

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

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

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

Configuring FA Services

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

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

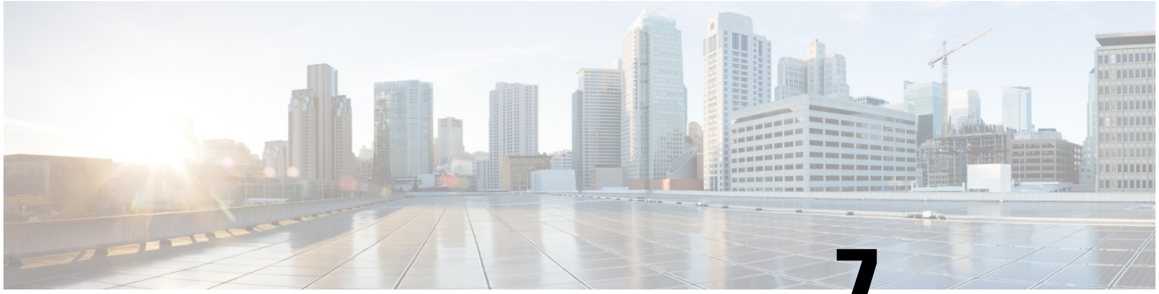
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring HA Services

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

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

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



CHAPTER 7

PMIPv6 Heartbeat

This chapter describes the Proxy Mobile IPv6 (PMIPv6) feature.

Feature Description

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

The PMIPv6 Heartbeat or Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

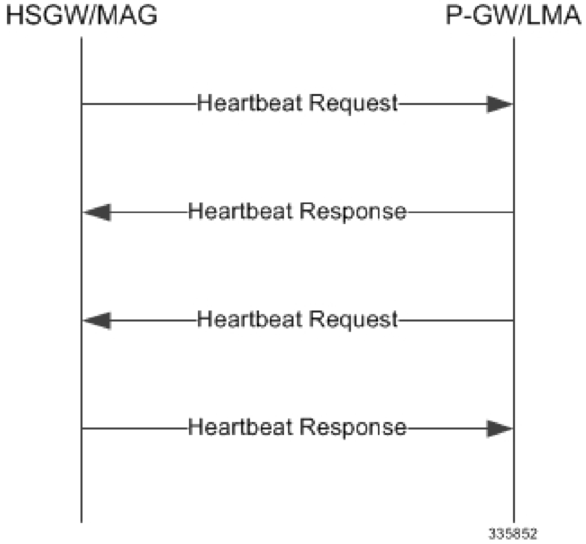
The PMIP Heartbeat feature support on HSGW/MAG and P-GW/LMA is based on RFC 5847.

How it Works

PMIPv6 Heartbeat Mechanism

The MAG and the LMA exchange Heartbeat messages at regular intervals to detect the current status of reachability between the two of them. The MAG initiates the heartbeat exchange to test if the LMA is reachable by sending a Heartbeat Request message to the LMA. Each Heartbeat Request contains a sequence number that is incremented monotonically. Heartbeat Request messages are sent to LMA only if the MAG has at least one PMIPv6 session with a corresponding LMA. Similarly, the LMA also initiates a heartbeat exchange with the MAG by sending a Heartbeat Request message to check if the MAG is reachable.

Figure 10: MAG and LMA exchange Heartbeat messages



Refer to the **heartbeat** CLI command in the LMA Service mode or MAG Service mode respectively to enable this heartbeat and configure the heartbeat variables.

The heartbeat messages are used only for checking reachability between the MAG and the LMA. They do not carry information that is useful for eavesdroppers on the path. Therefore, confidentiality protection is not required.

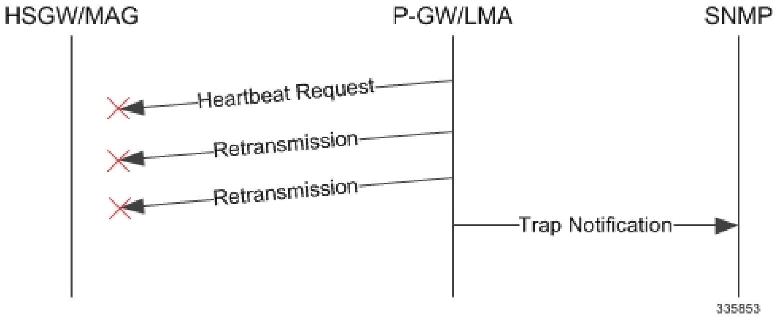
Failure Detection

The sequence number sent in the Heartbeat Request message is matched when the Heartbeat response is received at the MAG/LMA. Before sending the next Heartbeat Request, the missing heartbeat counter is incremented if it has not received a Heartbeat Response for the previous request.

When the missing heartbeat counter exceeds the configurable parameter **max-heartbeat-retransmission**, the MAG/LMA concludes that the peer is not reachable. The heartbeat request to the peer will be stopped and a notification trap is triggered to indicate the failure.

If a heartbeat response message is received, then the missing heartbeat counter is reset.

Figure 11: Failure Detection



The **starPMIPPathFailure** trap is cleared and the periodic heartbeat starts when the heartbeat request is received or when a new session is established from the corresponding peer.

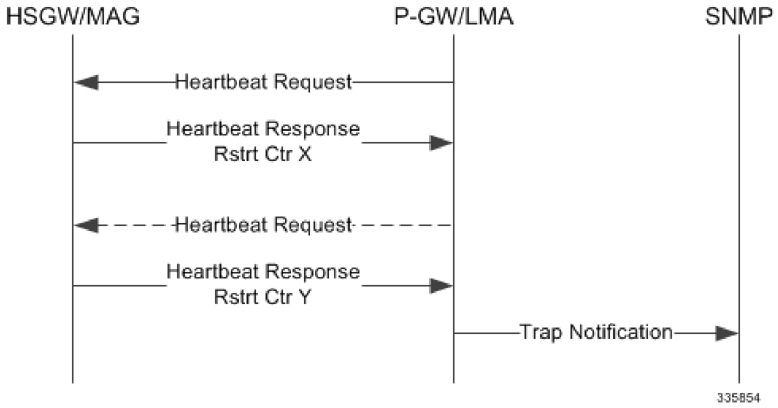
Important The failure detection at MAG will be the same as the one described in the Failure Detection figure for LMA.

Restart Detection

MAG/LMA generates restart counter when the service is started. This counter is generated based on the service start timestamp. The restart counter is stored as part of the config and it is incremented whenever the service is restarted. The counter is not incremented if the sessions are recovered properly after a crash. MAG/LMA includes the restart counter mobility option in a heartbeat response message to indicate the current value of the restart counter. MAG/LMA also stores the restart counter values of all the peers with which it currently has PMIPv6 sessions.

