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

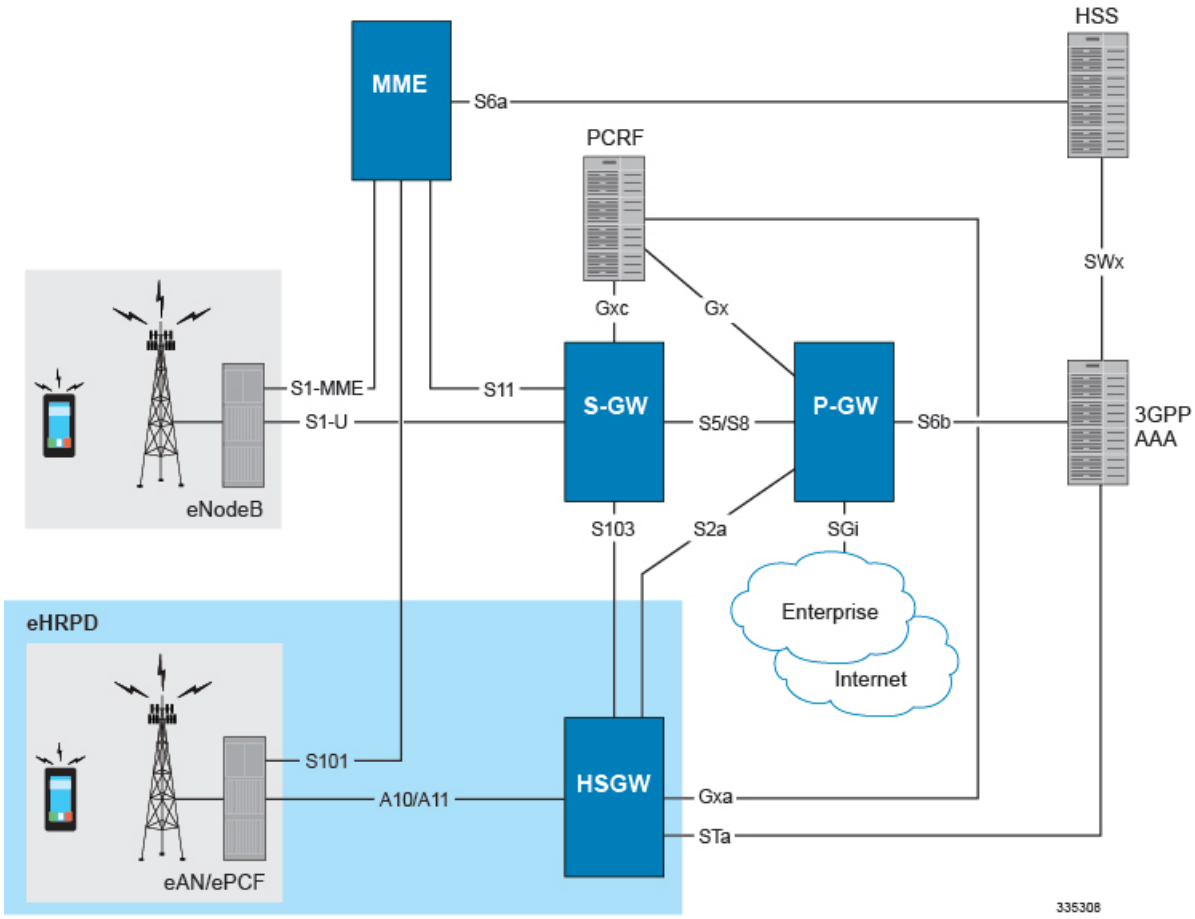
The HSGW provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE (4G System Architecture Evolution) core network and performs the following functions:

- 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*.

