E-UTRAN - eHRPD
Connectivity and Interworking: Core Network Aspects
# REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description of Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev 0 v1.0</td>
<td>Initial publication (3GPP Rel 8 alignment)</td>
<td>April 2009</td>
</tr>
<tr>
<td>Rev 0 v2.0</td>
<td>Revision 0 Version 2.0</td>
<td>December 2009</td>
</tr>
<tr>
<td>Rev 0 v3.0</td>
<td>Revision 0 Version 3.0</td>
<td>September 2010</td>
</tr>
<tr>
<td>Rev A v1.0</td>
<td>Revision A (3GPP Rel 9 alignment)</td>
<td>April 2011</td>
</tr>
<tr>
<td>Rev A v2.0</td>
<td>Revision A Version 2.0</td>
<td>October 2012</td>
</tr>
</tbody>
</table>
E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

CONTENTS

1 Introduction .......................................................................................................................... 1
  1.1 Scope ............................................................................................................................ 1
  1.2 Document Convention ................................................................................................. 1
  1.3 References .................................................................................................................... 2
    1.3.1 Normative References .......................................................................................... 2

2 Definitions, Symbols and Abbreviations ............................................................................. 7
  2.1 Definitions ..................................................................................................................... 7
    2.1.1 Symbols and Abbreviations .................................................................................. 10

3 E-UTRAN - eHRPD Connectivity and Interworking Architecture ........................................ 13
  3.1 E-UTRAN – eHRPD Interworking Non-Roaming Architecture ...................................... 13
  3.2 E-UTRAN – eHRPD Interworking Roaming Architecture (Home-Routed Traffic) ............. 14
  3.3 E-UTRAN – eHRPD Interworking Roaming Architecture (Local Breakout) ..................... 15
  3.4 Reference Points .......................................................................................................... 16
    3.4.1 H1/H2 Reference Points ....................................................................................... 16
    3.4.2 Gxa Reference Point ............................................................................................. 16
    3.4.3 Pi* Reference Point ............................................................................................... 16
    3.4.4 S101 Reference Point ........................................................................................... 16
    3.4.5 S103 Reference Point ........................................................................................... 16
    3.4.6 S2a Reference Point ............................................................................................... 16
    3.4.7 STa Reference Point ............................................................................................... 17
  3.5 Protocol Stacks Between the UE and the HSGW ............................................................ 18
    3.5.1 User Plane .............................................................................................................. 18
    3.5.2 Control Plane ......................................................................................................... 22
  3.6 H1/H2 Interface Protocol Stacks ................................................................................... 24
  3.7 Control Plane HSGW to P-GW – PMIPv6 ...................................................................... 26

4 eHRPD Functionality ........................................................................................................... 27
  4.1 General HSGW Capabilities ........................................................................................ 27
  4.2 Authentication and Subscription Information Retrieval ................................................ 28
    4.2.1 EAP Protocol Negotiation .................................................................................... 28
    4.2.2 UE Requirements ................................................................................................. 29
    4.2.3 HSGW Requirements ......................................................................................... 30
    4.2.4 3GPP AAA Server Requirements ....................................................................... 31
    4.2.5 Authentication Call Flows .................................................................................... 31
  4.3 Use of EAP-AKA’ – Fast Re-Authentication ................................................................ 35
  4.4 IP Address Allocation .................................................................................................. 35
    4.4.1 General .................................................................................................................. 35
    4.4.2 IPv4 Address Allocation during Default and Additional PDN Connection Establishment ................................................................................................................. 41
    4.4.3 IPv6 Prefix Allocation via IPv6 Stateless Address Auto-configuration ...................... 41
15.4.1 Behavior of the HSGW .............................................................. 240
15.4.2 Behavior of the 3GPP2 AAA Proxy/Server .................................. 241
15.4.3 Result-Code and Experimental-Result AVP values ...................... 242
15.4.4 AVPs ...................................................................................... 243
15.4.5 Service-Option-Profile ............................................................. 244
15.4.6 Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort-Traffic 244
15.4.7 Authorized-Flow-Profile-IDs-for-the-User ................................... 244
15.4.8 Inter-User-Priority ................................................................. 244
15.4.9 Maximum-Per-Flow-Priority-for-the-User ................................... 245
15.4.10 ProfileID-Forward .................................................................. 245
15.4.11 ProfileID-Reverse ................................................................... 245
15.4.12 ProfileID-Bi-Directional ......................................................... 245
15.4.13 Max-Link-Flows .................................................................... 245
15.4.14 Service-Option-Number ......................................................... 245

16  Annex A (Informative) – Mapping QoS between 3GPP and 3GPP2 .................................................. 246
17  Annex B (Informative) – Mapping Gxa Parameters between 3GPP and 3GPP2 ...................................... 251
18  Annex C (Informative) – CDR Parameters Supported for Offline Charging ........................................ 255
19  Annex D (Normative) – 3GPP2 Subscriber QoS Profile Parameters ........................................................ 258
LIST OF FIGURES

Figure 1   E-UTRAN - eHRPD Interworking Non-Roaming Architecture.................................13
Figure 2   E-UTRAN – eHRPD Interworking – Roaming Architecture (Home-Routed Traffic) .........................................................14
Figure 3   E-UTRAN – eHRPD Interworking – Roaming Architecture (Local Breakout) .............15
Figure 4   Protocol stack for traffic multiplexed on an SO72 Auxiliary Connection ..............18
Figure 5   Protocol stack for non-multiplexed traffic on an Auxiliary Connection ..............19
Figure 6   Main Service Connection User-Plane Protocol Stack via SO59 .........................20
Figure 7   SO64 Auxiliary Service Connection User-Plane Protocol Stack ......................21
Figure 8   Main Service Connection Protocol Stack for EAP ........................................22
Figure 9   Main Service Connection Control Plane Protocol Stack for VSNCP ...................22
Figure 10  RSVP Over the Main Service Connection Using VSNP ..................................23
Figure 11  H1 Interface Control Plane Protocol Stack ......................................................24
Figure 12  H2 Interface Downlink User Plane Protocol Stack .........................................25
Figure 13  H2 Interface Uplink User Plane Protocol Stack ..............................................26
Figure 14  EAP-AKA’ Authentication for eHRPD ............................................................32
Figure 15  IPv4 address allocation during PDN connection establishment ......................44
Figure 16  IPv4 Address Allocation using DHCPv4 with Rapid Commit Option ..............46
Figure 17  IPv4 Address Allocation using DHCPv4 without Rapid Commit Option ............48
Figure 18  IPv6 Address Allocation ..............................................................................50
Figure 19  Sample Bearer Mapping in eHRPD .................................................................53
Figure 20  Network Initiated Dedicated Bearer Setup ......................................................56
Figure 21  PCRF Initiated Dedicated Bearer Deactivation .................................................58
Figure 22  UE Requested Bearer Resource Allocation .....................................................59
Figure 23  UE Requested Radio Bearer State Modification ..............................................62
Figure 24  HSGW Policy Enforcement ............................................................................63
Figure 25  Already Authenticated UE Attach Procedure for Emergency Services ..........74
Figure 26  Not-Authenticated UE Attach Procedure for Emergency Services ................76
Figure 27  PCRF Initiated Detach Procedure for Emergency Services ............................79
Figure 28  P-GW Initiated Disconnect Procedure for Emergency PDN Connection ..........81
Figure 29  UE Requested Bearer Resource Allocation .....................................................83
Figure 30  Network Initiated Dedicated Bearer Setup ......................................................85
Figure 31  UE Initiated Emergency Bearer Removal .......................................................87
Figure 32  PCRF Initiated Dedicated Bearer Deactivation .................................................88
Figure 33  eHRPD Pre-registration via E-UTRAN ..........................................................90
Figure 34  Active Mode Optimized Handoff E-UTRAN to eHRPD .................................93
Figure 35  Non-Optimized Handoff: No Existing eHRPD Session ..................................96
Figure 36  Partial Context Establishment on eHRPD without PMIP Tunnel .....................99
Figure 37  S2a Connection Establishment with the Default PDN ....................................104
Figure 38  Initial attachment over S2a ..........................................................................118
Figure 39  Auxiliary service connections .....................................................................154
Figure 40  UE Requested PDN Connectivity ................................................................155
Figure 41  UE Initiated PDN Disconnection Procedure ..................................................159
Figure 42  UE Initiated Detach Procedure ....................................................................161
Figure 43  HSS/AAA Initiated UE Detach Procedure .....................................................163
Figure 44  HSGW Initiated UE Detach Procedure ..........................................................165
Figure 45  HSS/AAA Initiated PDN Disconnection Procedure .............................................. 167
Figure 46  P-GW Initiated PDN Disconnection Procedure ..................................................... 169
Figure 47  HSGW Initiated PDN Disconnection Procedure ..................................................... 171
Figure 48  P-GW Initiated Resource Deactivation ................................................................. 173
Figure 49  Inter-HSGW Interworking Architecture in eHRPD ............................................... 176
Figure 50  Inter-HSGW Context Transfer ............................................................................. 178
Figure 51  Handoff when the UE is Dormant on the eHRPD Radio ....................................... 182
Figure 52  Intra-eHRPD Handoff with HSGW Relocation without Context Transfer ............ 185
Figure 53  eHRPD Pre-registration via E-UTRAN ................................................................. 214
Figure 54  Active Mode Optimized Handoff E-UTRAN to eHRPD ........................................ 217
Figure 55  Idle Mode Optimized Handoff from E-UTRAN to eHRPD ................................... 220
Figure 56  Non-Optimized Handoff from E-UTRAN to eHRPD – Partial HSGW Context .... 222
Figure 57  Non-Optimized Handoff – Null HSGW Context .................................................... 225
Figure 58  Non-Optimized Handoff: No Existing eHRPD Session ......................................... 227
Figure 59  eHRPD to E-UTRAN Non-Optimized Idle Handoff ............................................. 229
Figure 60  eHRPD to E-UTRAN Non-Optimized Active Handoff .......................................... 231
Figure 61  Retrieval of Subscriber QoS Profile Information from 3GPP2 AAA – During Authentication ........................................................................................................... 234
Figure 62  Retrieval of Subscriber QoS Profile Information from 3GPP2 AAA – Intra-eHRPD Handoff with HSGW Relocation with Context Transfer ........................................... 236
Figure 63  Flow ID and QCI Applicability .............................................................................. 247
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table 1</th>
<th>3GPP2 Diameter AVPs</th>
<th>...................................................................................................................................... 65</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2</td>
<td>Features of Feature-List-ID = “Query Group” Defined for the Pi*3GPP2 Diameter Application</td>
<td>.................................................................................................................................... 111</td>
</tr>
<tr>
<td>Table 3</td>
<td>3GPP2 VSNCP packet format</td>
<td>..................................................................................................................................... 123</td>
</tr>
<tr>
<td>Table 4</td>
<td>VSNCP Configuration Options</td>
<td>................................................................................................................................... 124</td>
</tr>
<tr>
<td>Table 5</td>
<td>Error Code values</td>
<td>.................................................................................................................................. 126</td>
</tr>
<tr>
<td>Table 6</td>
<td>Address Allocation Cause values</td>
<td>.................................................................................................................................. 126</td>
</tr>
<tr>
<td>Table 7</td>
<td>Configuration Option Data Format</td>
<td>.................................................................................................................................. 127</td>
</tr>
<tr>
<td>Table 8</td>
<td>3GPP2 VSNP packet format</td>
<td>.................................................................................................................................... 133</td>
</tr>
<tr>
<td>Table 9</td>
<td>3GPP2 VSNP extended packet format</td>
<td>.................................................................................................................................. 133</td>
</tr>
<tr>
<td>Table 10</td>
<td>3GPP2 VSNP Extend Codes and Data Field Contents</td>
<td>.................................................................................................................................. 134</td>
</tr>
<tr>
<td>Table 11</td>
<td>TFT Error Codes</td>
<td>.................................................................................................................................. 140</td>
</tr>
<tr>
<td>Table 12</td>
<td>3GPP2 OBJECT</td>
<td>.................................................................................................................................. 141</td>
</tr>
<tr>
<td>Table 13</td>
<td>3GPP2 OBJECT-IE List</td>
<td>.................................................................................................................................. 142</td>
</tr>
<tr>
<td>Table 14</td>
<td>3GPP2 OBJECT-IE Type #</td>
<td>.................................................................................................................................. 142</td>
</tr>
<tr>
<td>Table 15</td>
<td>TFT IPv4 IE Type# = 0</td>
<td>.................................................................................................................................. 143</td>
</tr>
<tr>
<td>Table 16</td>
<td>TFT IPv6 IE Type# = 2</td>
<td>.................................................................................................................................. 143</td>
</tr>
<tr>
<td>Table 17</td>
<td>TFT OpCodes</td>
<td>.................................................................................................................................. 145</td>
</tr>
<tr>
<td>Table 18</td>
<td>QoS List Layout</td>
<td>.................................................................................................................................. 146</td>
</tr>
<tr>
<td>Table 19</td>
<td>Result Code Values</td>
<td>.................................................................................................................................. 148</td>
</tr>
<tr>
<td>Table 20</td>
<td>List of MS Capabilities</td>
<td>.................................................................................................................................. 152</td>
</tr>
<tr>
<td>Table 21</td>
<td>List of PDSN Capabilities</td>
<td>.................................................................................................................................. 152</td>
</tr>
<tr>
<td>Table 22</td>
<td>LCP Echo-Request packet format</td>
<td>.................................................................................................................................. 157</td>
</tr>
<tr>
<td>Table 23</td>
<td>3GPP2 Vendor Specific Information Element Structure for the LCP Echo-Request packet</td>
<td>.................................................................................................................................. 158</td>
</tr>
<tr>
<td>Table 24</td>
<td>Information Element Identifier for 3GPP2 Vendor Specific Information Element Structure in the LCP Echo-Request packet</td>
<td>.................................................................................................................................. 158</td>
</tr>
<tr>
<td>Table 25</td>
<td>Format of Context Parameter TLVs</td>
<td>.................................................................................................................................. 188</td>
</tr>
<tr>
<td>Table 26</td>
<td>User NAI TLV</td>
<td>.................................................................................................................................. 189</td>
</tr>
<tr>
<td>Table 27</td>
<td>User MSID TLV</td>
<td>.................................................................................................................................. 189</td>
</tr>
<tr>
<td>Table 28</td>
<td>LCP Info TLV</td>
<td>.................................................................................................................................. 190</td>
</tr>
<tr>
<td>Table 29</td>
<td>CCP Info TLV</td>
<td>.................................................................................................................................. 191</td>
</tr>
<tr>
<td>Table 30</td>
<td>VSNCP State and Common Info TLV</td>
<td>.................................................................................................................................. 191</td>
</tr>
<tr>
<td>Table 31</td>
<td>PDN Info TLV</td>
<td>.................................................................................................................................. 192</td>
</tr>
<tr>
<td>Table 32</td>
<td>PCO Info TLV</td>
<td>.................................................................................................................................. 192</td>
</tr>
<tr>
<td>Table 33</td>
<td>PDN Address Info TLV</td>
<td>.................................................................................................................................. 193</td>
</tr>
<tr>
<td>Table 34</td>
<td>PMIPv6 Info TLV</td>
<td>.................................................................................................................................. 195</td>
</tr>
<tr>
<td>Table 35</td>
<td>ROHC Configuration Info TLV</td>
<td>.................................................................................................................................. 196</td>
</tr>
<tr>
<td>Table 36</td>
<td>ROHC IR Info TLV</td>
<td>.................................................................................................................................. 197</td>
</tr>
<tr>
<td>Table 37</td>
<td>QoS Info TLV</td>
<td>.................................................................................................................................. 197</td>
</tr>
<tr>
<td>Table 38</td>
<td>TFTv4 Info TLV</td>
<td>.................................................................................................................................. 198</td>
</tr>
<tr>
<td>Table 39</td>
<td>TFTv6 Info TLV</td>
<td>.................................................................................................................................. 199</td>
</tr>
<tr>
<td>Table 40</td>
<td>AAA Profile Info TLV</td>
<td>.................................................................................................................................. 199</td>
</tr>
<tr>
<td>Table 41</td>
<td>Gxa Info TLV</td>
<td>.................................................................................................................................. 200</td>
</tr>
<tr>
<td>Table 42</td>
<td>Vendor Specific Info TLV</td>
<td>.................................................................................................................................. 200</td>
</tr>
<tr>
<td>Table 43</td>
<td>MSK Info TLV</td>
<td>.................................................................................................................................. 201</td>
</tr>
</tbody>
</table>
FOREWORD