After receiving the Heartbeat Response message, MAG/LMA compares the Restart Counter value with the previously received value. If the value is different, then it assumes that the peer had crashed and recovered. If the restart counter value changes or if there was no previously stored values, then the new value is stored for the corresponding peer.

Figure 12: Restart Detection



The second heartbeat request in the Restart Detection figure is shown as a dashed arrow because the restart detection can happen even when an unsolicited heartbeat response is received with a change in restart counter.

The **starPMIPPathFailure** trap is cleared when the Heartbeat request is received or when a new session is established with the corresponding peer.

Important The restart detection at MAG will the be same as the one described in Restart Detection figure for LMA.

Standards Compliance

The PMIPv6 Heartbeat functionality complies with the following standards:

- RFC 5847 (June 2010): Heartbeat Mechanism for Proxy Mobile IPv6
- 3GPP TS 29.275 Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols Stage 3

Configuring PMIPv6 Heartbeat

The configuration examples in this section can be used to control the heartbeat messages interval and retransmission timeout and max retransmission.

Configuring PMIPv6 MAG Heartbeat

The following command configures the PMIPv6 heartbeat message interval and retransmission timeout and max retransmission for the MAG/HSGW Service.

```
configure
      context context_name
            mag-service hsgw_svc_name
                 heartbeat { interval seconds | retransmission { max number
 | timeout seconds } }
                  default heartbeat { interval | retransmission { max |
timeout } }
                  no heartbeat
                  end
```

Notes:

- **interval**: The interval in seconds at which heartbeat messages are sent from 30-3600 seconds. Default: 60 seconds.
- **retransmission max**: The maximum number of heartbeat retransmissions allowed from 0-15. Default: 3.
- **retransmission timeout**: The timeout in seconds for heartbeat retransmissions from 1-20 seconds. Default: 3 seconds.

Configuring PMIPv6 LMA Heartbeat

The following command configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the LMA/P-GW Service.

```
configure
      context context_name
            lma-service pgw_lma_name
                 heartbeat { interval seconds | retransmission { max number
 | timeout  seconds } }
                  default heartbeat { interval | retransmission { max |
timeout } }
                  no heartbeat
                  end
```

Notes:

- **interval**: The interval in seconds at which heartbeat messages are sent.

  seconds must be an integer from 30 to 2600. Default: 60
- **retransmission max**: The maximum number of heartbeat retransmissions allowed.

number must be an integer from 0 to 15.

Default: 3

- **retransmission timeout**: The timeout in seconds for heartbeat retransmissions.

  seconds must be an integer from 1 to 20.

  Default: 3

Verifying the PMIPv6 Heartbeat Configuration

The following show commands can be used to verify the configured heartbeat configuration.

show mag-service name <mag-service>

```
Heartbeat support: Enabled
Heartbeat Interval: 60
Heartbeat Retransmission Timeout: 5
Heartbeat Max Retransmissions: 5
```

show lma-service name <lma-service>

```
Heartbeat support: Enabled
Heartbeat Interval: 60
Heartbeat Retransmission Timeout: 5
Heartbeat Max Retransmissions: 5
```

Monitoring and Troubleshooting the PMIPv6 Heartbeat

This section includes show commands in support of the PMIPv6 Heartbeat, traps that are triggered by the MAGMGR/HAMGR after path failure and Heartbeat bulk statistics.

- PMIPv6 Heartbeat Show Commands, on page 83
- PMIPv6 Heartbeat Traps on failure detection, on page 84
- PMIPv6 Heartbeat Bulk Statistics, on page 85

PMIPv6 Heartbeat messages can be monitored using monitor protocol. HAMGR and MAGMGR log messages can be enabled to troubleshoot and debug PMIPv6 Heartbeat scenarios.

SNMP traps are generated on failure detection and restart detection. The traps can be enabled to know path failure or node restart

Heartbeat message statistics and path failure statistics on MAG and LMA can be used to troubleshoot and debug PMIPv6 Heartbeat scenarios.

PMIPv6 Heartbeat Show Commands

This section provides information regarding show commands and/or their outputs in support of the PMIPv6 Heartbeat.

show mag-service statistics

This show command displays heartbeat output similar to the following for heartbeat statistics.

```
Path Management Messages:
Heartbeat Request:
Total TX: 0                                Total RX: 0
Initial TX: 0                              Initial RX: 0
Retrans TX: 0
Heartbeat Response:
Total TX: 0                                Total RX: 0
Bind Error: 0
Heartbeat Messages Discarded:
Total: 0
Decode error: 0                            Invalid Buffer Length:  0
Heartbeat Rsp From Unknown Peer: 0         Heartbeat Rsp Seq. Num Mismatch: 0
Reasons for path failure:
Restart counter change: 0
No Heartbeat Response received: 0
Total path failures detected: 0
```

show lma-service statistics

This show command displays heartbeat output similar to the following for heartbeat statistics.

```
Path Management Messages:
Heartbeat Request:
Total TX: 0                                Total RX: 0
Initial TX: 0                              Initial RX: 0
Retrans TX: 0
Heartbeat Response:
Total TX: 0                                Total RX: 0
Bind Error: 0
Heartbeat Messages Discarded:
Total: 0
Decode error: 0                            Invalid Buffer Length: 0
Heartbeat Rsp From Unknown Peer: 0         Heartbeat Rsp Seq. Num Mismatch: 0
Reasons for path failure:
Restart counter change: 0
No Heartbeat Response received:  0
Total path failures detected: 0
```

PMIPv6 Heartbeat Traps on failure detection

PMIPv6 Path Failure Trap

The trap name is **starPMIPPathFailure**.

The following trap notifications are triggered by the MAGMGR/HAMGR when path failure or node restart is detected.

- Context Name
- Service Name
- Self Address
- Peer Address
- Peer old restart counter
- Peer new restart counter
- Failure reason

PMIPv6 Path Failure Clear Trap

The trap name is **starPMIPPathFailureClear**.

The following trap notifications are generated by MAGMGR/HAMGR to clear the Path Failure Trap when a node is responding for heartbeat messages.

- Context Name
- Service Name
- Self Address
- Peer Address

PMIPv6 Heartbeat Bulk Statistics

The following Schema bulk statistics have been introduced for the PMIPv6 Heartbeat feature:

MAG schema

The following bulkstats have been added for PMIPv6 heartbeat statistics:

- lma-fallback-attempted
- lma-fallback-success
- lma-fallback-failure
- lma-fallback-demux-update-fail
- lma-fallback-alt-pgw-not-found
- lma-fallback-pgw-rejects
- lma-fallback-pgw-timeouts
- mag-txhbreqinitial
- mag-txhbreqretrans
- mag-txhbrsptotal
- mag-rxhbreqtotal
- mag-rxhbrsptotal
- mag-rxhbrspbinderror
- mag-rxhbdiscardtotal
- mag-rxhbdecodeerror
- mag-rxhbinvalidbufflen
- mag-rxhbrspunknownpeer
- mag-rxhbrspseqnummismatch
- mag-rxhbrsprstctrmissing
- mag-pathfailurestotal
- mag-pathfailrstctrchange
- mag-pathfailnohbrsprcvd

For descriptions of these variables, see "MAG Schema Statistics" in the *Statistics and Counters Reference*.