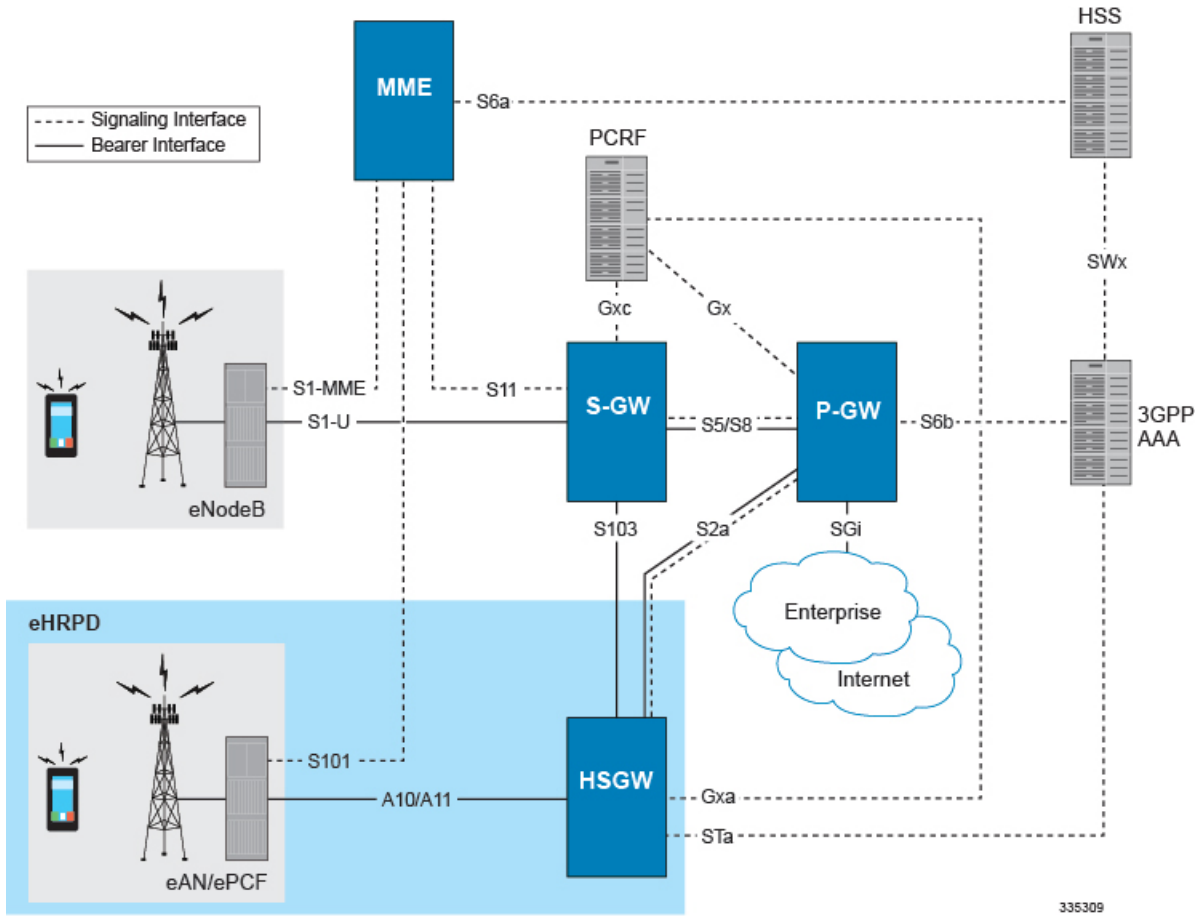
Network Deployment

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.