(This foreword is not part of this document.)

This document was prepared by 3GPP2 TSG-X. It describes the attachment of cdma2000® eHRPD (evolved High Rate Packet Data) systems to the 3GPP EPC (Enhanced Packet Core).

This document is the second version of revision A of this specification.

This document is aligned with 3GPP release 9.

This document contains portions of material copied from 3GPP document number(s):

TS 23.401

TS 23.402

TS 33.402

The copyright on the 3GPP documents is owned by the Organizational Partners of 3GPP (ARIB - Association of Radio Industries and Businesses, Japan; CCSA - the China Communications Standards Association, China; ETSI – European Telecommunications Standards Institute; ATIS, USA- Alliance for Telecommunication Industry Solutions; TTA - Telecommunications Technology Association, Korea; and TTC – Telecommunication Technology Committee, Japan), which have granted license for reproduction and for use by 3GPP2 and its Organizational Partners.

This document is subject to change following formal approval. Should this document be modified, it will be re-released with a change of release date and an identifying change in version number as follows:

X.S0057-X version n.0

where:

X is an uppercase numerical or alphabetic character [0, A, B, C, …] that represents the revision level.

n is a numeric string [1, 2, 3, …] that indicates a point release level.

---

1 cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.
1 Introduction

This document provides a specification of the functions and interfaces of the evolved High Rate Packet Data (eHRPD) Serving Gateway (HSGW) and the IP level interfaces of the eHRPD user equipment (UE).

The eHRPD network provides an IP environment that supports attachment to multiple Packet Data Networks (PDNs) and allocation of IPv4 address or IPv6 address or both IPv4 and IPv6 addresses for each PDN via the 3GPP Evolved Packet Core (EPC). The UE uses network-based mobility and relies on the use of Proxy Mobile IPv6 (PMIPv6) within the network for mobility management.

1.1 Scope

The scope of this document covers support for an evolved access terminal (UE as known in this specification) using the eHRPD air interface and the S101 tunnel to access the core network architecture defined in 3GPP TS 23.401 [22] and TS 23.402 [23]. Specifically, this specification covers:

- An interface between the HRPD Serving Gateway (HSGW) and the Packet Data Network Gateway (P-GW, also known as PDN GW) and procedures for that interface.
- An interface between the UE and the HSGW and procedures for that interface.
- An interface between the HSGW and the PCRF and procedures for that interface.
- An interface between the HSGW and the AAA and procedures for that interface.
- Internal functions and responsibilities of the HSGW.
- Interfaces between HSGWs to support inter-HSGW handoff procedures.
- An interface from the S-GW to the HSGW to support data forwarding during handoff from E-UTRAN to eHRPD.
- Interfaces between the HSGW and the eAN/ePCF.

1.2 Document Convention

“Shall” and “shall not” identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the standard. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical, or causal.

All fields that are marked as “Reserved” shall be filled with zeros by the sender of that field, and shall be ignored by the receiver of that field.
1.3 References

1.3.1 Normative References

This section provides references to other specifications and standards that are necessary to implement this document.

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.


[17] **3GPP**: SC.R4002-0 v8.0: GHA (Global Hexadecimal Administrator) Assignment Guidelines and Procedures for Mobile Equipment Identifier (MEID) and Short Form Expanded UIM Identifier (SF_EUIMID), April 2012.


[20] **3GPP**: TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2 (Release 9).


[24] **3GPP**: TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 9).


[26] **3GPP**: TS 24.302: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3; (Release 9).


[28] **3GPP**: TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet-based services and Packet Data Networks (PDN), (Release 9).

[29] **3GPP**: TS 29.212: Policy and charging control over Gx reference point, (Release 9).


[31] **3GPP**: TS 29.214: Policy and charging control over Rx reference point; (Release 9).

[32] **3GPP**: TS 29.229: Cx and Dx Interfaces based on the Diameter Protocol; Protocol Details; (Release 9).

[33] **3GPP**: TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol; (Release 9).
[34] **3GPP**: TS 29.273: 3GPP EPS AAA Interfaces, (Release 9).

[35] **3GPP**: TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3 (Release 9).


[38] **3GPP**: TS 32.251: Charging Management; Packet Switched (PS) domain charging (Release 9).

[39] **3GPP**: TS 32.299: Telecommunication Management; Charging Management; Diameter Charging Applications (Release 9).

[40] **3GPP**: TS 32.422: Subscriber and equipment trace; Trace control and configuration management (Release 9).

[41] **3GPP**: TS 33.102: 3G Security; Security architecture (Release 9).


[56] **IETF**: RFC 2890: Dommety, “Key and Sequence Number Extensions to GRE”, September 2000.


2 Definitions, Symbols and Abbreviations

This section contains definitions, symbols and abbreviations that are used throughout the document.

2.1 Definitions

APN

An APN is an Access Point Name as defined in TS 23.003 [19].

eAN/ePCF

eAN/ePCF includes a logical entity in the Radio Access Network (RAN) used for radio communications with the UE and an evolved Packet Control Function entity (ePCF) that manages the relay of packets between the eAN and the HSGW.

eHRPD

Evolved HRPD (eHRPD): The eHRPD network supports attachment to the EPC (evolved packet core) of 3GPP. The eHRPD network optionally supports seamless handoffs between E-UTRAN and evolved HRPD with single-radio terminals.

eHRPD Mobile States

INACTIVE/NULL State
In the Inactive/Null State, there is no physical traffic channel between the UE and the eAN, no connection exists between the eAN and the ePCF, no connection exists between the ePCF and the HSGW, and there is no PPP link between the UE and the HSGW (ref. A.S0008/9-C section 1.12.1 [1] and [2]). The UE may have a Universal Access Terminal Identifier (UATI) that has been assigned by an eHRPD eAN.

DORMANT State
In the Dormant State, no physical traffic channel exists between the UE and the eAN and no connection exists between the eAN and the ePCF. However a connection exists between the ePCF and the HSGW and there is a PPP link between the UE and the HSGW (ref. A.S0008/9-C section 1.12.1 [1] and [2]).

• For purposes of this specification, a UE is first in the DORMANT state before participating in the “idle-mode” trusted non-3GPP procedures referred to in TS 23.402 [23]. That is, the eHRPD DORMANT state equates to the “idle” state referred to in TS 23.402.

ACTIVE/CONNECTED State
In the Active/Connected State, a physical traffic channel exists between the UE and the eAN over which data may be sent. A connection exists between the eAN and the ePCF, and between the ePCF and the HSGW, and there is a PPP link between the UE and the HSGW. (See A.S0008/9-C section 1.12.1 [1] and [2]).
• For purposes of this specification, a UE is first in the ACTIVE/CONNECTED state before participating in the “active-mode” trusted non-3GPP procedures referred to in TS 23.402 [23].

**Emergency Attached**

A UE is defined to be ‘Emergency Attached’ to the network, if the UE is connected to an emergency PDN and has not successfully performed EAP access authentication.

**Emergency Bearer Services**

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving eHRPD access network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and depending on local regulation, to UEs that are in limited service state.

**EPC**

The evolved packet core: The EPC domain name is defined in TS 23.003 [19]. The EPC architecture is defined in TS 23.401 [22] and TS 23.402 [23].

**EPS**

The evolved packet system is defined in TS 23.003 [19], TS 23.401 [22], and TS 23.402 [23]. It consists of the EPC plus the E-UTRAN.

**EPS Bearer**

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), for a PDN connection, receiving the same QoS treatment, carried over a service connection between a UE and a HSGW. A service connection is defined by X.S0011 [6] as the concatenation of a forward/reverse RLP flow and an A8/A10 tunnel.

**Handoff/Handover**

In this specification, the terms “handoff” and “handover” are synonymous and used interchangeably.

**Handover Attach**

When performing an inter-technology handoff/handover between E-UTRAN and eHRPD, the UE sends an Attach Type parameter of “handoff” when re-attaching to packet data networks on the target technology in order to distinguish from the “Initial Attach” scenario.

**HSGW**

The HSGW is the HRPD Serving Gateway that connects the evolved HRPD access network with the evolved packet core (EPC) as a trusted non-3GPP access network. The HSGW provides the PMIPv6 mobile access gateway (MAG) function to support layer 3 mobility with the P-GW (LMA).
Inter-HSGW Mobility with Context Transfer

Inter-HSGW mobility with context transfer occurs when a source HSGW transfers context for a UE to a target HSGW using the H1 interface, including the use of the H2 interface for data packet forwarding.

Inter-HSGW Mobility without Context Transfer

Inter-HSGW mobility without context transfer occurs if there is no H1/H2 connectivity between the source HSGW and target HSGW, or if for some reason the context transfer signaling exchange fails.

Legacy AT

A legacy AT is defined as an AT that is compliant to X.S0011 [6]. A legacy AT cannot communicate properly with an HSGW as defined in this specification. Within this specification, the use of “AT” implies a legacy AT or a UE functioning as a legacy AT.

Legacy PDSN

A legacy PDSN is defined as a PDSN that is compliant with X.S0011 [6]. Within this specification, the use of “PDSN” implies a legacy PDSN.

Limited Service State

A UE is in a limited service state when it connects to an eHRPD network without performing EAP AKA’ authentication.

Non-Optimized Handoff/Handover

Non-optimized handoff/handover involves the movement of the UE from E-UTRAN to eHRPD or vice-versa without the use of tunneled signaling (i.e., S101 signaling) between the source access network and the target access network. The UE leaves the radio environment of the source access network and performs a radio-level attachment to the target access network (e.g., creates an eHRPD session for the case of the UE moving from E-UTRAN to eHRPD), and then performs a handover attach procedure to the Packet Data Network(s) it had been communicating with over the source access network. Non-optimized Handoff/Handover applies to both Active and Idle (Dormant) UEs.

Optimized Handoff/Handover

Optimized handoff/handover involves the movement of the UE from E-UTRAN to eHRPD or vice-versa using tunneled signaling (i.e., S101 signaling) between the source access network and the target access network. While still on the source access network, the UE tunnels signaling to the target access network to pre-register through the source access network, i.e., to create both a radio and an IP context on the target system. After pre-registration, the UE performs a radio-level handoff/handover to the target technology per specified procedures. Optimized Handoff/Handover applies to both Active and Idle (dormant) UEs.

Service Connection

A logical connection between a UE and HSGW used to transport user data and signaling for the UE. There are two types of service connections: main and auxiliary. Each service connection is comprised of two parts: UE to RAN and RAN to HSGW.
“Structure and Identification of Management Information for TCP/IP-based Internets” (SMI) (RFC1155 [44]).

Tunnel Mode

The UE operating in tunnel mode means that there is an S101 interface between MME and eAN/ePCF across which signaling is passed in both directions while the UE is operating on E-UTRAN.

UE

In this specification, a UE is the User Equipment.