LMA Schema

The following bulkstats have been added for PMIPv6 heartbeat statistics:

- lma-txhbreqinitial
- lma-txhbreqretrans

- lma-txhbrsptotal
- lma-rxhbreqtotal
- lma-rxhbrsptotal
- lma-rxhbrspbinderror
- lma-rxhbdiscardtotal
- lma-rxhbdecodeerror
- lma-rxhbinvalidbufflen
- lma-rxhbrspunknownpeer
- lma-rxhbrspseqnummismatch
- lma-rxhbrsprstctrmissing
- lma-pathfailurestotal
- lma-pathfailrstctrchange
- lma-pathfailnohbrsprcvd

For descriptions of these variables, see "LMA Schema Statistics" in the *Statistics and Counters Reference*.

CHAPTER 8

Proxy-Mobile IP

This chapter describes system support for Proxy Mobile IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model before using the procedures in this chapter.

Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:

Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

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

The Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Table 7: Applicable Products and Relevant Sections

Applicable Product(s)	Refer to Sections
PDSN	• Proxy Mobile IP in 3GPP2 Service, on page 89 • How Proxy Mobile IP Works in 3GPP2 Network, on page 90 • Configuring FA Services, on page 116 • Configuring Proxy MIP HA Failover, on page 117 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 117 • RADIUS Attributes Required for Proxy Mobile IP, on page 118 • Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN, on page 119 • Configuring Default Subscriber Parameters in Home Agent Context, on page 120
GGSN	• Proxy Mobile IP in 3GPP Service, on page 90 • How Proxy Mobile IP Works in 3GPP Network, on page 97 • Configuring FA Services, on page 116 • Configuring Proxy MIP HA Failover, on page 117 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 117 • RADIUS Attributes Required for Proxy Mobile IP, on page 118 • Configuring Default Subscriber Parameters in Home Agent Context, on page 120 • Configuring APN Parameters, on page 120

Applicable Product(s)	Refer to Sections
ASN GW	• Proxy Mobile IP in WiMAX Service, on page 90 • How Proxy Mobile IP Works in WiMAX Network, on page 102 • Configuring FA Services, on page 116 • Configuring Proxy MIP HA Failover, on page 117 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 117 • RADIUS Attributes Required for Proxy Mobile IP, on page 118 • Configuring Default Subscriber Parameters in Home Agent Context, on page 120
PDIF	• How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication, on page 108 • Configuring FA Services, on page 116 • Configuring Proxy MIP HA Failover, on page 117 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 117 • RADIUS Attributes Required for Proxy Mobile IP, on page 118 • Configuring Default Subscriber Parameters in Home Agent Context, on page 120

Proxy Mobile IP in 3GPP2 Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

How Proxy Mobile IP Works in 3GPP2 Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.

- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 13: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

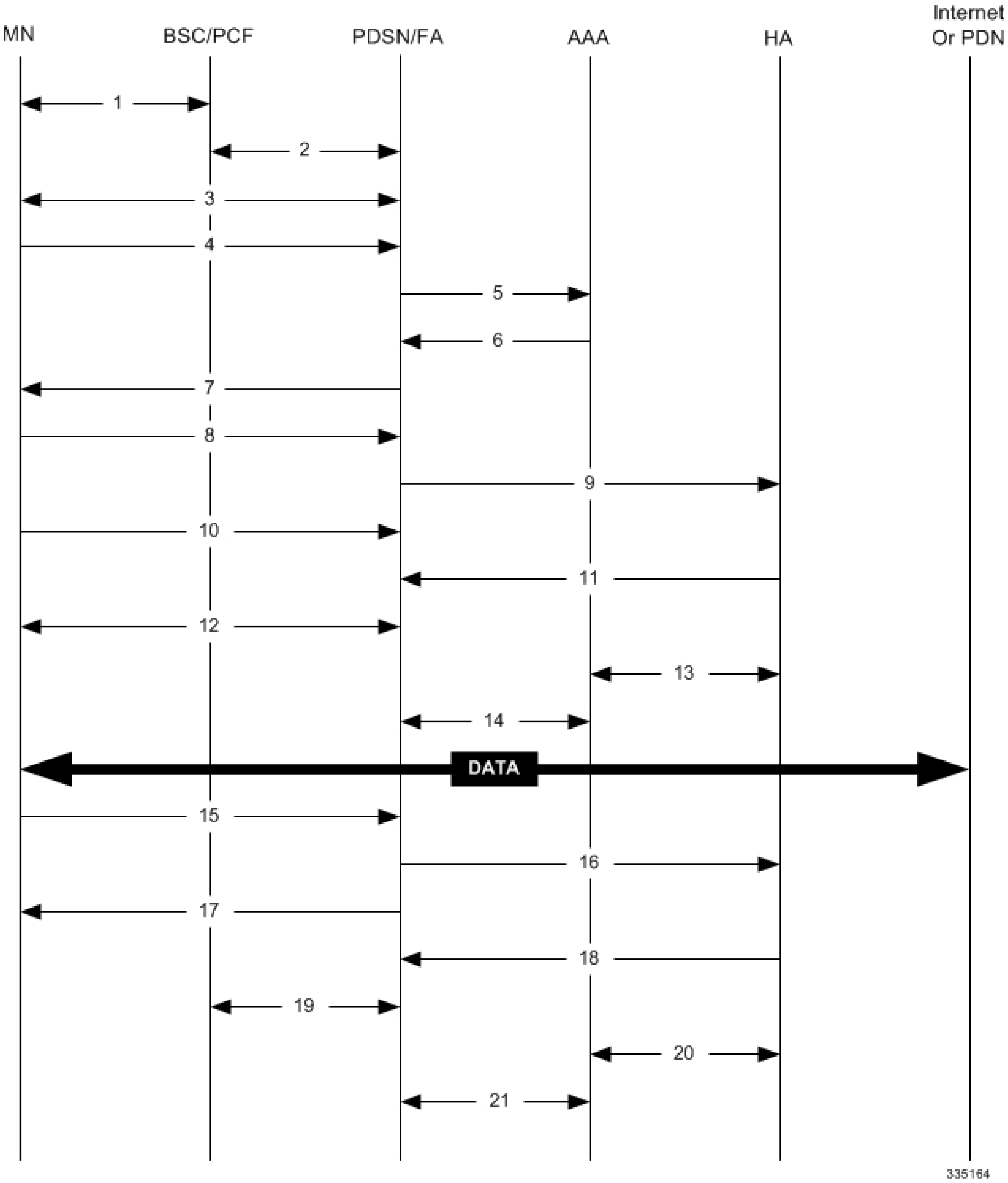


Table 8: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.