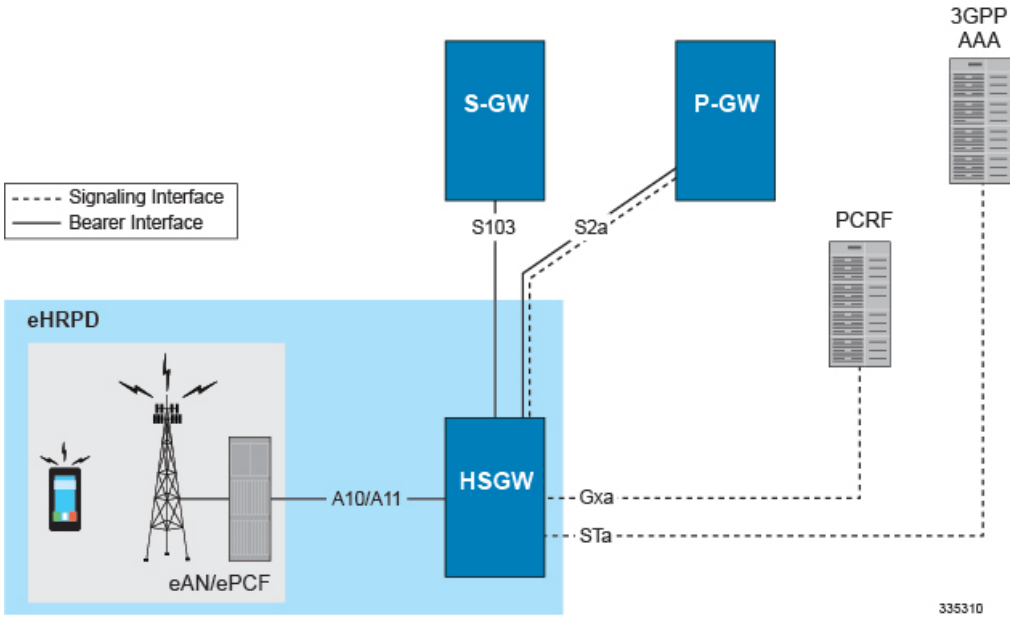
Figure 2: HSGW in an eHRPD Network Architecture



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

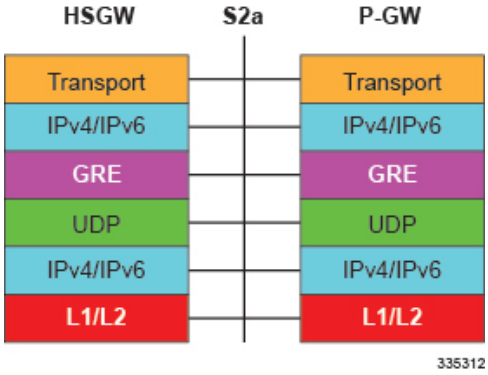
This interface exists between the Evolved Access Network/Evolved Packet Control Function (eAN/ePCF) and the HSGW and implements the A10 (bearer) and A11 (signaling) protocols defined in 3GPP2 specifications.

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

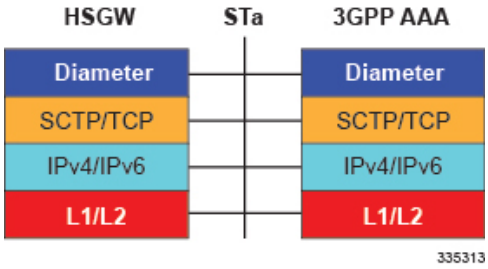


STa Interface

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

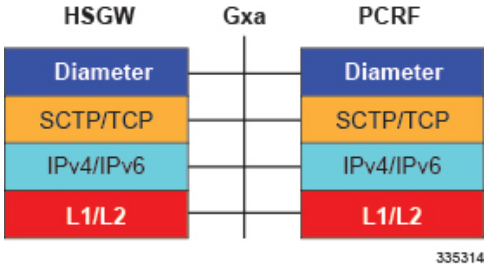


Gxa Interface

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

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.