2.1.1 Symbols and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>3GPP2</td>
<td>3rd Generation Partnership Project 2</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, Accounting</td>
</tr>
<tr>
<td>ABNF</td>
<td>Augmented BACKUS-Naur Form</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>AMBR</td>
<td>Aggregated Maximum Bit Rate</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>APN-AMBR</td>
<td>per APN Aggregate Maximum Bit Rate</td>
</tr>
<tr>
<td>ARP</td>
<td>Allocation and Retention Priority</td>
</tr>
<tr>
<td>AT</td>
<td>Access Terminal</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute Value Pair</td>
</tr>
<tr>
<td>BAK</td>
<td>BCMCS Access Key</td>
</tr>
<tr>
<td>BBERF</td>
<td>Bearer Binding and Event Reporting Function</td>
</tr>
<tr>
<td>BCE</td>
<td>Binding Cache Entry</td>
</tr>
<tr>
<td>BCM</td>
<td>Bearer Control Mode</td>
</tr>
<tr>
<td>BCMCS</td>
<td>Broadcast Multicast Service</td>
</tr>
<tr>
<td>BE</td>
<td>Best Effort</td>
</tr>
<tr>
<td>BLOB</td>
<td>BLock Of Bits</td>
</tr>
<tr>
<td>BRA</td>
<td>Binding Revocation Acknowledgement</td>
</tr>
<tr>
<td>CCP</td>
<td>Compression Configuration Protocol</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Data Record</td>
</tr>
<tr>
<td>CMIP</td>
<td>Client Mobile IP</td>
</tr>
<tr>
<td>CSIM</td>
<td>cdma2000 Subscriber Identity Module</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DL</td>
<td>Down Link</td>
</tr>
<tr>
<td>eAN</td>
<td>evolved Access Network</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>eHRPD</td>
<td>evolved High Rate Packet Data</td>
</tr>
<tr>
<td>eNB</td>
<td>evolved NodeB</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packet Core</td>
</tr>
<tr>
<td>ePCF</td>
<td>evolved Packet Control Function</td>
</tr>
<tr>
<td>EPS</td>
<td>Evolved Packet System</td>
</tr>
<tr>
<td>E-UTRAN</td>
<td>Evolved Universal Terrestrial Radio Access Network</td>
</tr>
<tr>
<td></td>
<td>Term</td>
</tr>
<tr>
<td>---</td>
<td>---------------</td>
</tr>
<tr>
<td>1</td>
<td>FQDN</td>
</tr>
<tr>
<td>2</td>
<td>GBR</td>
</tr>
<tr>
<td>3</td>
<td>GRE</td>
</tr>
<tr>
<td>4</td>
<td>HRPD</td>
</tr>
<tr>
<td>5</td>
<td>HSGW</td>
</tr>
<tr>
<td>6</td>
<td>HSS</td>
</tr>
<tr>
<td>7</td>
<td>IANA</td>
</tr>
<tr>
<td>8</td>
<td>IETF</td>
</tr>
<tr>
<td>9</td>
<td>IMSI</td>
</tr>
<tr>
<td>10</td>
<td>IP</td>
</tr>
<tr>
<td>11</td>
<td>IP-CAN</td>
</tr>
<tr>
<td>12</td>
<td>LCP</td>
</tr>
<tr>
<td>13</td>
<td>LMA</td>
</tr>
<tr>
<td>14</td>
<td>MAC</td>
</tr>
<tr>
<td>15</td>
<td>MAG</td>
</tr>
<tr>
<td>16</td>
<td>MBR</td>
</tr>
<tr>
<td>17</td>
<td>MEID</td>
</tr>
<tr>
<td>18</td>
<td>MME</td>
</tr>
<tr>
<td>19</td>
<td>MN NAI</td>
</tr>
<tr>
<td>20</td>
<td>MRU</td>
</tr>
<tr>
<td>21</td>
<td>MSID</td>
</tr>
<tr>
<td>22</td>
<td>MSK</td>
</tr>
<tr>
<td>23</td>
<td>MUPSA</td>
</tr>
<tr>
<td>24</td>
<td>NAI</td>
</tr>
<tr>
<td>25</td>
<td>OUI</td>
</tr>
<tr>
<td>26</td>
<td>P-GW</td>
</tr>
<tr>
<td>27</td>
<td>PBA</td>
</tr>
<tr>
<td>28</td>
<td>PBU</td>
</tr>
<tr>
<td>29</td>
<td>PCC</td>
</tr>
<tr>
<td>30</td>
<td>PCEF</td>
</tr>
<tr>
<td>31</td>
<td>PCO</td>
</tr>
<tr>
<td>32</td>
<td>PCRF</td>
</tr>
<tr>
<td>33</td>
<td>PDN</td>
</tr>
<tr>
<td>34</td>
<td>PDN-ID</td>
</tr>
<tr>
<td>35</td>
<td>PDSN</td>
</tr>
<tr>
<td>36</td>
<td>PMIP</td>
</tr>
<tr>
<td>37</td>
<td>PPP</td>
</tr>
<tr>
<td>38</td>
<td>QCI</td>
</tr>
<tr>
<td>39</td>
<td>QoS</td>
</tr>
<tr>
<td>40</td>
<td>RA</td>
</tr>
<tr>
<td>41</td>
<td>RAN</td>
</tr>
<tr>
<td>42</td>
<td>RAT</td>
</tr>
<tr>
<td>43</td>
<td>RK</td>
</tr>
<tr>
<td>44</td>
<td>ROHC</td>
</tr>
<tr>
<td>45</td>
<td>RS</td>
</tr>
<tr>
<td>46</td>
<td>RSVP</td>
</tr>
<tr>
<td>47</td>
<td>S-GW</td>
</tr>
<tr>
<td>48</td>
<td>SDF</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SK</td>
<td>Session Key</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Stateless Address Autoconfiguration</td>
</tr>
<tr>
<td>TK</td>
<td>Temporary Key</td>
</tr>
<tr>
<td>TNL</td>
<td>Transport Network Layer</td>
</tr>
<tr>
<td>TFT</td>
<td>Traffic Flow Template</td>
</tr>
<tr>
<td>TLV</td>
<td>Type Length Value</td>
</tr>
<tr>
<td>UATI</td>
<td>Universal Access Terminal Identifier</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UE-AMBR</td>
<td>per UE Aggregate Maximum Bit Rate</td>
</tr>
<tr>
<td>UL</td>
<td>Uplink</td>
</tr>
<tr>
<td>VSA</td>
<td>Vendor Specific Attribute</td>
</tr>
<tr>
<td>VSNCP</td>
<td>Vendor Specific Network Control Protocol</td>
</tr>
<tr>
<td>VSNP</td>
<td>Vendor Specific Network Protocol</td>
</tr>
</tbody>
</table>
3 E-UTRAN - eHRPD Connectivity and Interworking Architecture

3.1 E-UTRAN – eHRPD Interworking Non-Roaming Architecture

Figure 1 shows the architecture for interworking between the 3GPP Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the 3GPP2 evolved High Rate Packet Data (eHRPD) network. This architecture supports the interworking interfaces defined in TS 23.402 [23], including the following interfaces:

- S101: the signaling interface between the EPC Mobility Management Entity (MME) and the evolved HRPD Access Network (eAN/ePCF) (ref. TS 29.276 [36]). Note that the eAN/ePCF functions are defined in A.S0022 [4],

- S103: the bearer interface between the Evolved Packet Core (EPC) Serving Gateway (S-GW) and the HSGW (ref. TS 29.276 [36]).

Figure 1  E-UTRAN - eHRPD Interworking Non-Roaming Architecture
3.2 E-UTRAN – eHRPD Interworking Roaming Architecture (Home-Routed Traffic)

Figure 2 illustrates the E-UTRAN – eHRPD interworking architecture for home-routed traffic. In this case the anchor point (i.e., the P-GW) is located in the home network.

Figure 2  E-UTRAN – eHRPD Interworking – Roaming Architecture (Home-Routed Traffic)
3.3 E-UTRAN – eHRPD Interworking Roaming Architecture (Local Breakout)

Figure 3 illustrates the E-UTRAN – eHRPD interworking architecture for local breakout traffic. In this case the anchor point (i.e., the P-GW) is located in the visited network.

Figure 3   E-UTRAN – eHRPD Interworking – Roaming Architecture (Local Breakout)
3.4 Reference Points

As shown in Figure 1 through Figure 3, for the interworking between E-UTRAN and eHRPD, the following reference points are defined:

3.4.1 H1/H2 Reference Points

The H1 reference point carries signaling information between a source HSGW (S-HSGW) and a target HSGW (T-HSGW) for optimized inter-HSGW handoff.

The H2 reference point carries user traffic, both uplink and downlink, from a source HSGW (S-HSGW) to a target HSGW (T-HSGW) for optimized inter-HSGW handoff.

3.4.2 Gxa Reference Point

The Gxa reference point connects the Policy and Charging Rules Function (PCRF) in the 3GPP EPC to the BBERF in the HSGW in the 3GPP2 eHRPD access network.

Detailed requirements and operation of this interface is defined in TS 23.203 [20], TS 29.212 [29] and TS 29.213 [30].

3.4.3 Pi* Reference Point

The protocol used on the Pi* reference point connects the HSGW to the 3GPP2 AAA Proxy. The requirements for this interface to support the Pi*3GPP2 Diameter Application are as defined in section 6. If the Pi*3GPP2 Diameter Application is not supported, the Pi* reference point is identical to that used on the STa reference point.

3.4.4 S101 Reference Point

The S101 reference point connects the MME in the 3GPP EPS to the eAN/ePCF in the 3GPP2 eHRPD access network per A.S0022 [4]. This reference point provides tunneling of signaling and data between the UE and the target access network via the source/serving access network.

The detailed operation of this interface is defined in TS23.402 [23] and TS 29.276 [36].

3.4.5 S103 Reference Point

The S103 reference point connects the Serving Gateway (S-GW) in the 3GPP EPC to the HSGW in the 3GPP2 eHRPD network. Its function is to forward downlink data between the S-GW and the HSGW to minimize packet losses in mobility from E-UTRAN to eHRPD.

Detailed requirements and operation of this interface is defined in TS 23.402 [23] and TS 29.276 [36].

3.4.6 S2a Reference Point

The S2a reference point connects the PDN Gateway in the 3GPP EPC to the HSGW in the 3GPP2 eHRPD network. This reference point provides the user plane with related control and mobility support between eHRPD access and the P-GW.
Detailed requirements and operation of this interface is defined in TS 23.402 [26], TS 29.275 [35], and Section 5.

### 3.4.7 STa Reference Point

The STa reference point connects the AAA server/proxy in the 3GPP EPC to the AAA proxy in the 3GPP2 eHRPD network. This reference point is used to authenticate and authorize the UE and carries PMIPv6 mode related Diameter parameters between the 3GPP AAA server/proxy and the 3GPP2 AAA Proxy.

Detailed requirements and operation of this interface is defined in TS 23.402 [23] and TS 29.273 [34].
3.5 Protocol Stacks Between the UE and the HSGW

The figures in the following subsections illustrate the user plane and the control plane protocol stacks between the UE and the HSGW used in eHRPD.

For octet stream connections (SO64, SO59) user plane traffic between the HSGW and the UE is encapsulated in HDLC-like framing between the UE and the HSGW. For packet stream connections (SO72 and SO67) user plane traffic through the eAN is transported directly over the RLP and A10 connections. In the case of service connections shared between different PDNs (SO59, SO64, SO72), user traffic is encapsulated with a PDN identifier. Otherwise, the PDN of each user packet is identified via the A10 connection that is associated with the upper four bits of the Reservation Label (Flow ID) that is associated with the A10.

3.5.1 User Plane

The figures in this section provide the protocol stacks for user plane bearers.

3.5.1.1 User Plane Traffic via Service Option 72 (SO72)

The protocol stack in Figure 4 indicates that traffic for multiple PDNs may share the same auxiliary service connection using SO72. In particular, a BE auxiliary service connection with Flow ID 0xFE and using SO72 can be established during HRPD session configuration.

![Figure 4 Protocol stack for traffic multiplexed on an SO72 Auxiliary Connection](image-url)
3.5.1.2 User Plane Traffic via Service Option 67 (SO67)

Figure 5 illustrates the use of an auxiliary service connection that is dedicated to one or more IP flows with similar QoS characteristics for a single PDN. This type of auxiliary service connection uses SO67 and does not involve use of the PDN-ID for multiplexing. For the HSGW, the PDN of each uplink user packet is identified via the A10 connection that is associated with the upper four bits of the Reservation Label (Flow ID). For the UE, the PDN of each downlink user packet is identified by the RLP that it is received on. Such a service connection may be used for, for example, VoIP traffic or streaming video. Header compression is optional and may be configured for an SO67 auxiliary service connection.

Figure 5 Protocol stack for non-multiplexed traffic on an Auxiliary Connection
3.5.1.3 **User Plane Traffic via VSNP on the Main Service Connection using Service Option 59 (SO59)**

The protocol stack in Figure 6 indicates that traffic for different PDNs may share the main service connection. Packets are separated with a PDN identifier (PDN-ID) within VSNP. This protocol stack also serves to carry RSVP packets between the UE and HSGW as shown in section 3.5.2.

*Figure 6* Main Service Connection User-Plane Protocol Stack via SO59
3.5.1.4 User Plane Traffic via Service Option 64 (SO64)

The protocol stack in Figure 7 indicates that traffic for different PDNs may share an auxiliary service connection configured with SO64. Packets are separated with a PDN identifier (PDN-ID) within VSNP to provide multiplexing of traffic for multiple PDNs.

![Figure 7 SO64 Auxiliary Service Connection User-Plane Protocol Stack](image-url)
3.5.2 Control Plane

3.5.2.1 Control Plane HSGW to UE – EAP

The protocol stack in Figure 8 indicates that the EAP protocol uses PPP over the main service connection.

![Diagram of Main Service Connection Protocol Stack for EAP](image)

Figure 8 Main Service Connection Protocol Stack for EAP

3.5.2.2 Control Plane HSGW to UE – VSNCP

The protocol stack in Figure 9 indicates that VSNCP control signaling within PPP is used over the main service connection.

![Diagram of Main Service Connection Control Plane Protocol Stack for VSNCP](image)

Figure 9 Main Service Connection Control Plane Protocol Stack for VSNCP
3.5.2.3 Control Plane HSGW to UE – RSVP

RSVP signaling is carried as IP traffic within the user plane via VSNP. See Figure 10. The PDN-ID is used to specify the PDN to which the RSVP message applies (ref section 9.1.5).

![Diagram](image)

**Figure 10** RSVP Over the Main Service Connection Using VSNP
3.6 H1/H2 Interface Protocol Stacks

The protocol stack used for inter-HSGW handover is per RFC 5949 [85].

- H1 interface signaling procedures between the S-HSGW and the T-HSGW are based on the reactive handover procedures in RFC 5949 [85].

- H2 interface supports the ability to tunnel traffic on a per-UE basis.