Step	Description
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.

Step	Description
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 14: HA Assigned IP Address Proxy Mobile IP Call Flow

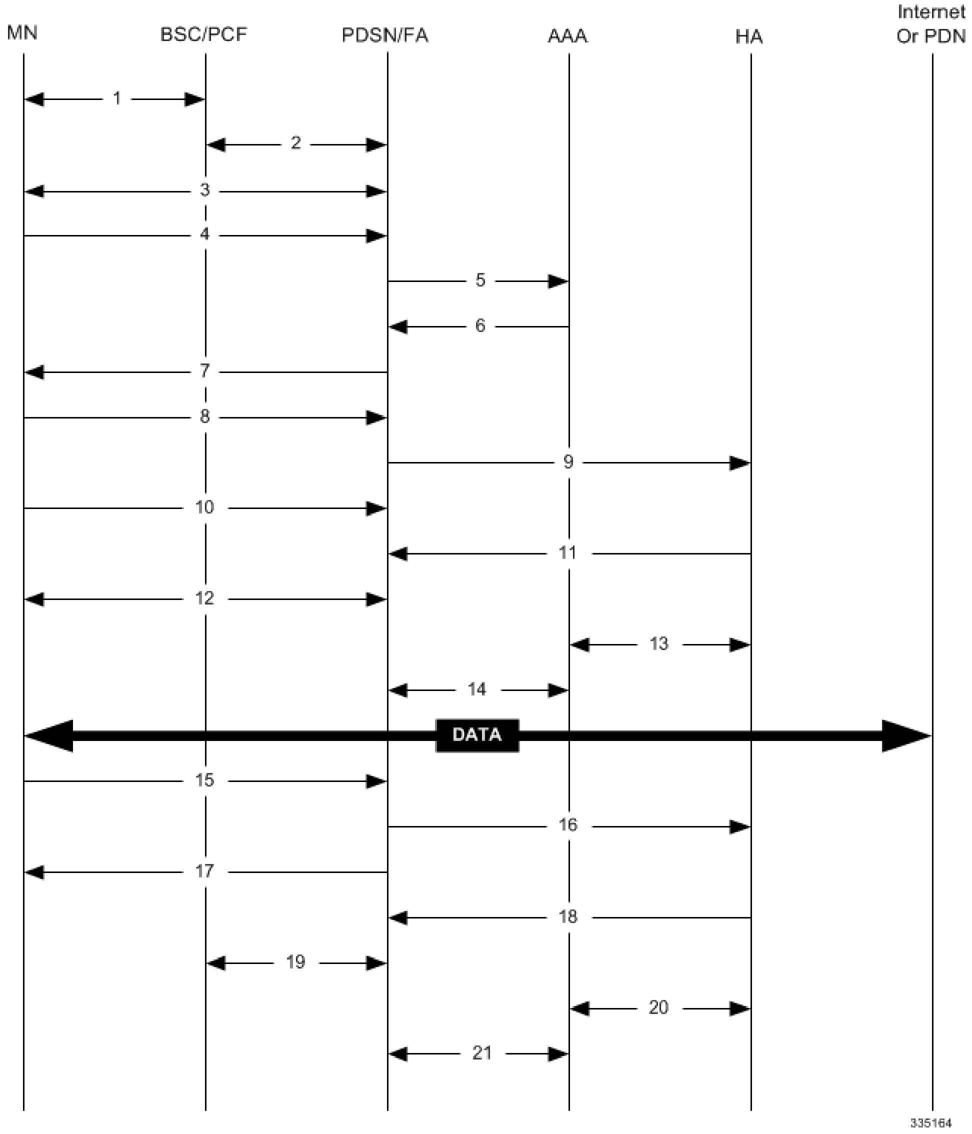


Table 9: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network.

The following figure and the text that follows describe a a sample successful Proxy Mobile IP session setup call flow in 3GGP service.