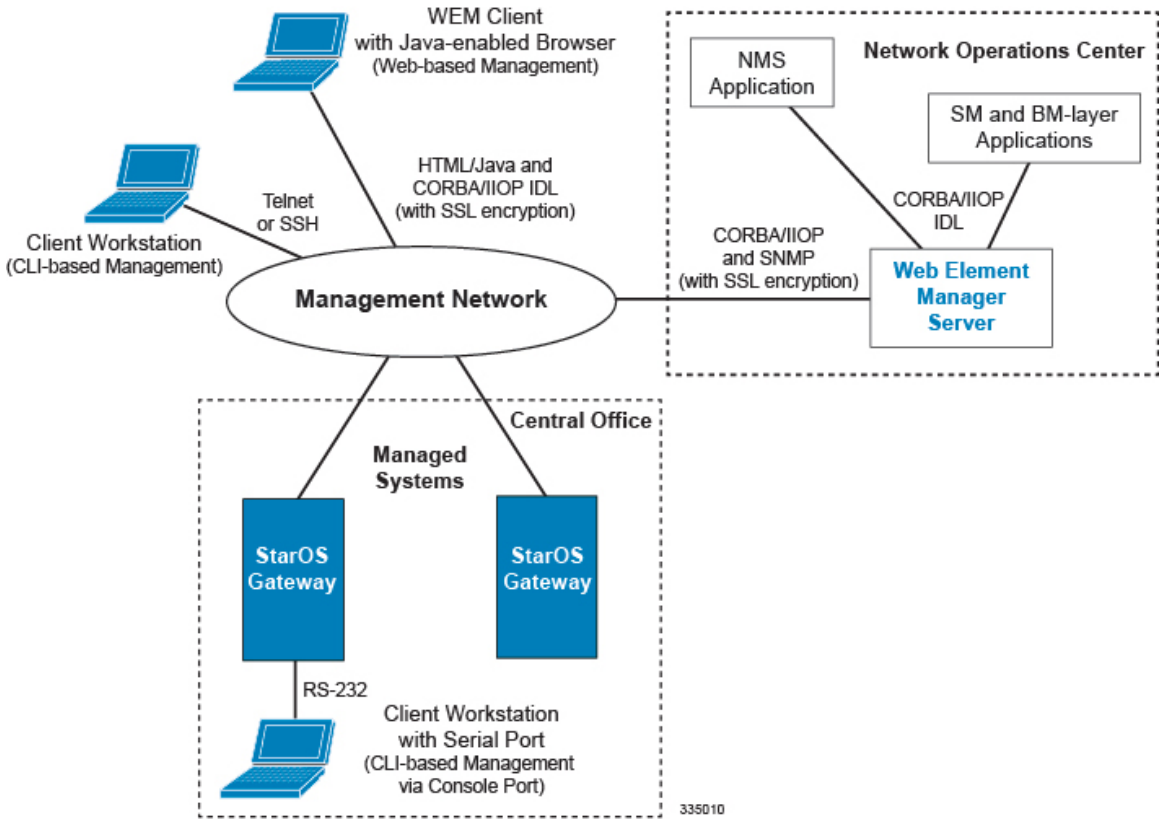
Cisco Systems' O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