- H2 interface supports Generic Routing Encapsulation (GRE) RFC 2784 [55] including the Key Field extension RFC 2890 [56]. The Key field value of each GRE packet header identifies the uplink or downlink traffic flow for a given UE.

- For the downlink traffic, the H2 interface carries user IPv4/IPv6 packets identified by the associated PDN-ID, over either an IPv4 or an IPv6 transport network.

- For uplink traffic, the H2 interface carries PDN-Mux or dedicated service connection traffic, identified by the associated service connection SR-ID, over either an IPv4 or IPv6 transport network.

The protocol stack in Figure 11 below illustrates the H1 interface control signaling stack between the S-HSGW and the T-HSGW.

![H1 Interface Control Plane Protocol Stack](image)

Figure 11  H1 Interface Control Plane Protocol Stack

Note: In this version of this specification only IPv4 addresses are supported between the S-HSGW and T-HSGW.
Figure 12 illustrates the protocol stack for the flow of downlink user traffic from the S-HSGW to the T-HSGW. Each user IPv4/IPv6 packet, encapsulated by the S-HSGW with the PDN-ID of the PDN from which it is received, is sent over the transport network between the S-HSGW and the T-HSGW using the downlink GRE key assigned by the use of H1 signaling.

![Diagram of Protocol Stack]

**Figure 12**  H2 Interface Downlink User Plane Protocol Stack
Figure 13 illustrates the protocol stack for the flow of uplink user traffic from the S-HSGW to the T-HSGW. Each A10 payload received over the service connection(s) identified by the associated service connection SR-ID is sent over the transport network between the S-HSGW and the T-HSGW using the uplink GRE key assigned by the use of H1 signaling.

3.7 Control Plane HSGW to P-GW – PMIPv6

The PMIPv6 signaling specified in RFC 5213 [78] is used to manage mobility between the P-GW and multiple HSGWs. The protocol stack for UE mobility management using PMIPv6 over S2a is specified in 3GPP TS29.275 (Release 9) [35].
4 eHRPD Functionality

eHRPD provides interworking of the UE with the 3GPP EPC architecture and protocols specified in TS 23.402 [23]. In addition, eHRPD also supports seamless inter-technology mobility with E-UTRAN with the following requirements:

a. Inter-technology handoff between 3GPP E-UTRAN and eHRPD shall be supported.

b. Bearer interruption for an optimized handoff shall be less than the 300 msec interruption time for the RAT change procedures specified in TS 22.278 [16].

4.1 General HSGW Capabilities

The HSGW is the entity that terminates the eHRPD access network interface from the eAN/ePCF (i.e., A10/A11 interfaces). The functions of the eHRPD eAN/ePCF are specified in AS0022 [4]. The HSGW routes UE originated or UE terminated packet data traffic. 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 specified in TS 23.402 [23]. This includes support for mobility, policy control and charging (PCC), access authentication, and roaming. The HSGW supports inter-HSGW handoff as well, using S2a (PMIPv6). The HSGW may also support inter-HSGW handoff with context transfer. The HSGW may use inter-HSGW handoff without context transfer.

The HSGW shall perform the following functions:

a. Mobility anchoring for inter-eAN handoff.

b. Packet routing and forwarding.

c. 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.

d. Accounting with user and service class granularity for inter-operator charging.

e. Uplink and downlink charging per UE, PDN, and QCI.

f. Event reporting (e.g., change of RAT) to the PCRF.

g. Downlink bearer binding based on policy information.

h. Uplink bearer binding verification with packet dropping of uplink traffic that does not comply with established uplink policy.

i. MAG functions for S2a mobility (i.e., Network-based mobility using PMIPv6).

j. Support for IPv4 address and/or IPv6 prefix delivery during IPv4 address and/or IPv6 prefix assignment procedures.

k. Authenticator function.

l. PCC support defined for the Gxa interface.

m. Support for ROHC.

n. Support for PPP-based operation (e.g., terminating the PPP signaling protocol over the main A10 connection with HDLC-like framing).

o. Support for packet-based or HDLC-like framing on auxiliary connections.

p. Support for RAN flow control.
q. Mapping between 3GPP QoS parameters and eHRPD QoS parameters.

r. Packet data forwarding during inter-RAT and inter-HSGW handoff.

4.2 Authentication and Subscription Information Retrieval

This section defines eHRPD authentication and authorization procedures.

EPS authentication in this document refers to EPS AKA authentication over E-UTRAN or EAP-AKA' authentication over eHRPD.

When eHRPD access is used to connect to the 3GPP EPC and when the eAN/ePCF does not indicate that the UE is attaching for emergency services, 3GPP-based access authentication is required across a SWx/STa/Pl* reference point as depicted in section 3. The following principles shall apply in this case:

- Transport of authentication signaling shall be independent of the eHRPD technology.
- Access authentication signaling shall be based on IETF protocols, e.g., Extensible Authentication Protocol (EAP) as specified in RFC 3748 [66].
- Access authentication signaling procedures shall be based on TS 33.402 [42].

When eHRPD access is used to connect to the 3GPP EPC and the eAN/ePCF indicates that the UE is attaching for emergency services, depending on local regulation (ref. TS 33.402 [42]) the HSGW shall do one of the following:

- Bypass the authentication procedures specified in this section, and mark the UE in an “emergency services - unauthenticated” limited service state.
- Authenticate the UE according to the principles set out in this section for a non-emergency service, and then mark the UE in an “emergency services - authenticated” state. If authentication fails, depending on local regulation the attachment for emergency services may be rejected, or the UE may be placed in an “emergency services – unauthenticated” limited service state.

Authentication, if performed, shall follow trusted non-3GPP access procedures specified in TS 33.402 [42]. The UE as the EAP Peer and the 3GPP AAA as the EAP Authentication Server mutually authenticate each other using the EAP-AKA’ procedures. Upon successful authentication, if the UE is authorized to access the network, the 3GPP AAA sends the Master Session Key (MSK) to the HSGW which acts as the EAP Authenticator.

4.2.1 EAP Protocol Negotiation

During the PPP session negotiation between the HSGW and the UE, the HSGW shall propose EAP as the authentication protocol in the LCP Configure-Request message by setting Authentication-Protocol option to 0xC227 (see RFC 3748 [66]).

Once the UE receives an LCP Configure-Request message from the HSGW that contains the Authentication-Protocol option that is set to 0xC227, the UE shall respond with LCP Configure-Ack, indicating to the HSGW the acceptance of EAP-based authentication for PPP session establishment as described in RFC 3748 [66] and RFC 1661 [43].

If the HSGW receives LCP Configure-Ack from the UE indicating the acceptance of EAP-based authentication, the HSGW shall select EAP as the PPP authentication protocol and
proceed to play the role of EAP authenticator. Otherwise, the HSGW shall follow the operator defined policy.

4.2.2 UE Requirements

The UE shall support the EAP-AKA’ protocol defined in TS 33.402 [42] for Network Access Authentication.

If the UE supports a Universal Subscriber Identity Module (USIM) for authentication, the UE shall support EAP-AKA’, which relies on AKA authentication defined in TS 33.102 [40]. AKA requires a pre-defined common set of algorithms (consisting of a set of “f” functions, i.e., f1, ..., f5, f1* and f5*) between the UE and the home network.

If the UE does not support USIM for authentication, the UE shall support the following AKA authentication and algorithm profiles:

- AKA authentication profile:
  1. The UE shall use AKA as specified in TS33.102 [40].
  2. The UE shall use the AKA identity (IMSI), 128-bit root key (K), and the AKA algorithm customization parameters. These parameters may be either factory provisioned or (re)provisioned using over-the-air (OTA) mechanisms (e.g., using OTASP as specified in C.S0016-D [7]).
  3. AKA SQN management scheme shall be as specified in section C.2.2 and C.3.2 of Annex C in TS 33.102 [40].
  4. Anonymity Key (AK) shall be used for SQN concealment (i.e., f5 and f5* shall be non-zero).
     NOTE: SQN concealment is required if SQN generation is predictable.
  5. The UE shall support MILENAGE as the AKA algorithm as specified in TS 35.206 [43].

- MILENAGE algorithm profile:
  1. The MILENAGE algorithm “f” functions (f1, ..., f5, f1* and f5*) shall be as defined in TS 35.206 [43].
  2. The UE shall support customization of MILENAGE algorithm using a 128-bit Operator Variant Algorithm Configuration Field. This customization parameter may be either OP or OPc as specified in TS 35.206 [43].
  3. OP or OPc may be either factory provisioned or (re)provisioned using OTA mechanisms (e.g., using OTASP as specified in C.S0016-D [9]).
  4. If OP is used, then OPc shall be derived from OP; otherwise, OPc shall be used directly.
  5. All other MILENAGE algorithm constants shall be as specified in TS 35.206 [43].

4.2.2.1 UE Identity Management

The UE shall have a permanent ID that is an IMSI-based NAI as defined in TS 23.003 [19]. The UE shall support temporary identities (pseudonym and fast-reauthentication) as specified in TS 24.302 [26] and TS 33.402 [42]. Temporary identities are defined in TS 23.003 [19] and are one time identities.
Upon receiving the EAP Request / Identity, the UE shall respond with the EAP Response / Identity carrying its identity complying with Network Access Identifier (NAI) format specified in TS 23.003 [19]. See TS 24.302 [26] for further information on UE identity management.

If upon successful EAP-AKA’ access authentication (see RFC 5448 [80]), a protected pseudonym and/or re-authentication identity were received, the UE shall store the temporary identity(s) for future authentications.

4.2.2.2 UE Network Access Authentication

Upon receiving the EAP Request / AKA’ Challenge, the UE shall check whether the AMF separation bit is set to 1. If this is not the case the UE shall reject the authentication. Otherwise, the UE shall execute the AKA’ algorithms on the UE.

If verification of the AT_AUTN is incorrect per RFC 5448 [80] and TS 33.402 [42], the UE shall reject the authentication. If the sequence number is out of synch, the UE shall initiate a synchronization procedure, refer to RFC 5448 [80].

If AT_AUTN is correct, the UE shall compute AT_MAC and AT_RES. The UE shall use the access network name received in AT_KDF_INPUT of the EAP Request/AKA’ Challenge to derive IK’ and CK’ and send the AT_MAC and AT_RES to the HSGW in the EAP Response / AKA’ Challenge, as specified in RFC 5448 [80].

4.2.2.3 UE Key Generation for Access Security

The UE shall derive required additional new keying material, including the key MSK, according to EAP-AKA’ RFC 5448 [80] and TS 33.402 [42] from the new computed CK’, IK’ and check the received AT_MAC with the new derived keying material.

The UE shall separate the 512 bits of generated MSK into four equal portions of 128 bits each, i.e., four Sub-MSKs. The UE shall use each Sub-MSK to generate the four PMKs as follows:

PMK1 = HMAC-SHA-256(Sub-MSK, “pmk@hrpd.3gpp2”, 0x01), [0:127]
PMK2 = HMAC-SHA-256(Sub-MSK, “pmk@hrpd.3gpp2”, 0x01) [128:255],
PMK3 = HMAC-SHA-256(Sub-MSK, “pmk@hrpd.3gpp2”, 0x02) [0:127],
PMK4 = HMAC-SHA-256(Sub-MSK, “pmk@hrpd.3gpp2”, 0x02) [128:255],
where the key label “pmk@hrpd.3gpp2” is set to ASCII strings without NULL termination.

The UE may pre-compute the PMKs and PairwiseMasterKeyID associated with each PMK as specified in C.S0067 [14]. In addition, the UE may also pre-compute the PMKs and PairwiseMasterKeyIDs associated with the other Sub-MSKs. This pre computation of PMKs and PairwiseMasterKeyIDs enables the UE to identify the PMK it needs to use upon receiving request from the access network to derive session keys for access security.

4.2.3 HSGW Requirements

The HSGW shall support the following:

- RFC 3748 [66], Extensible Authentication Protocol (EAP).
RFC 5448 [80], Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA’).

The HSGW shall be the EAP authenticator in eHRPD. Therefore, the HSGW is the entity that receives the MSK from the 3GPP AAA after EAP authentication. The HSGW sends the serving network identity which is identical to access network identity specified in TS 24.302 to the 3GPP2 AAA Proxy/3GPP AAA during authentication.

If the HSGW receives an indication in A11-Registration Request message that the PMK is needed for this session, and if HSGW determines that it has no unused PMKs, the HSGW shall set Sub-MSK as the 128-bit portion (Sub-MSK) occupying the highest order bit positions of the unused MSK information, as specified in section 11.3.2. The HSGW shall use the Sub-MSK for the computation of PMKs using the procedures specified in section 4.2.2.3. Once the HSGW generates the PMK or determines that the new PMK needs to be sent to the eAN/ePCF, the HSGW shall send a PMK and its lifetime in seconds to the ePCF using A11-Registration Reply or A11-Session Update message [1] if the ePCF has indicated in the A11-Registration Request that the PMK is used for this session. The lifetime of the PMK shall not be more than the remaining value of the MSK lifetime. If the HSGW runs out of PMKs, the HSGW may use the unused MSK information to generate new PMKs as specified above.

The HSGW (EAP Authenticator) shall initiate EAP re-authentication prior to MSK expiry, if the HSGW determines that the session needs to be maintained.

If the Diameter protocol is used, the HSGW shall support the following RFCs:

- RFC 3588 [63], Diameter Base Protocol.
- RFC 4005 [69], Diameter Network Access Server Application.
- RFC 4072 [73], Diameter Extensible Authentication Protocol (EAP) Application.

4.2.4 3GPP AAA Server Requirements

3GPP AAA Server requirements are defined in TS 29.273 [34] and in TS 24.302 [26].

4.2.5 Authentication Call Flows

4.2.5.1 Use of EAP-AKA’ – Initial Authentication

The following figure shows authentication of the UE with the 3GPP AAA Server using EAP-AKA’ via the 3GPP2 AAA Proxy and the authenticator in the HSGW, or directly from the 3GPP AAA Server via the authenticator in the HSGW. Note that all EAP-AKA’ procedures in this message flow shall follow the rules of RFC 5448 [80]. The subscription information from the HSS/AAA is also retrieved during this procedure.
Figure 14  EAP-AKA' Authentication for eHRPD
0. PPP LCP negotiation occurs. EAP is negotiated as the authentication protocol.