Figure 15: Proxy Mobile IP Call Flow in 3GPP

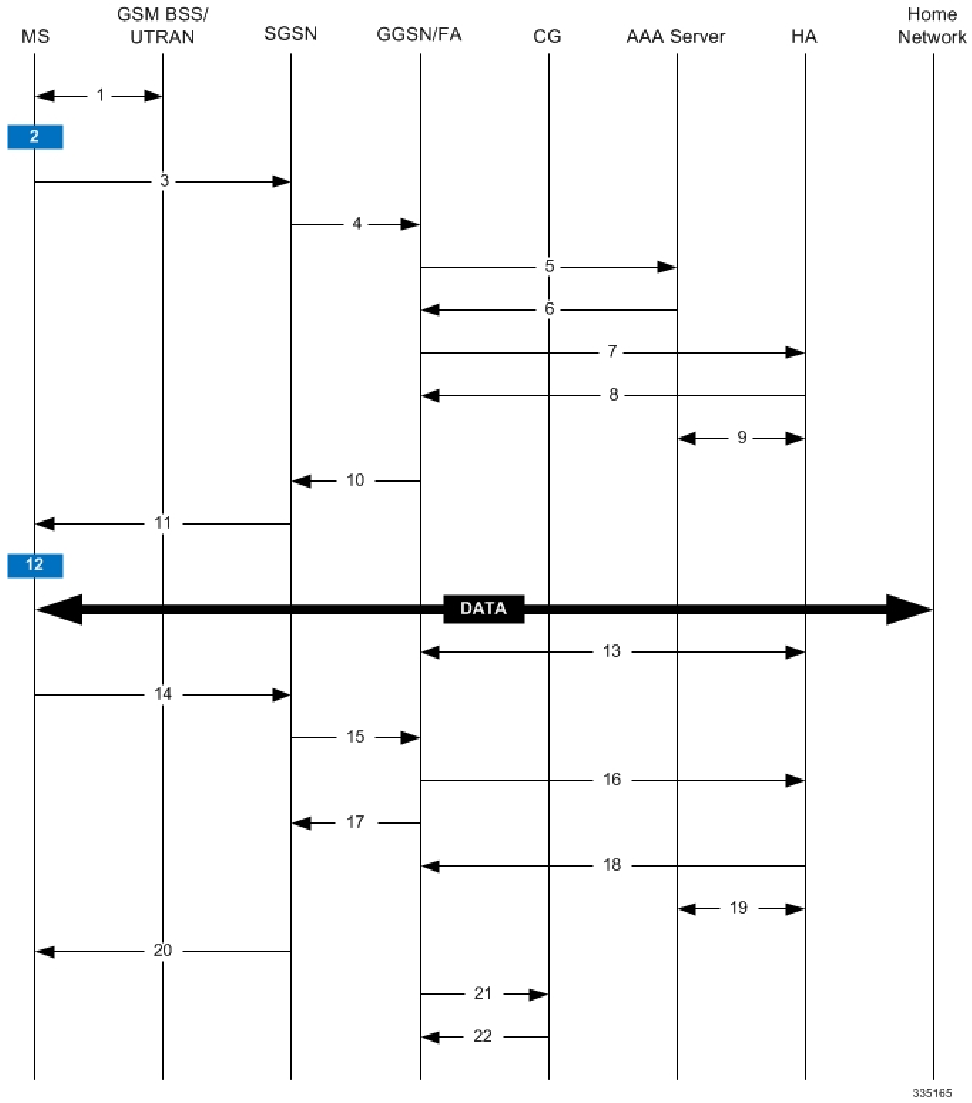


Table 10: Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

Step	Description
2	The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the MS to place it into PPP mode. The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information. Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.
3	The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.
4	The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signalling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).

Step	Description
5	The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact. Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings. If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to a AAA server.
6	If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.
7	If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
8	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
9	The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10	The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

Step	Description
11	The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
12	The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
13	The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
14	The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
15	The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16	The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
17	The GGSN returns a Delete PDP Context Response message to the SGSN.
18	The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19	The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20	The SGSN returns a Deactivate PDP Context Accept message to the MS.
21	The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.

Step	Description
22	For each accounting message received from the GGSN, the CG responds with an acknowledgement.

How Proxy Mobile IP Works in WiMAX Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and ASN GW/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.

Figure 16: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

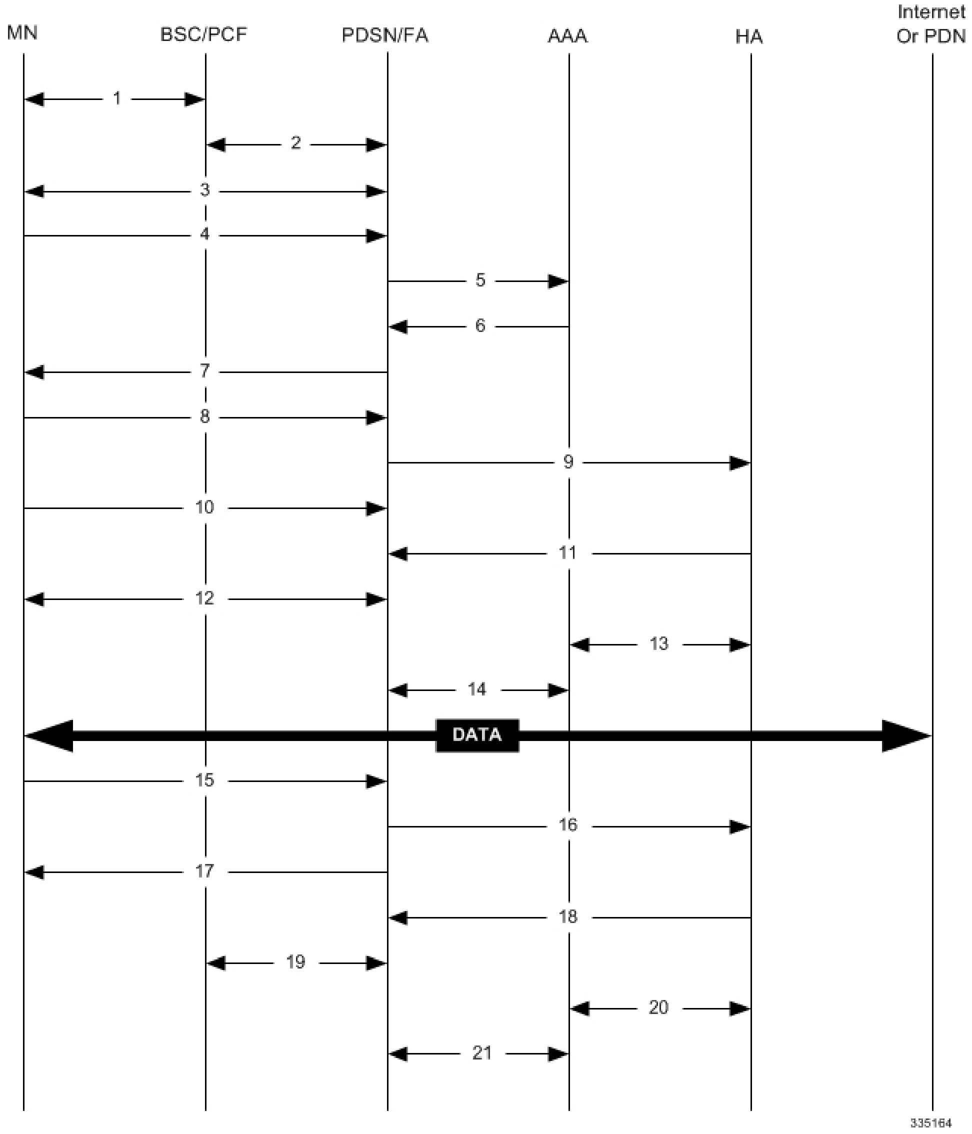


Table 11: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The ASN GW/FA sends a EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 17: HA Assigned IP Address Proxy Mobile IP Call Flow