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

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

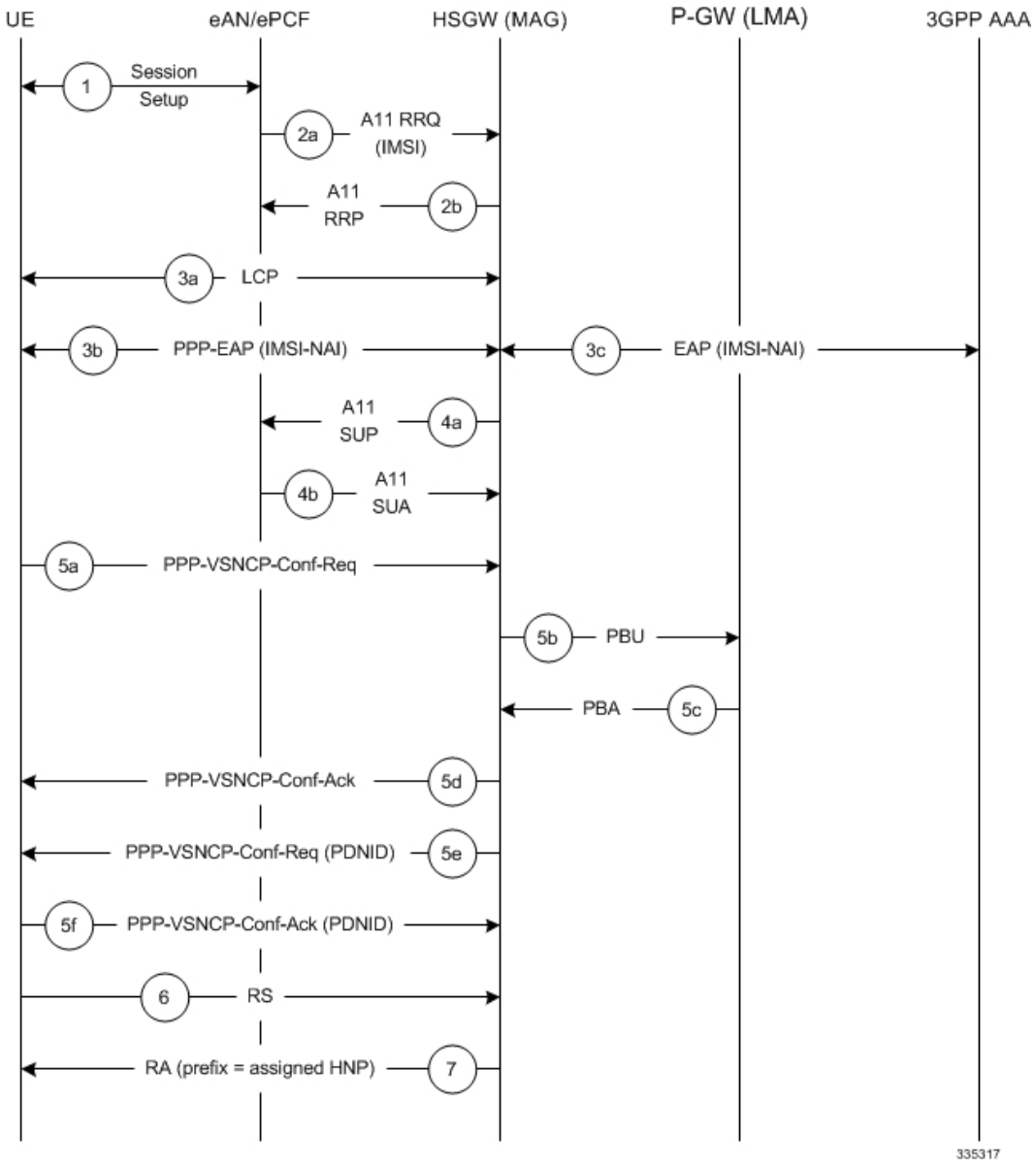


Table 2: Initial Attach with IPv6/IPv4 Access Call Flow Description

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

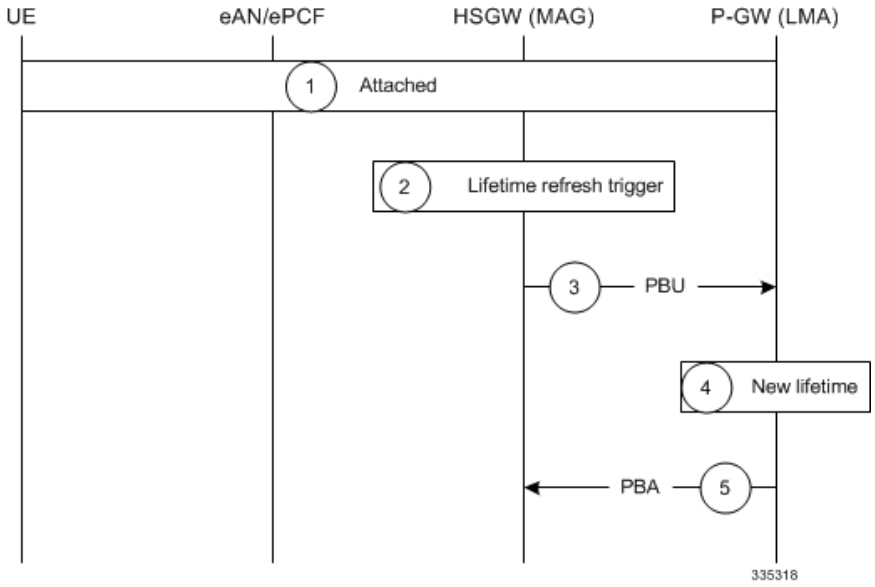