1. The HSGW sends an EAP-Request / Identity message to the UE.

2. The UE responds with EAP-Response / Identity (NAI). If UE uses its permanent NAI, it shall use the IMSI-based Network Access Identifier (NAI) format specified in TS 23.003 [19].

3. The HSGW forwards the unmodified NAI received in the EAP-Response/Identity message to the EAP Server in the 3GPP AAA.

3a: The HSGW, as the authenticator, encapsulates the EAP payload in a AAA message and forwards it, along with the access type (i.e., RAT type), and NAS-ID = {the FQDN of the HSGW} to the 3GPP2 AAA Proxy. In this message, the HSGW shall also include the serving network identity (serving network identity is identical to access network identity specified in TS 24.302). The format of the serving network identity is specified in TS 24.302 [26].

3b. The 3GPP2 AAA Proxy forwards the unmodified contents to the 3GPP AAA Server.

Steps 4 through 7 are conditional. They will occur if the 3GPP AAA Server decides to send the EAP-Request / AKA-Identity message.

4. 4a: The 3GPP AAA Server sends the EAP-Request / AKA-Identity to the 3GPP2 AAA Proxy (ref. RFC 4187 [74]).

4b. The 3GPP2 AAA Proxy forwards the EAP-Request / AKA-Identity to the HSGW.

5. The HSGW sends the EAP-Request / AKA-Identity to the UE.

6. The UE sends EAP-Response/ AKA-Identity containing the permanent UE Identity to the HSGW.

7. 7a: The HSGW encapsulates the EAP-Response / AKA-Identity in a AAA message and sends it to the 3GPP2 AAA Proxy.

7b. The 3GPP2 AAA Proxy forwards the message to the 3GPP AAA Server.

8. The 3GPP AAA Server will terminate the EAP protocol. If the UE identified itself with the pseudonym, the 3GPP AAA server determines the real identity of the UE and derives the IMSI from it. The 3GPP AAA Server checks that it has an unused authentication vector with AMF separation bit = 1 and the matching access network identifier available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS using IMSI. The 3GPP AAA server includes in a message sent to the HSS an indication that the authentication vector is requested for EAP-AKA’, and the serving network identity. The 3GPP AAA Server ensures that the given access network is authorized to use the claimed serving network identity.

9. The HSS calculates the AKA’ vector(s). The HSS then transforms this AKA vector as specified in TS 33.402 [42].

10. The HSS returns the transformed AKA’ vector(s), including AT_RAND, AT_AUTN, and AT_RES, IK’ and CK’, to the 3GPP AAA. The 3GPP AAA Server stores the received AKA’ vector(s).

11. New keying material is derived from IK’ and CK’ according to EAP-AKA’ (see RFC 5448 [80]). A new pseudonym and/or re-authentication ID may be chosen and if chosen are protected (i.e., encrypted and integrity protected) using keying material generated from EAP-AKA’.

12. The 3GPP AAA Server sends AT_RAND, AT_AUTN, a message authentication code (AT_MAC), AT_KDF, AT_KDF_INPUT and two user identities (if they are generated): protected pseudonym and/or protected re-authentication id in EAP Request/AKA’-Challenge message. The sending of the re-authentication ID depends on the operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the 3GPP AAA Server decides (based on policies set by the operator) whether to include the re-authentication id or not, thus allowing or
disallowing the triggering of the fast re-authentication process. The 3GPP AAA Server may use a protected success indication by including the AT_RESULT_IND attribute in the EAP Request/AKA'-Challenge message, in order to indicate to the UE that it would like result indications in both successful and unsuccessful cases. The inclusion of the result indications for the protection of the result messages depends on home operator's policies.

12a: The 3GPP AAA Server sends the EAP-Request / AKA'-Challenge and the other parameters to the 3GPP2 AAA Proxy.

12b. The 3GPP2 AAA Proxy forwards the EAP-Request / AKA'-Challenge and other parameters to the HSGW.

13. The HSGW sends the EAP-Request / AKA'-Challenge and other parameters to the UE.

14. The UE runs the AKA’ algorithms on the UE. The UE verifies that AT_AUTN is correct and thereby authenticates the network. If AT_AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of sync, the terminal initiates a synchronization procedure (not shown in this example), c.f. RFC 5448 [80]. If AT_AUTN is correct, the UE computes AT_RES, IK’ and CK’. The UE derives required additional new keying material, including the key MSK, according to RFC 5448 [80] and TS 24.302 [26] from the new computed IK’ and CK’, and checks the received AT_MAC with the new derived keying material. If a protected pseudonym and/or re-authentication identity were received, then the UE stores the temporary identity(s) for future authentications.

15. The UE calculates a new AT_MAC value covering the EAP message with the new keying material. UE sends EAP Response/AKA'-Challenge containing calculated AT_RES and the new calculated AT_MAC value to the HSGW. The UE includes in this message the result indication if it supports result indications and if it received the same indication from the 3GPP AAA Server. Otherwise, the UE omits this indication.

16. The HSGW sends the authentication response to the EAP server.

16a: The HSGW encapsulates the EAP-Response / AKA'-Challenge, AT_RES, and AT_MAC in a AAA message and sends it to the 3GPP2 AAA Proxy.

16b. The 3GPP2 AAA Proxy forwards the message to the 3GPP AAA Server.

17. The 3GPP AAA Server checks the received AT_MAC and verifies the AT_RES value to the XRES value from the AKA vector received in step 10 above. The remainder of this flow assumes that the comparison succeeds. If the 3GPP AAA Server sent a pseudonym and/or fast re-authentication identity to the UE in the step 12, it now associates these identities with the permanent identity of the UE.

Steps 18 through 21 are conditional based on the EAP Server and the UE having indicated the use of protected successful result indications (see steps 11 and 13).

18. If the 3GPP AAA Server requested previously to use protected result indications and received the same result indications from the UE as in RFC 5448 [80], the 3GPP AAA Server sends the message EAP Request/AKA'-Notification.

18a: The 3GPP AAA Server sends EAP Request/AKA'-Notification to the 3GPP2 AAA Proxy.

18b. The 3GPP2 AAA Proxy forwards it to the HSGW.

19. The HSGW sends EAP Request/AKA'-Notification to the UE.

20. The UE sends EAP Response/AKA'-Notification to the HSGW.

21. 21a: The HSGW encapsulates the EAP-Response / AKA'-Notification in an AAA message and sends it to the 3GPP2 AAA Proxy.

21b. The 3GPP2 AAA Proxy forwards the message to the 3GPP AAA Server. The 3GPP AAA Server ignores the contents of this message if the AT_NOTIFICATION code in the EAP-AKA’ Notification was “success”.

34
22. The 3GPP AAA Server creates an EAP-Success message that also includes the subscription profile that has been retrieved from the HSS and the MSK (see RFC 5448 [80]), in the underlying AAA protocol message (i.e., not at the EAP level).

22a: The 3GPP AAA Server sends the EAP-Success message and other parameters (e.g., AMBR) in a AAA message to the 3GPP2 AAA Proxy.

22b. The 3GPP2 AAA Proxy forwards the information including the subscription information elements (defined in TS 29.273 [34]) on to the HSGW.

If the peer indicated that it wants to use protected success indications with AT_RESULT_IND, then the peer MUST NOT accept EAP-Success after a successful EAP/AKA'-Reauthentication round. In this case, the peer MUST only accept EAP-Success after receiving an EAP-AKA' Notification with the AT_NOTIFICATION code "Success".

If the peer receives an EAP-AKA' Notification that indicates failure, then the peer MUST no longer accept the EAP-Success packet, even if the server authentication was successfully completed.

23. The HSGW stores the keying material to be used in communication with the authenticated UE as required. The HSGW also stores the other parameters sent in the AAA message. The HSGW signals EAP-Success to the UE. If the UE received the pseudonym and/or fast reauthentication identity in step 13, it now accepts these identities as valid for next authentication attempt.

At this point, the EAP-AKA' exchange has been successfully completed, and the UE and the access network share keying material derived during that exchange.

The authentication process may fail at any moment, for example because of unsuccessful checking of AT_MACs or no response from the UE after a network request. In that case, the EAP-AKA' process will be terminated as specified in RFC 5448 [80] and an indication shall be sent to the HSS.

4.3 Use of EAP-AKA' – Fast Re-Authentication

EAP-AKA' Fast Re-Authentication shall be supported per RFC 5448 [80] and as specified in TS 24.302 [26] and TS 33.402 [42]. Fast re-authentication uses keys derived on the previous full authentication.

The use of fast re-authentication is optional and depends on operator policy. The 3GPP AAA server indicates fast re-authentication for EAP-AKA' to the UE by sending the re-authentication identity to the UE.

4.4 IP Address Allocation

This section specifies IP address allocation in eHRPD.

4.4.1 General

The requirements and procedures of this section are per TS 23.401 [22] and TS 23.402 [23].

A UE shall be able to request an IPv4 address and/or IPv6 address/prefix. A UE shall perform the address allocation procedures for at least one IP address (either IPv4 or IPv6) after establishing the PDN connection if no IPv4 address is allocated during PDN connection setup.

For IPv4 addressing, the UE shall use one of the following procedures:
1. Acquire the IPv4 address and IPv4 parameter configuration via VSNCP signaling during PDN connection establishment.

2. Acquire the IPv4 address and IPv4 parameter configuration using DHCPv4 after the PDN connection establishment.

For IPv6 addressing, the UE shall perform the following procedures:

1. Acquire the Interface Identifier via the VSNCP signaling during PDN connection establishment. The UE configures its link local address using this Interface Identifier.

2. Configure the /64 prefix using Router Advertisement from the HSGW (Access Router) for the PDN connection.

3. Configure the 128-bits IPv6 address using IPv6 SLAAC (see RFC 4862 [76]).


The IP address or prefix allocated to the UE’s PDN connection shall be used for the UE’s default and dedicated bearers associated with that PDN connection.

Each service connection, i.e., each concatenation of an RLP flow with an A8+A10 connection, between the UE and the HSGW supports both IPv4 and IPv6 packets.

The UE may indicate to the network whether it wants to obtain the IPv4 address during PDN connection setup procedures or by executing IETF procedures after the PDN connection setup:

- If the UE indicates that it prefers to obtain an IPv4 address as part of the PDN connection setup procedure, the UE relies on the HSGW to provide an IPv4 address from the P-GW to the UE as part of the PDN connection setup procedure, i.e., using VSNCP procedures specified in section 9.1.4.

- If the UE indicates (e.g., by including the Address Allocation Preference in the PCO) that it prefers to obtain the IPv4 address after the PDN connection setup by executing DHCPv4 (see RFC 2131 [47]) procedures, the HSGW may provide the IPv4 address for the UE as part of procedures used to establish the PDN connection. If the HSGW receives UE’s IP address through PMIP tunnel establishment without the deferred IPv4 address allocation indicator included, the HSGW shall respond to the UE by setting the PDN Address field to the IP address received from P-GW. Otherwise, after the PDN connection establishment procedure is completed, the UE initiates the IPv4 address configuration on its own using DHCPv4. See details in section 4.4.4.

The HSGW is responsible for delivering the IPv4 address and/or IPv6 prefix to the UE.

The HSGW shall support the following mechanisms:

a. IPv4 address allocation during PDN connection establishment procedures (per section 7.2.1 and 9.3.1).

b. IPv4 address allocation after PDN connection establishment procedures (e.g., via DHCPv4).
The eHRPD network shall also support the following mechanisms following the PDN connection establishment procedures:

a. \(/64\) IPv6 prefix allocation via IPv6 Stateless Address auto-configuration according to RFC 4862 [76];

b. IPv4 address allocation and IPv4 parameter configuration via DHCPv4 according to RFC 2131 [47] and RFC 4039 [70]. See call flows in Section 4.4.5.1 and Section 4.4.5.3 for details;

c. IPv6 parameter configuration via Stateless DHCPv6 according to RFC 3736 [65].

During PDN connection establishment, the P-GW sends the IPv6 prefix and Interface Identifier to the HSGW. If the UE indicates that it prefers to obtain an IPv6 address, the HSGW shall forward the IPv6 Interface Identifier to the UE using VSNCP message. The HSGW shall convey the assigned IPv6 prefix to the UE using Router Advertisement.

### 4.4.1.1 IP Address Allocation using VSNCP and PMIPv6 in eHRPD

This section describes the interactions between the VSNCP protocol and the PMIPv6 protocol to accomplish IP address allocation on S2a.

The VSNCP stage 3 protocol details are in section 9.1.4.

For PMIPv6 stage 3 protocol details, refer to TS 29.275 [35].

Note: TS 23.401 [22] refers to "Address Allocation Preference" at the stage 2 level. This maps into the names "IP address allocation via NAS signaling" (immediate allocation) and "IPv4 address allocation via DHCPv4" (deferred allocation) in TS 24.008. The deferred allocation indicator in the Proxy Binding Acknowledgement (PBA) is specified in TS 29.275 [35], "3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication option", which indicates to the HSGW that deferred allocation is used.

### 4.4.1.1.1 Initial Attach

There are seven parameters of significance to the IP address allocation process that are sent by the UE on the VSNCP Configure-Request message for an initial attach:

- PDN Type
- PDN Address
- Protocol Configuration Options (PCO) that may contain an indication that deferred IPv4 address allocation is desired
- Address Allocation Cause
- APN
- IPv4 Default Router Address if PDN Type indicates IPv4 or IPv4v6.
- Emergency Indicator, if the UE is connecting to an emergency PDN.

In the VSNCP Configure-Request message sent from the UE to the HSGW, the “PDN Type” option carries information on the UE IP capabilities. It shall be used to indicate to the HSGW whether the UE supports IPv4, IPv6, or IPv4v6.
In the VSNCP Configure-Request, on initial attach the UE shall include PDN Address option as specified in section 9.1.4.1. However, the HSGW shall ignore the contents of the “PDN Address” option.

In the VSNCP Configure-Request, the PCO indicates the bearer control mode, and may contain an indication that deferred IPv4 address allocation is desired. See TS 29.275 [35].