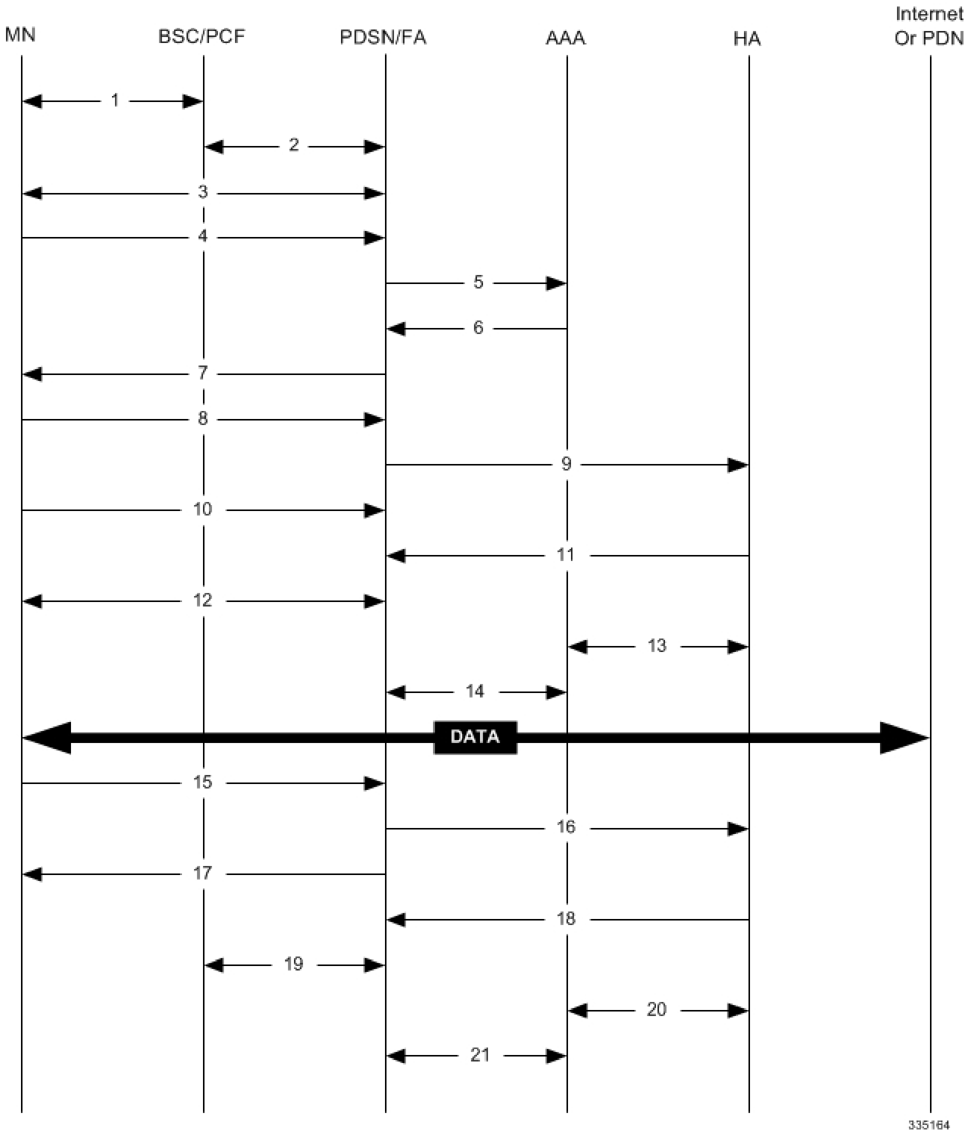


Table 12: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The ASN GW/FA sends an EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.

Step	Description
16	The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers. Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool.The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.

Figure 18: Proxy-MIP Call Setup using CHAP Authentication

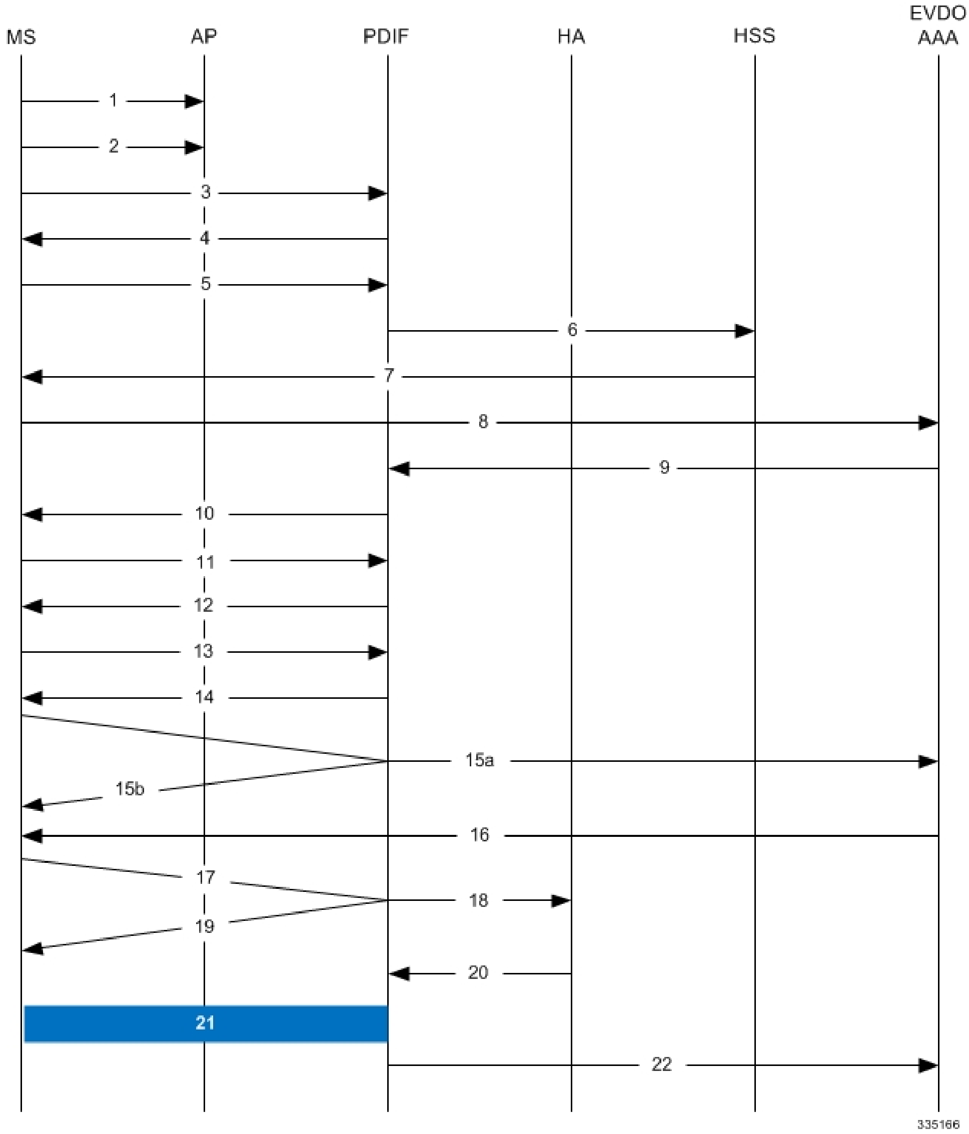


Table 13: Proxy-MIP Call Setup using CHAP Authentication

Step	Description
1	On connecting to WiFi network, MS first send DNS query to get PDIF IP address
2	MS receives PDIF address from DNS

Step	Description
3	MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.
4	PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP address in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDIF service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Response. PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.
5	On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload which contains the NAI, SA, TSi, TSr, CP (requesting IP address and DNS address) payloads. MS will not include AUTH payload to indicate that it will use EAP methods.
6	On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA servers are selected based on domain profile, default subscriber template or default domain configurations. PDIF includes Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details are explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Request from MS.
7	PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Payload AVP contents and sends IKE_ AUTH Response back to MS in the EAP payload. PDIF allows IDr and CERT configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is configured to do so.