Table 3: PMIPv6 Lifetime Extension (without handover) Call Flow Description

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

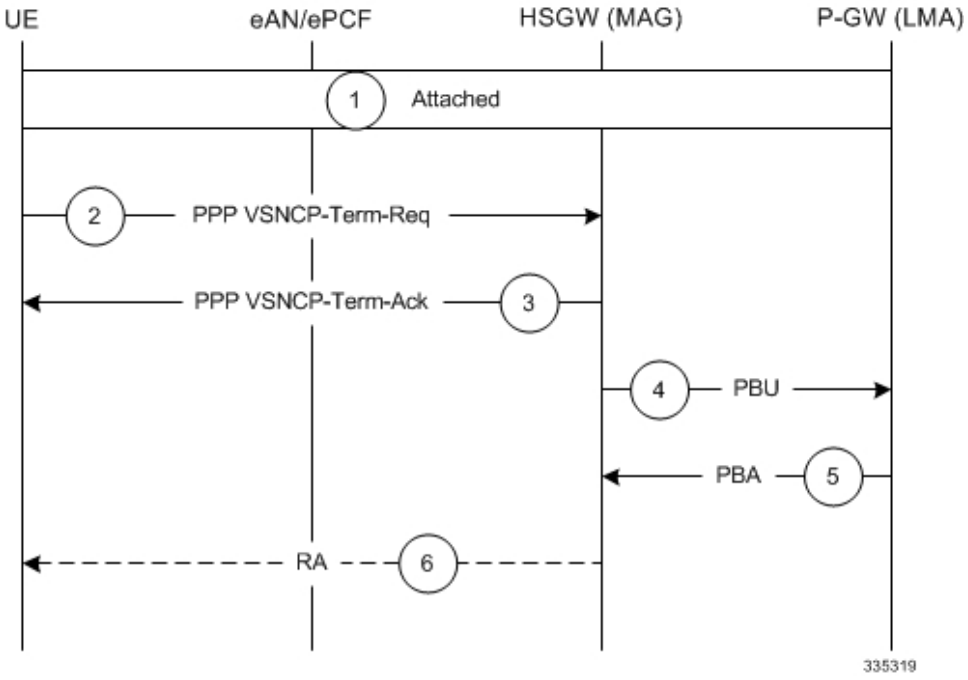


Table 4: PDN Connection Release by the UE Call Flow Description

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