In the VSNCP Configure-Request, the “Address Allocation Cause” option shall be set to a value of 0 (“Null value”).

Per section 9.1.4.2, in the VSNCP Configure-Request, the UE shall set the “IPv4 Default Router Address” option to value 0.0.0.0 and the HSGW shall ignore the content of this option.

If the UE is attaching for emergency services, the VSNCP Configure-Request shall contain the Emergency Indicator configuration option with the value set to 1.

4.4.1.1.1.2 Handover Attach

The following parameters of significance to the IP address allocation process are sent by the UE on the VSNCP Configure-Request message for a handover attach:

- PDN Type
- PDN Address
- Protocol Configuration Options (PCO)
- Address Allocation Cause
- APN
- IPv4 Default Router Address, if PDN Type indicates IPv4 or IPv4v6
- IPv6 HSGW Link Local Address IID, if PDN Type indicates IPv6 or IPv4v6 and if the UE is operating in the tunneled mode

In the VSNCP Configure-Request message sent from the UE to the HSGW, the “PDN Type” option carries information on the UE IP capabilities. It shall be used to indicate to the HSGW whether the UE supports IPv4, IPv6, or IPv4v6.

In the VSNCP Configure-Request, on handover attach the “PDN Address” option will contain the valid IP address value(s) assigned to the UE for the APN. The PDN type field within the “PDN Address” option indicates what values the “PDN Address” option is carrying. Refer to section 9.1.4.1.1 for exact coding of the “PDN Address” option.

In the VSNCP Configure-Request, the PCO indicates the bearer control mode, and may contain an indication that deferred IPv4 address allocation is desired. See TS 29.275 [35].

In the VSNCP Configure-Request, the “Address Allocation Cause” option shall be set to a value of 0 (“Null value”).

Per section 9.1.4.2, in the VSNCP Configure-Request, if the UE has the currently assigned IPv4 default router address, the UE shall set the “IPv4 Default Router Address” option to the currently assigned IPv4 default router address. Per section 9.1.4.2, in the VSNCP Configure-Request, if the UE does not have the currently assigned IPv4 default router address, the UE shall set the IPv4 Default Router Address option to 0.0.0.0.
4.4.1.2 IP Address Allocation: Proxy Binding Update

4.4.1.2.1 Initial Attach

When the HSGW receives a VSNCP Configure-Request message indicating initial attach, it shall examine the “PDN Type” option to determine the UE’s IP capabilities, and compare this value to the subscription data for the APN. If the UE indicates support in the “PDN Type” option for IPv4v6 but the subscription data only allows IPv4 or IPv6 IP address for this APN, the HSGW shall set the PDN type to match the subscription limitation. If the resulting “PDN Type” option does not indicate support for at least one IP address type allowed by the subscription data for the APN, a VSNCP Configure-Reject message with error code set to “subscription limitation” shall be sent to the UE. See section 9.1.4.5.

If the “PDN Type” received from the UE includes at least one IP address type allowed by the subscription data for the APN, the HSGW constructs a Proxy Binding Update (PBU) message requesting IP address allocation according to the PDN Type by including appropriate options in the PBU (see TS 29.275 [35]) and sends it to the P-GW. Additionally, the “3GPP Vendor-Specific Mobility Option – Protocol Configuration Options” carries the PCO sent from the UE in the VSNCP Configure-Request message.

4.4.1.2.2 Handover Attach

When the HSGW receives a VSNCP Configure-Request message indicating handover attach, it shall examine the “PDN Address” option to determine the IP address(es) already assigned to the UE and compare this information to the subscription data for the APN. If the UE indicates IP address(es) that do not match the subscription data for this APN, the HSGW shall send a VSNCP Configure-Reject message to the UE.

Otherwise, the HSGW constructs a Proxy Binding Update (PBU) message including the already allocated IP address(es) and sends it to the P-GW.

4.4.1.3 IP Address Allocation: Proxy Binding Acknowledgement

4.4.1.3.1 Initial Attach

When the P-GW receives the PBU containing an indication for initial attach, it follows the 3GPP EPC procedures for allocation of IP addresses. See TS 23.402 [23] and TS 29.275 [35]. If the P-GW determines that the initial attachment to the APN cannot be completed, it will indicate that via the Status field in a PBA message. If the HSGW receives a 3GPP2-Reconnect-Indication mobility option in the PBA message with a status value of "129 Administratively prohibited" and MO Data set to “Reconnect to this APN not allowed”, then the HSGW shall send VSNCP Configure-Reject message to the UE with the error code set to “Reconnect to this APN not allowed”.

Assuming there are no errors, the P-GW returns the assigned IP address(es) in a PBA message to the HSGW. If the UE requested deferred IPv4 address allocation, and the P-GW supports deferred IPv4 address allocation, the Vendor-Specific Mobility Option of subtype “3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication” is returned to the HSGW in the PBA message (see TS 29.275 section 12.1.1.5 [35]).

If the HSGW had indicated IPv4 and IPv6 capabilities in the PBU, but the P-GW decided to allocate only IPv4 or IPv6, the P-GW also includes the Vendor-Specific Mobility Option of
subtype “3GPP Vendor-Specific PMIPv6 PDN Type Indication” in the PBA message to indicate the actual allocation and a cause value to indicate the reason for the change.

4.4.1.1.3.2 Handover Attach

When the P-GW receives the PBU containing an indication for handover attach, it follows the 3GPP EPC procedures for handover (see TS 23.402 [23] and TS 29.275 [35]). If the P-GW determines that the handover attachment to the APN cannot be completed, it will indicate that via the Status field in a PBA message. If the HSGW receives a 3GPP2-Reconnect-Indication mobility option in the PBA with a status value of “129 Administratively prohibited” and the MO Data is set to “Reconnect to this APN not allowed”, then the HSGW shall send a VSNCP Configure-Reject message to the UE with the error code set to “Reconnect to this APN not allowed”.

4.4.1.1.4 IP Address Allocation: VSNCP Configure-Ack

4.4.1.1.4.1 Initial Attach and Handover Attach

When the HSGW receives the PBA message from the P-GW indicating successful IP address allocation, it examines the contents to determine what IP address(es) have been allocated to the UE and constructs a VSNCP Configure-Ack message.

If the “IPv4 Address Acknowledgment option” option is present in the PBA message, the HSGW shall check whether a Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication" has been received in the PBA message.

- If no such deferred allocation indication was received, the IPv4 home address shall be copied to the “PDN Address” option in the VSNCP Configure-Ack message.
- If such deferred allocation indication has been received, the IPv4 address 0.0.0.0 shall be inserted in the "PDN Address" option. (NOTE: In this case, the UE has requested deferred IPv4 address allocation and it may request an IPv4 address via DHCPv4.)

If the “IPv6 Home Network Prefix” option is present, the IID shall be copied to the “PDN Address” option in the VSNCP Configure-Ack message. The UE shall use the IPv6 home network prefix that it receives in the RA message, refer to section 4.4.3.

If the UE included the IPv6 HSGW Link Local Address IID option, and if the Attach Type option is “Handoff”, and if the Tunnel Mode Indicator is set to 1 in the last received A11-Registration Request message for the UE, then the HSGW shall include the IPv6 HSGW Link Local Address IID option in the VSNCP Configure-Ack message and shall set the value to the interface ID of the HSGW link local address.

The PDN Type in the “PDN Address” option shall be set to indicate which address(es) is contained in the “PDN Address” option.

If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN Type Indication" is present in the PBA message, the PDN type value is copied to the “PDN Type” option in the VSNCP Configure-Ack message and to the PDN type field in the “PDN Address” option in the VSNCP Configure-Ack message.

If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN Type Indication" is present in the PBA message, the HSGW shall copy the cause field value to the “Address Allocation Cause” option in the VSNCP Configure-Ack message.
If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN Type Indication" is not present in the PBA message, then:

- If the HSGW changed the PDN Type received from the UE to match a subscription limitation for the APN, the HSGW shall set the “Address Allocation Cause” option to indicate “New PDN type due to subscription limitation”, see TS 29.275 clause 12.1.1.3 [35].
- If the HSGW did not change the PDN Type received from the UE, the HSGW shall set the “Address Allocation Cause” option in the VSNCP Configure-Ack message to 255 (“success”).

### 4.4.2 IPv4 Address Allocation during Default and Additional PDN Connection Establishment

This section specifies the case in which the IPv4 address is provided to the UE as part of the (default or additional) PDN connection establishment procedures (VSNCP signaling). For both home/visited PLMN-based and external PDN-based address allocation procedures, the P-GW obtains, allocates, refreshes, and releases IPv4 address for the UE.

( Default or additional) PDN connection is requested by the UE using a 3GPP2 VSNCP Configure-Request message. The UE that supports IPv4 shall indicate it by setting the PDN Type option to IPv4 or IPv4v6 in the VSNCP Configure-Request message. The UE shall indicate that it wants the IPv4 address allocated during the PDN connection establishment procedures using Address Allocation Preference contained in the PCO.

When the HSGW receives VSNCP Configure-Request, the HSGW triggers PMIPv6 procedures to the requested P-GW as specified in Section 5 if the UE is authorized to connect to it. The HSGW shall forward the Protocol Configuration Options (PCO) that are requested by the UE to the P-GW.

The P-GW allocates an IPv4 address during PDN connection establishment. The P-GW sends the allocated IPv4 address in the PBA message to the HSGW. If the UE indicated that it wants to obtain the IPv4 address during PDN connection setup procedures, the P-GW does not include the "3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication" option in the PBA message; therefore, the HSGW shall include the allocated IP address in the VSNCP Configure-Ack message sent to the UE.

See sections 5.4.1 and 9.3.1 for more details.

### 4.4.3 IPv6 Prefix Allocation via IPv6 Stateless Address Auto-configuration

For IPv6 prefix allocation the following procedures apply.

The HSGW shall act as the access router. Any prefix that the HSGW advertises to the UE is unique; therefore, there is no need for the UE to perform Duplicate Address Detection for any IPv6 address configured from the allocated IPv6 prefix. However, the HSGW shall respond with Neighbor Advertisement upon receiving Neighbor Solicitation messages from a given UE. For example, the UE may perform Neighbor Unreachability Detection towards the HSGW.

( Default or additional) PDN connection is requested by the UE using a 3GPP2 VSNCP Configure-Request message. The UE that supports IPv6 shall indicate it by setting the PDN Type option set to IPv6 or IPv4v6 in the VSNCP Configure-Request message.
When the HSGW receives VSNCP Configure-Request, the HSGW triggers PMIPv6 procedures to the requested P-GW as specified in Section 5 if the UE is authorized to connect to it. The HSGW shall forward the Protocol Configuration Options (PCO) that are requested by the UE to the P-GW.

The P-GW allocates an IPv6 prefix and the IPv6 interface identifier to the UE during PDN connection establishment. The P-GW sends the allocated IPv6 prefix and the IPv6 interface identifier in the PBA message to the HSGW. Upon receiving the PBA message, the HSGW shall send a VSNCP Configure-Ack message to the UE with the IPv6 interface identifier to the UE. Subsequently, the HSGW shall send Router Advertisement message to the UE including the assigned IPv6 prefix received in the PBA message.

After the UE has received the Router Advertisement message, it shall construct its full IPv6 address via IPv6 Stateless Address Autoconfiguration in accordance with RFC 4862 [76]. For privacy, RFC 3041 [57], the UE may change the interface identifier used to generate full IPv6 addresses, without involving the network. The UE may use stateless DHCPv6 for additional parameter configuration. The UE shall configure the HSGW IPv6 link local address using the Router Advertisement received from the HSGW.

If the UE is operating in the tunneled mode, the UE receives the interface ID of the HSGW Link Local Address in the VSNCP Configure-Ack message sent from HSGW to the UE.

The detailed call flow for IPv6 prefix allocation after the PDN connection establishment procedure is provided in section 4.4.5.4.

Stateless Address Autoconfiguration for IPv6 global and link local addresses are supported by the UE by default. Stateful address configuration using DHCPv6 is not supported in this specification per TS 23.402 [23].

### 4.4.4 IPv4 Address Allocation in eHRPD Access using DHCPv4

This section specifies the case in which the UE requests deferred IPv4 address allocation.

The UE that supports IPv4 shall indicate it by setting the PDN Type option to IPv4 or IPv4v6 in the VSNCP Configure-Request message. The UE shall indicate that it wants deferred IPv4 address allocation using Address Allocation Preference contained in the PCO. If the UE indicates using the Address Allocation Preference that it wants deferred IPv4 address allocation, and the P-GW chooses to allow deferred allocation, the P-GW includes the deferred IPv4 address allocation indicator (i.e., 3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication option) in the Proxy Binding Acknowledgement message. Upon reception of a Proxy Binding Acknowledgement message with a deferred IPv4 address allocation indicator included, the HSGW shall set the IPv4 address to 0.0.0.0 in the VSNCP Configure-Ack message, even if an IPv4 address is assigned by the P-GW. If the HSGW receives the UE’s IP address through PMIP tunnel establishment without the deferred IPv4 address allocation indicator included, the HSGW shall set the IPv4 address in the VSNCP Configure-Ack message to the IPv4 address that is received from the P-GW.

If the UE receives an IPv4 address during the PDN connection establishment, the UE shall not use DHCPv4 for another address allocation to the same PDN connection even if the UE indicates deferred IP address allocation in PCO.

The UE that requested deferred IPv4 address allocation may send the DHCPDISCOVER message to the HSGW. If the UE supports RFC 4039 [70], the UE shall send the DHCPDISCOVER message with Rapid Commit option.
If the HSGW receives a DHCPDISCOVER message, the HSGW shall act as a DHCPv4 relay agent and forward the DHCPv4 message within the PMIPv6 tunnel to the P-GW.

When the HSGW receives a DHCPDISCOVER message, if the HSGW had previously received a PBA message with the deferred IPv4 address allocation indicator and no IPv4 Address Acknowledgement option, the HSGW also triggers PMIP procedures as specified in Section 5 to obtain the IPv4 address allocated to the UE, as well as the IPv4 default router address.