Step	Description
8	MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AUTH Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challenge received from MS.
9	The AAA server sends the DEA back to the PDIF with Result-Code AVP as "success." The EAP-Payload AVP message also contains the EAP result code with "success." The DEA also contains the IMSI for the user, which is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions such as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.
10	PDIF sends the IKE_AUTH Response back to MS with the EAP payload.
11	MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed from the keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS Notify payload also.

Step	Description
12	PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH payload computed from the MSK. PDIF does not assign any IP address for the MS pending second authentication. Nor will the PDIF include any configuration payloads. a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify payload is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 session by sending INFORMATIONAL (Delete) Request.b. If ANOTHER_AUTH_FOLLOWS Notify payload is not present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. However, if **proxy-mip-required** is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ. When PDIF receives the Proxy-MIP RRP, it takes the Home Address (and DNS addresses if any) and sends the IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. In either case, IKEv2 setup will finish at this stage and IPSec tunnel gets established with a Tunnel Inner Address (TIA).
13	MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include the NAI. This NAI may be completely different from the NAI used in the first authentication.

Step	Description
14	On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second authentication methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP methods may be either EAP-Passthru or EAP-Terminated. a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload including challenge.b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC.c. MS processes the IKE_AUTH Response: • If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the challenge, compute the response and send IKE_AUTH Request with EAP payload including Challenge and Response. • If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the MS sends legacy-Nak with EAP-GTC.
15(a)	PDIF receives the new IKE_AUTH Request from MS. If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Access Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.).
15(b)	If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_AUTH Response with EAP-GTC.
16	PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.
17	PDIF receives the final IKE_AUTH Request with AUTH payload.
18	PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Agent if **proxy-mip-required** is enabled. The HA address may be received from the RADIUS server in the Access Accept (Step 16) or may be locally configured. PDIF may also remember the HA address from the first authentication received in the final DEA message.

Step	Description
19	If **proxy-mip-required** is disabled, PDIF assigns the IP address from the local pool.
20	PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.
21	PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also sets up the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by including the CP payload with the IP address and optionally the DNS addresses. This completes the setup.
22	PDIF sends a RADIUS Accounting start message.

Important For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.

Figure 19: Proxy-MIP Call Setup using PAP Authentication

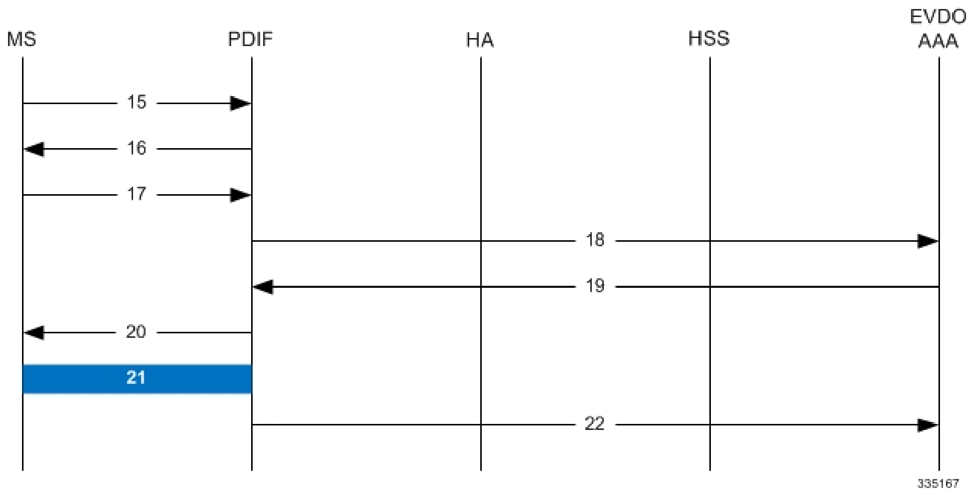


Table 14: Proxy-MIP Call Setup using PAP Authentication

Step	Description
15	MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.

Step	Description
16	PDIF then initiates EAP-GTC procedure, and requests a password from MS.
17	MS includes an authentication password in the EAP payload to PDIF.
18	Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Name attribute and PAP-password.
19	Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may include Framed-IP-Address attribute.
20	The attribute content in the Access Accept message is encoded as EAP payload with EAP success when PDIF sends the IKE_AUTH Response to the MS.
21	The MS and PDIF now have a secure IPSec tunnel for communication.
22	Pdif sends an Accounting START message.

Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:

Important Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip allow
 proxy-mip max-retransmissions <integer>
 proxy-mip retransmission-timeout <seconds>
 proxy-mip renew-percent-time percentage
 fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number
 { encrypted secret enc_secret | secret secret } [ description string ][
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | replay-protection {
timestamp | nonce } | timestamp-tolerance tolerance ]
authentication mn-ha allow-noauth
 end
```

Notes:

- The **proxy-mip max-retransmissions** command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- **proxy-mip retransmission-timeout** configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
- **proxy-mip renew-percent-time** configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of **600** seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after **300** seconds have passed.

- Use the **fa-ha-spi remote-address**command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the *Command Line Interface Reference* for the full command syntax.

Important Note that FA-HA SPIs **must** be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the **authentication mn-ha allow-noauth** command to configure the FA service to allow communications from the HA without authenticating the HA.

Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Proceed to the optional Configuring Proxy MIP HA Failover, on page 117 to configure Proxy MIP HA Failover support or skip to the *Configuring HA Services* to configure HA service support for Proxy Mobile IP.

Configuring Proxy MIP HA Failover

Use this example to configure Proxy Mobile IP HA Failover:

Important This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip ha-failover [ max-attempts <max_attempts> |
num-attempts-before-switching <num_attempts> | timeout <seconds> ]
```

Notes:

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

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

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

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

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

RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

Table 15: Required RADIUS Attributes for Proxy Mobile IP

Attribute	Description	Values
SN-Subscriber- Permission OR SN1-Subscriber- Permission	Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute **must** be set to Simple IP.	• None (0) • Simple IP (0x01) • Mobile IP (0x02) • Home Agent Terminated Mobile IP (0x04)
SN-Proxy-MIP OR SN1-Proxy-MIP	Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute **must** be enabled to support Proxy Mobile IP.	• Disabled **-** do not perform compulsory Proxy-MIP (0) • Enabled **-** perform compulsory Proxy-MIP (1)
SN-Simultaneous- SIP-MIP OR SN1-Simultaneous- SIP-MIP	Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services. **Note** Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will **not** allow simultaneous Simple IP and Mobile IP sessions for the MN.	• Disabled (0) • Enabled (1)