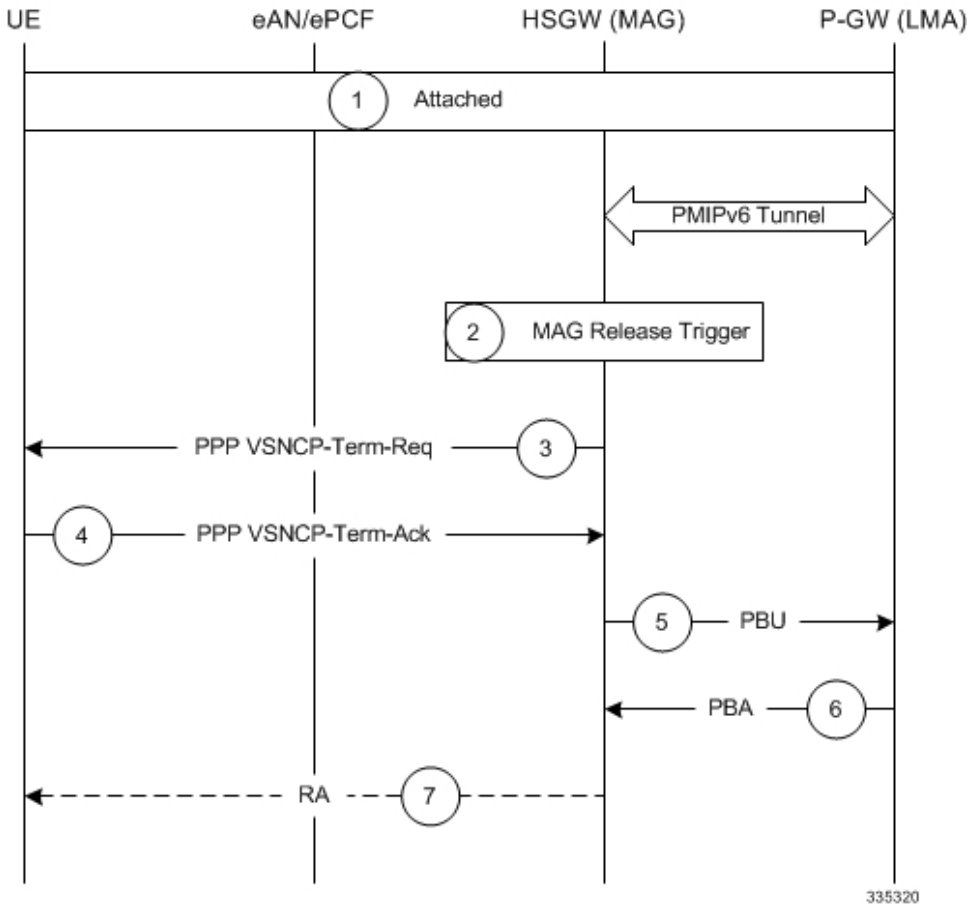


Table 5: PDN Connection Release by the HSGW Call Flow Description

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

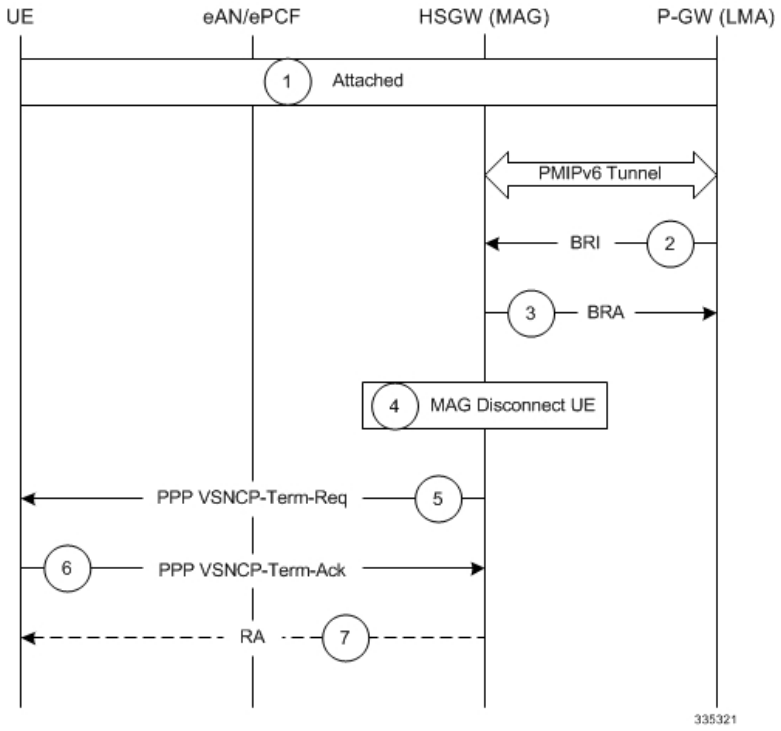


Table 6: PDN Connection Release by the P-GW Call Flow Description

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