If the UE receives the DHCPACK with Rapid Commit, the UE shall configure its IP address with the IP address in the ‘yiaddr’ field. If the UE receives the DHCPACK with Rapid Commit, the UE shall configure its IP address with the IP address in the ‘yiaddr’ field, and shall set the IPv4 Default Router Address to the value of the IPv4 Default Router Address field.

If the UE receives the DHCPOFFER message from the HSGW, the UE shall send the DHCPREQUEST message to the HSGW. The ‘requested IP address’ option shall be set to the value of ‘yiaddr’ contained in the DHCPOFFER message from the HSGW. When the UE receives the DHCPOFFER message from the HSGW, the UE shall configure its IP address with the IP address in the ‘yiaddr’ field, and shall set the IPv4 Default Router Address to the value of the IPv4 Default Router Address field.
4.4.5 Call Flows

This section shows example call flows for IPv4 and IPv6 address allocation. Note that the PCRF interaction is not shown in the call flows.

4.4.5.1 IPv4 Address Allocation during PDN Connection Establishment

Figure 15 illustrates an example call flow for IPv4 address allocation during PDN connection establishment.

Figure 15 IPv4 address allocation during PDN connection establishment

1. The UE has performed successful authentication and is attached to the eHRPD access network.

2. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, APN, PDN Type, PDN Address (IPv4, PDN Address=0), Protocol Configuration Options, IPv4 Default Router Address, and Attach Type (Initial Attach). Using the Address Allocation Preference contained in the PCO, the UE indicates that it wants to perform IPv4 address allocation during the PDN connection establishment procedure.

3. Since the Attach Type is set to “Initial Attach” in this call flow, the HSGW selects a new P-GW based on APN received from HSS/HAAA (for default PDN connection, if the UE does not identify a requested APN in step 2) or received from the UE. The HSGW sends a PMIPv6 Binding Update to the P-GW. See 3GPP 23.402 [23] and 29.275 [35].

4. The P-GW updates the 3GPP AAA Server/HSS with P-GW’s identity (i.e., FQDN, or IP address). See 3GPP 23.402 [23].

5. The P-GW responds with a PBA message to the HSGW. See 3GPP 23.402 [23] and 29.275 [35].
6. The HSGW sends a VSNCP Configure-Ack message (PDN-ID, APN, PDN Type, PDN Address, IPv4 Default Router Address, PCO, and Attach Type) to the UE over the main service connection. The PDN Address option contains an IPv4 address received in the PBA message (step 5).

7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The information in the message includes the PDN-ID configuration option. This message also includes the APN-AMBR if received from the HSS/AAA.

8. The UE responds with a VSNCP Configure-Ack message (PDN-ID). This message also includes the APN-AMBR configuration option if received from the HSGW in the VSNCP Configure-Request and if the APN-AMBR is supported by the UE.
**IPv4 Address Allocation with DHCPv4 Rapid Commit Option**

Figure 16 illustrates an example call flow for IPv4 address allocation using DHCPv4 Rapid Commit Option (see TS 23.402 [23]). In the example provided the UE sets PDN Type to IPv4 in VSNCP Configure-Request, indicating that it supports IPv4 only. This example also applies to a UE that indicates IPv4v6 capabilities, but the HSGW limits the PBU to IPv4 only due to subscription limitation for the APN.

1. UE is authenticated and attached to the eHRPD access network

2. VSNCP Configuration-Request (PDN-ID, APN, PDN Type, PDN Address=0, PCO, Attach Type, Address Allocation Cause, IPv4 Default Router Address)

3. PMIP Binding Update (Handoff Indicator, etc.)

4. PDN-GW updates HSS/AAA with P-GW address

5. PMIP Binding Ack (Deferred IPv4 Address Allocation Indicator)

6. VSNCP Configuration-Ack (PDN-ID, APN, PDN Type, PDN Address=0, PCO, Attach Type Address Allocation Cause, IPv4 Default Router Address=0)

7. VSNCP Configuration-Request (PDN-ID)

8. VSNCP Configuration-Ack (PDN-ID)

9. DHCPDISCOVER with Rapid Commit

10. DHCPDISCOVER with Rapid Commit

11. DHCPACK with Rapid Commit (IPv4 Address, IPv4 Default Router Address)

12. DHCPACK with Rapid Commit (IPv4 Address, IPv4 Default Router Address)

---

**Figure 16 IPv4 Address Allocation using DHCPv4 with Rapid Commit Option**

1. The UE has performed successful authentication and is attached to the eHRPD access network.

2. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, APN, PDN Type, PDN Address (IPv4, PDN Address=0), IPv4 Default Router Address, Protocol Configuration Options, and Attach Type (Initial Attach). Using the Address Allocation Preference contained in the PCO, the UE indicates that it wants deferred IPv4 address assignment.

3. Since the Attach Type is set to “Initial Attach” in this call flow, the HSGW selects a new P-GW based on APN received from HSS/HAAA (for default PDN connection, if the UE does not identify a requested APN in step 2) or received from the UE. The HSGW sends a PBU to the P-GW. See 3GPP 23.402 [23] and 29.275 [35].

4. The P-GW updates the 3GPP AAA Server/HSS with P-GW’s identity (i.e., FQDN, or IP address). See 3GPP 23.402 [23].
5. The P-GW responds with a PBA message to the HSGW. The P-GW in this scenario includes 3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication option in the Proxy Binding Acknowledgement message indicating that the UE requested deferred IPv4 address allocation. The P-GW in this case assigns and returns an IPv4 address and an IPv4 default router address to the HSGW as described in section 4.4.1.1.3. See 3GPP 23.402 [23] and 29.275 [35].

6. The HSGW sends a VSNCP Configure-Ack (PDN-ID, APN, PDN Type, PDN Address, IPv4 Default Router Address, PCO, and Attach Type) message to the UE over the main service connection. Note that the PDN address in VSNCP Configure-Ack contains the 0.0.0.0 address since the HSGW received a deferred IPv4 address allocation indicator in the Proxy Binding Acknowledgement message in step 5. In the case that the UE had indicated IPv4v6 capabilities in step 2, but the HSGW indicated only IPv4 in the PBU in step 3, then the HSGW sets the Address Allocation Cause option to “New PDN type due to subscription limitation”.

7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The information in the message includes the PDN-ID configuration option. This message also includes the APN-AMBR configuration option if received from the HSS/AAA.

8. The UE responds with a VSNCP Configure-Ack message. The information in the message includes the PDN-ID configuration option. This message also includes the APN-AMBR configuration option if received from the HSGW in the VSNCP Configure-Request and if the APN-AMBR is supported by the UE.

9. The UE sends a DHCPDISCOVER message with the Rapid Commit option in broadcast to the network to find available servers.

10. Upon receiving the DHCPDISCOVER with Rapid Commit message, the HSGW acting as a DHCPv4 Relay Agent shall add its address in the GIADDR option and add the assigned UE IP address (received from P-GW in the PBA message) in the "Address Request" option, and relay the message in unicast within the PMIPv6 tunnel to the P-GW. The P-GW acts as a DHCPv4 server.

11. When receiving the DHCPDISCOVER message, the P-GW should verify the GIADDR option. Then the P-GW uses "Address Request" option to identify the UE binding and update it with the 'client identifier' and 'chaddr' combination for subsequent DHCPv4 procedure.

   The P-GW extends the IP lease offer and sends a DHCPACK message with the Rapid Commit option to the HSGW. This message is sent through the PMIPv6 tunnel established between the HSGW/MAG and the P-GW/LMA.

12. The HSGW forwards the DHCPACK with the Rapid Commit option to the UE.
4.4.5.3 IPv4 Address Allocation without DHCPv4 Rapid Commit Option

Figure 17 illustrates an example call flow for IPv4 address allocation by using DHCPv4 without the DHCPv4 rapid commit option (see TS 23.402 [23]). In the example provided the UE sets PDN Type to IPv4 in VSNCP Configure-Request, to indicate that it supports IPv4 only. This example also applies to a UE that indicates IPv4v6 capabilities, but the HSGW limits the PBU to IPv4 only due to subscription limitation for the APN.

![Diagram of IPv4 Address Allocation using DHCPv4 without Rapid Commit Option](image)

**Figure 17  IPv4 Address Allocation using DHCPv4 without Rapid Commit Option**

1. The UE has performed successful authentication and is attached to the eHRPD access network.

2-8. Steps 2 to 8 are the same as steps 2 to 8 specified in section 4.4.5.2.

9. The UE sends a DHCPDISCOVER message in broadcast to the network to find available servers.

10. Upon receiving the DHCPDISCOVER message, the HSGW acting as a DHCPv4 Relay Agent shall add its address in the GIADDR option and add the assigned UE IP address (received from P-GW in the PBA message) in the "Address Request" option, and relay the message in unicast within the PMIPv6 tunnel to the P-GW acting as a DHCPv4 server.

11. When receiving the DHCPDISCOVER message, the P-GW should verify the GIADDR option. Then the P-GW uses "Address Request" option to identify the UE binding and update it with the 'client identifier' and 'chaddr' combination for subsequent DHCPv4 procedure.
After that the P-GW extends an IP lease offer and sends the DHCPoffer with the assigned
UE IP address.

12. The HSGW acting as DHCPv4 Relay Agent relays the DHCPv4 message to the UE.

13. When the UE receives the lease offer, it sends a DHCPREQUEST message containing the
received IP address.

14. The HSGW acting as DHCPv4 Relay Agent relays the DHCPv4 message to the P-GW.

15. When the P-GW receives the DHCPREQUEST message from the UE, it sends a DHCPack
message to the UE. This message includes the lease duration and any other configuration
information that the client might have requested.

16. The HSGW acting as DHCPv4 relay agent relays the DHCPv4 message to the UE.
### 4.4.5.4 IPv6 Address Allocation

Figure 18 shows an example call flow for IPv6 address allocation.

---

**Figure 18 IPv6 Address Allocation**

1. The UE and the network has performed successful authentication and is attached to the eHRPD access network.

2. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, APN, PDN Type, PDN Address (IPv6, PDN address=0), Protocol Configuration Options, Attach Type (Initial Attach).

3. Since the Attach Type is set to “Initial Attach”, the HSGW selects a new P-GW based on APN received from HSS/HAAA (for the default PDN connection, if the UE does not identify a requested APN in step 2) or received from the UE. The HSGW sends a PBU to the P-GW. See 3GPP 23.402 [23] and 29.275 [35].

4. The P-GW updates the 3GPP AAA Server/HSS with P-GW’s identity (i.e., FQDN, or IP address). See 3GPP 23.402 [23].

5. The P-GW responds with a PBA message to the HSGW. See 3GPP 23.402 [23] and 29.275 [35].
6. The HSGW sends a VSNCP Configure-Ack message (PDN-ID, APN, PDN Type, PDN Address, PCO, and Attach Type) to the UE over the main service connection. The PDN Address Information contains the IPv6 interface ID in this example.

7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID configuration option. This message also includes the APN-AMBR if received from the HSS/AAA.

8. The UE responds with a VSNCP Configure-Ack message that contains the PDN-ID configuration option.

9. This step is optional. The UE may send a Router Solicitation (RS) message to the HSGW via the eAN.

10. Upon receiving the Route Solicitation message or any time after step 8, the HSGW sends an IPv6 Router Advertisement message (see RFC 4862 [76]) to the UE which includes the UE’s home network prefix.

11. The UE generates an IPv6 global unicast address via IPv6 stateless address auto-configuration (see RFC 4862 [76]). The UE may use the interface ID received from step 6 to configure its link local IPv6 address.
4.5 Quality of Service

The HSGW performs a number of Quality of Service related functions that are defined for the PDSN in X.S0011 [6]. Such functions include the following:

- TFT handling
- Downlink bearer binding based on policy information.
- Uplink bearer binding verification with packet dropping of traffic that does not comply with established uplink policy.
- Transport level packet marking in the uplink and the downlink based on the assigned QCI.

The HSGW shall perform bearer establishment procedures, e.g., trigger the creation of link flows, TFTs, and mapping of downlink flows to A10 connections in accordance with X.S0011 [6] and in accordance with this specification. Bearer establishment procedures may occur directly over the eHRPD air interface or via S101.

Policy related QoS processing, including uplink packet marking, traffic shaping, etc, are performed in the P-GW in accordance with TS 23.203 [20] and TS 23.402 [23]. For E-UTRAN/eHRPD interworking scenarios, that same paradigm is followed; hence, these functions are not performed in the HSGW.
4.5.1 The EPS Bearer with PMIP-based S2a and eHRPD Access

The 3GPP Evolved Packet System (EPS) provides IP connectivity between a UE and an external packet data network. This is referred to as PDN Connectivity Service. The PDN Connectivity Service supports the transport of one or more IP flows (also known as Service Data Flows (SDFs) and is defined in TS 23.401 [22]).

Figure 19 shows an example bearer mapping in eHRPD.

Figure 19 Sample Bearer Mapping in eHRPD

* PDN-ID is used to multiplex EPS bearers from multiple PDNs. PDN-ID is used on auxiliary service connections configured with SO72, on HDLC-based framing auxiliary service connections configured with SO64, and on the main service connection configured with SO59.

An EPS bearer is mapped to a service connection in one of the two ways: (1) by multiplexing EPS bearers from multiple PDNs over a single service connection by using the PDN-ID, or (2) by assigning only one EPS bearer to a dedicated service connection, in which case the PDN-ID is not used. The choice of mapping approach and the assigned service connection is communicated to the UE and HSGW by the eAN/ePCF.

If an eHRPD BE auxiliary service connection has been created, then the BE IP packets (SDFs) from all PDNs are multiplexed across that BE auxiliary service connection (i.e., using SO72) by including an extra octet immediately ahead of the IP packet. This extra octet shall contain the PDN-ID of the PDN that the IP packet is associated with. This is referred to as PDN multiplexing (PDN-Mux). Otherwise, the BE IP packets from all PDNs shall be multiplexed across the main service connection. See section 9.1.5 for the stage 3 details on the use of the main service connection to carry multiplexed IP traffic using VSNP.

- Other auxiliary service connections (i.e., using SO72) may be created to support multiplexing of traffic with similar QoS from multiple PDNs by including an extra
octet immediately ahead of the IP packet. This extra octet shall contain the PDN-ID of
the PDN that is the source/destination of the IP packet (PDN-Mux).