Attribute	Description	Values
SN-PDSN-Handoff- Req-IP-Addr OR SN1-PDSN-Handoff- Req-IP-Addr	Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.	• Disabled - do not reject (0) • Enabled - reject (1)
3GPP2-MIP-HA-Address	This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.	IPv4 Address

Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

```
configure
 context <context_name>
 subscriber name <subscriber_name>
 permission pdsn-simple-ip
 proxy-mip allow
 inter-pdsn-handoff require ip-address
 mobile-ip home-agent <ha_address>
 <optional> mobile-ip home-agent <ha_address> alternate
 ip context-name <context_name>
 end
```

Verify that your settings for the subscriber(s) just configured are correct.

```
show subscribers configuration username <subscriber_name>
```

Notes:

- Configure the system to enforce the MN\'s use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the **inter-pdsn-handoff require ip-address** command.
- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the **mobile-ip home-agent** *ha_address* alternate command to specify the secondary, or alternate HA.
- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

```
configure
 context <context-name>
 subscriber name <subscriber_name>
 proxy-mip require
```

Note

subscriber_name is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

```
configure
 context <context_name>
 ip context-name <context_name>
 end
```

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

Configuring APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.

Important This is an optional configuration. In addition, attributes returned from the subscriber's profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

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

```
[local]host_name
```

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

```
configure
```

The following prompt appears:

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

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

```
context <context_name>
```

context_name is the name of the system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.The following prompt appears:

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

Step 3 Enter the configuration mode for the desired APN by entering the following command:

```
apn <apn_name>
```

apn_name is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).The following prompt appears:

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

Step 4 Enable proxy Mobile IP for the APN by entering the following command:

```
proxy-mip required
```

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

Step 5 *Optional.* GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:

```
proxy-mip null-username static-homeaddr
```

This command will enables the accepting of MIP Registration Request without NAI extensions in this APN.

Step 6 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local]host_name
```

Step 7 Repeat *step 1* through *step 6* as needed to configure additional APNs.

Step 8 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a detailed listing of configured APN parameter settings.

Step 9 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

CHAPTER 9

Traffic Policing and Shaping

This chapter describes the support of per subscriber Traffic Policing and Shaping feature on Cisco's Chassis and explains the commands and RADIUS attributes that are used to implement this feature. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

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

The following topics are included:

Overview

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

- Traffic Policing
- Traffic Shaping

Traffic Policing

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

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

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

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

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

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

Traffic Shaping

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

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

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

Traffic Policing Configuration

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

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

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

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

Configuring Subscribers for Traffic Policing

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

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

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

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

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

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

Notes:

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

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

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

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

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN for Traffic Policing in 3GPP Networks

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

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

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

Table 16: Permitted Values for Committed and Peak Data Rates in GTP Messages

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

Step 1 Set parameters by applying the following example configurations:

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

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

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

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

Notes:

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

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

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

- Repeat as needed to configure additional Qos Traffic Policing profiles.

Important If a "subscribed" traffic class is received, the system changes the class to background and sets the following: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

Step 2 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Traffic Shaping Configuration

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

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

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

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

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

Configuring Subscribers for Traffic Shaping

This section provides information and instructions for configuring local subscriber profiles on the system to support Traffic Shaping.

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

Step 1 Set parameters by applying the following example configurations:

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

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

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

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

Notes:

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

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

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

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

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN for Traffic Shaping in 3GPP Networks

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

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

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

Table 17: Permitted Values for Committed and Peak Data Rates in GTP Messages 0

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

Step 1 Set parameters by applying the following example configurations.

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

```
configure
    context <context_name>
        subscriber name <user_name>
            qos rate-limit downlink
            end
```

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

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

Step 2 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

RADIUS Attributes

Traffic Policing for CDMA Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for CDMA subscribers (PDSN, HA) configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 18: RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers

Attribute	Description
SN-QoS-Tp-Dnlk (or SN1-QoS-Tp-Dnlk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Dnlk-Committed-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink committed-data-rate in bps.
SN-Tp-Dnlk-Peak-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink peak-data-rate in bps.
SN-Tp-Dnlk-Burst-Size (or SN1-Tp-Dnlk-Burst-Size)	Specifies the downlink-burst-size in bytes. **NOTE:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Dnlk-Exceed-Action (or SN1-Tp-Dnlk-Exceed-Action)	Specifies the downlink exceed action to perform.
SN-Tp-Dnlk-Violate-Action (or SN1-Tp-Dnlk-Violate-Action)	Specifies the downlink violate action to perform.
SN-QoS-Tp-Uplk (or SN1-QoS-Tp-Uplk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink committed-data-rate in bps.

Attribute	Description
SN-Tp-Uplk-Peak-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink peak-data-rate in bps.
SN-Tp-Uplk-Burst-Size (or SN1-Tp-Uplk-Burst-Size)	Specifies the uplink-burst-size in bytes. **Note** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Uplk-Exceed-Action (or SN1-Tp-Uplk-Exceed-Action)	Specifies the uplink exceed action to perform.
SN-Tp-Uplk-Violate-Action (or SN1-Tp-Uplk-Violate-Action)	Specifies the uplink violate action to perform.

Traffic Policing for UMTS Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for UMTS subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 19: RADIUS Attributes Required for Traffic Policing Support for UMTS Subscribers

Attribute	Description
SN-QoS-Conversation-Class (or SN1-QoS-Conversation-Class)	Specifies the QOS Conversation Traffic Class.
SN-QoS-Streaming-Class (or SN1-QoS-Streaming-Class)	Specifies the QOS Streaming Traffic Class.
SN-QoS-Interactive1-Class (or SN1-QoS-Interactive1-Class)	Specifies the QOS Interactive Traffic Class.
SN-QoS-Interactive2-Class (or SN1-QoS-Interactive2-Class)	Specifies the QOS Interactive2 Traffic Class.
SN-QoS-Interactive3-Class (or SN1-QoS-Interactive3-Class)	Specifies the QOS Interactive3 Traffic Class.
SN-QoS-Background-Class (or SN1-QoS-Background-Class)	Specifies the QOS Background Traffic Class.

Attribute	Description
SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)	This compound attribute simplifies sending QoS values for Traffic Class (the above attributes), Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.

APPENDIX A

HSGW Engineering Rules

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

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.

Important For releases 15.0 and earlier, mag-service can only bind with IPv6 address. For releases 16.0 and forward, mag-service is capable of binding with IPv6 and IPv4 interfaces.

- 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.

Important 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.