- Auxiliary service connections that use packet-based framing but do not use
  multiplexing of IP packets from multiple PDNs shall use SO67. SO67 shall not be
  used for a multiplexed auxiliary service connection.

Signaling traffic between the HSGW and UE shall be carried on the main service connection.

IP packets (SDFs) from all PDNs shall be multiplexed across the main service connection or
HDLC-based framing auxiliary service connections by the inclusion of a PDN Identifier field
immediately ahead of the IP packet. This PDN Identifier field shall contain the PDN-ID of
the PDN that the IP packet is associated with. See section 9.1.5 for the stage 3 details of the
use of the main service connection to carry multiplexed IP traffic using VSNP.

QoS control between a HSGW and a P-GW is provided at the Transport Network Layer
(TNL).

An EPS bearer is realized by the following elements:

- Uplink TFTs in the UE bind one or more IP flows (SDFs) to an EPS bearer in the
  uplink direction.
- Downlink TFTs in the HSGW bind one or more IP flows (SDFs) to an EPS bearer in
  the downlink direction.
- A radio bearer (RLP link) transports the packets of an EPS bearer between a UE and
  an eAN.
  - BE SDFs for all PDNs are mapped to the radio bearer that is configured for
    BE flows. Only one radio bearer is used for BE flows.
  - SDFs for multiple PDNs can also be mapped onto the radio bearer that is
    configured as the main service connection.
  - Packet framed EPS bearers and HDLC framed EPS bearers for multiple
    PDNs can be mapped onto a packet-based framing (SO72) and HDLC
    framing (SO64) auxiliary service connection, respectively, by the inclusion
    of a PDN Identifier field.
  - A packet framed EPS bearer can be mapped onto a packet-based framing
    (SO67) dedicated auxiliary service.
- The UE stores a mapping between an uplink packet filter and a radio bearer to create
  the binding between SDFs and a radio bearer in the uplink.
- The eAN stores a one-to-one mapping between a radio bearer and an A8 bearer to
  create the binding between a radio bearer and an A8 bearer in both the uplink and the
downlink directions.
- The ePCF stores a one-to-one mapping between an A8 bearer and an A10 bearer to
  create the A8/A10 bearer binding in both the uplink and downlink directions.
- An HSGW stores a mapping between downlink packet filters and an A10 bearer to
  create the binding between SDFs and an A10 bearer in the downlink.
The PDN Connectivity Service between a UE and an external packet data network is supported through a concatenation of an EPS Bearer and IP connectivity between HSGW and P-GW. Over the PMIP-based S2a interface, the transport of IP flows going to the P-GW is realized as follows:

- A per-UE per PDN tunnel transports the packets of EPS bearers between the HSGW and a P-GW. There is a many-to-one mapping between EPS bearers and this per-UE, per PDN tunnel.

- In the uplink direction in the case of multiplexed A10 connections, the HSGW shall use the PDN-ID information associated with the flow to determine the PDN tunnel. In the case of non-multiplexed A10 connections, the traffic is associated with only a single PDN; therefore, the A10 context can be used to determine which PDN the traffic belongs to.

4.5.2 Mapping Parameters for Multi-PDN connectivity

In eHRPD each SDF is mapped onto a single reservation identified by a Reservation Label, which in turn is mapped to an EPS bearer as described in the previous section. The UE and the eHRPD eAN identify a specific QoS IP flow with a unique number known as a Reservation Label. The EPS bearers are established on a per-QoS/per-PDN basis.

4.5.3 Network Initiated Dedicated Bearer Procedures for eHRPD Access

In eHRPD, UE initiated procedures are used to create link flows to support various applications and their QoS requirements. Depending on the requirements of a particular set of IP flows the eAN associates new Reservations with existing RLP flows, or creates new RLP flows if required. These procedures can be reused in the context of 3GPP network initiated bearer setup. To accomplish this, PCC methods are used in conjunction with RSVP messages to trigger eHRPD signaling. The procedures described in TS23.401 [22] and TS23.402 [23] for network initiated dedicated bearer setup, modification and deletion are used to trigger eHRPD procedures for bearer establishment and IP flow mapping. The encapsulation of RSVP messages over the main service connection is described in section 9.1.2.

4.5.3.1 Dedicated Bearer Activation

The following diagram illustrates network initiated dedicated resource allocation operations for eHRPD which are triggered by the PCRF. The procedures shown include PCRF interactions described in TS 23.402 [23] and eHRPD specific procedures. The bearer to be established is assumed in this example to be related to a PDN with which the UE has a current PDN connection.

On receiving the Gateway Control and QoS Rules Provisioning message from the PCRF, the HSGW decides that a new bearer needs to be activated, the HSGW uses this QoS policy to assign the bearer QoS, (i.e., it maps PCC QoS parameters to a set of eHRPD FlowProfileIDs). The HSGW follows this with the procedure shown in Figure 20 by sending an RSVP Resv message to the UE.
Figure 20  Network Initiated Dedicated Bearer Setup

Both the roaming and non-roaming scenarios are depicted in Figure 20. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules from the hPCRF in the hPLMN to the HSGW in the vPLMN. The vPCRF receives the Acknowledgment from the HSGW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved.

1. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20] by sending a message with the QoS rules and Event Trigger information to the HSGW.

2. The HSGW uses the received QoS policy information to determine the bearer level QoS parameters required for the eHRPD bearer. The HSGW maps these parameters to the appropriate eHRPD FlowProfileID(s) (see C.R1001 [12]).

3. The HSGW sends an RSVP Resv message transported over the main service connection. As indicated in section 9, the RSVP Resv message encapsulation includes the PDN-ID of the PDN for which the bearer is being created. The RSVP Resv message includes the Uplink/Downlink packet filter, the QoS list, and a Transaction ID. See section 9.1.6.7.1 for parameter details.

4. The UE performs the standard QoS establishment procedures defined in C.S0024 [7] and in C.S0063 [13]. There are two possible sequences that can occur at this step. If a new QoS link flow connection is needed to carry the new flow over the air interface, then the eAN will setup a new air interface link flow. If the eAN decides to carry the flow(s) on an existing link flow, it then reconfigures the parameters of that link flow.
5. If a new link flow is needed, a new A10 connection is also established. The eAN/ePCF sends an A11-Registration Request message to the HSGW indicating the GRE key, the Requested QoS information, and the Granted QoS information for the flow. The Granted QoS information includes the FLOW_ID. If a new QoS link flow is not needed, the eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, FLOW_ID, and the modified Granted QoS information for the existing connection (if required).

6. The UE sends an RSVP Resv message to the HSGW. The message includes the Flow ID for the bearer connection, and the same DL/UL TFT and Transaction ID received in step 3. This message can be sent in parallel with the start of the signaling in Step 4. The Transaction ID is used to associate the returned Flow ID with the new bearer connection. This message is also used as an acknowledgement to the RSVP Resv message in Step 3. The HSGW examines the QoS granted to the UE and compares it to the QoS authorized for the UE in step 2. If there is a discrepancy, the HSGW applies operator policy.

7. The HSGW acknowledges the delivery of the RSVP Resv message it received in Step 6 by sending a ResvConf message to the UE.

8. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or eAN) may trigger the transition to the open state.

9. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an A11-Registration Request (Active Start) message to initiate the accounting for this bearer connection.

10. Any time after Step 6 the HSGW responds to the PCRF indicating its ability to enforce the rules provisioned to it in Step 1 and thus completing the Gateway Control and QoS Rules Provision Ack procedure started in step 1.


NOTE: Step 11 may occur before step 2 or may be performed in parallel with steps 1 and 10 if acknowledgement of resource allocation is not required to update PCC rules in the PCEF. For details please refer to TS 23.203 [20].

4.5.3.2 Dedicated Bearer Deactivation

This section describes procedures for bearer deactivation. In the context of eHRPD an IP flow(s) associated with the allocated resources may be stopped, however the allocated resources are not torn down in anticipation of being used again. If the resources allocated for the IP flow(s) are no longer needed the network may trigger a complete release of the eHRPD resources associated with the flow (e.g., RLP and auxiliary A10).

4.5.3.2.1 PCRF Initiated Dedicated Bearer Deactivation

This procedure applies to cases where the QoS rules provided by the PCRF to the HSGW result in a decision to release or modify one or more of the established EPS bearers.

Network initiated bearer deactivation shall take into account the deactivation of both dedicated auxiliary service connections and the removal of bearers from a PDN-ID multiplexed shared service connection. While removing a bearer from a multiplexed shared service connection, it is necessary to retain the shared service connection for connectivity to other PDNs. A service connection is removed when the last Reservation associated with the service connection is removed.

This call flow assumes the PCRF initiated modification or release of an EPS bearer.
**Figure 21**  PCRF Initiated Dedicated Bearer Deactivation

1. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20] by sending a message with the QoS rules and Event Trigger information to the HSGW.

2. The HSGW sends a Resv message to the UE with OpCode set to ‘Initiate Delete Packet Filter from Existing TFT’ indicating the EPS bearer deletion. The message is indexed with the PDN-ID of the PDN for which the EPS bearer is being deleted.

3. The UE performs standard HRPD procedures to reconfigure the air interface in order to remove or modify the requested Reservation(s). If the last Reservation(s) associated with the link flow is removed, the link flow itself is also removed.

4. The eAN sends an A11-Registration Request message to the HSGW indicating the removed Flow ID(s). If the last Flow ID associated with the auxiliary A10 is removed, the auxiliary A10 itself is removed.

5. The UE sends a Resv message with OpCode set to ‘Initiate Delete Packet Filter from Existing TFT’ to indicate to the HSGW which flows have been removed. The TFT IE contains the list of flow identifiers for which filters have been deleted. The Transaction ID carried in this message shall be the same as the Transaction ID carried in the Resv message in step 2. This message is also used as an acknowledgement to the RSVP Resv message in Step 2.

6. The HSGW acknowledges a successful update of the IP flow mapping information by sending a ResvConf message to the UE.

7. The HSGW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not by sending a Gateway Control and QoS Rules Provision Acknowledgment message.

8. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203. The PCRF provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules Provision procedure specified in TS 23.203 [20].
NOTE: Step 8 may occur before step 1 or performed in parallel with steps 1 and 7 if acknowledgement of resource de-allocation is not required to update PCC rules in the PCEF. For details please refer to TS 23.203 [20].

4.5.4 UE Initiated Dedicated Bearer Procedures for eHRPD

4.5.4.1 UE Initiated Resource Request, Modification and Release

The UE requested bearer resource allocation and release model for eHRPD shall follow TS23.203 [20] and TS23.402 [23]. In the PCC model the UE request resources which are in turn granted and established by the network or modified and deleted depending on the nature of the UE request.

4.5.4.1.1 UE Requested Bearer Resource Allocation

The call flow in Figure 22 illustrates UE requested bearer activation procedures.

Figure 22 UE Requested Bearer Resource Allocation
1. The UE sends a Resv message to the HSGW with OpCode set to ‘QoS-Check’. The UE encapsulates the Resv message over the main service connection using VSNP and includes the PDN-ID to indicate to which PDN the additional bearer resource is linked. The message contains the UE requested FlowProfileIDs. The Transaction ID is dynamically allocated by the UE for UE requested bearer resource activation procedure. In the example presented in the figure, Transaction ID is 1.

2. The HSGW maps the received FlowProfileID(s) into a single set of QCI/MBR/GBR parameters.

3. The HSGW uses Gateway Control and QoS Rules Request/Reply procedures to validate UE requested QoS with the hPCRF. If the HSGW is deployed in a roaming scenario, the message including QCI/MBR/GBR(s) and packet filter(s) is sent to the vPCRF and the vPCRF forwards it to the hPCRF.

4. The HSGW maps the validated policy rules into appropriate FlowProfileID(s) that are being requested.

5. The HSGW sends a ResvConf message to the UE with OpCode set to ‘QoS-Check Conf’. The Resv message is an RSVP message transported over the main service connection. The ResvConf message contains the authorized FlowProfileIDs, which is the same or a subset of the UE requested FlowProfileIDs in step 1, and the same Transaction ID as in the Resv message sent in step 1. This step is used as an acknowledgment of the Resv message sent in step 1.

6. The UE performs the standard HRPD QoS establishment procedures defined in C.S0087 [15] / C.S0063 [13] using the authorized FlowProfileID list from step 5. There are two possible sequences that can occur at this step. If a new QoS link flow connection is needed to carry the new flow over the air interface, then the eAN will setup a new air interface link flow. If the eAN decides to carry the flow(s) on an existing link flow, it then reconfigures the parameters of that link flow.

7. If a new link flow is needed, a new A10 connection is also established. The eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, the Requested QoS information, and Granted QoS information for the flow. The A11 message includes the FLOW_ID. If a new QoS link flow is not needed, the eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, FLOW_ID, and the modified Granted QoS information for the existing connection (if required).

8. The UE sends a Resv message to the HSGW to associate the selected Reservation with the appropriate A10 connection and TFT. The message includes the Flow ID and associated packet filters for which the FlowProfileID(s) are authorized at step 5. This message can be sent in parallel with the start of the signalling in Step 6. The Transaction ID is different than that used in steps 1 and 5 to avoid having the HSGW view this message as a repetition of the message in step 1. The HSGW examines the QoS granted to the UE and compares it to the QoS authorized for the UE in step 5. If there is a discrepancy, the HSGW applies operator policy.

9. The HSGW acknowledges the Resv message with a ResvConf message.

10. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or eAN) may trigger the transition to the open state.

11. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an A11-Registration Request (Active Start) message to initiate the accounting for this bearer connection.

12. Upon a successful negotiation of QoS, the HSGW sends the acknowledgement to the PCRF based on the QoS that was selected in step 2.

13. The IP CAN Session Modification Procedure may occur as the result of the Gateway Control and QoS Rules Request message, either to forward an Event Report to the P-GW (PCEF) or to
issue revised PCC Rules and Event Triggers, or both an Event Report and a Rules and
Triggers provision. If an indication that resources have been acquired is not required then this
step may occur any time after step 3, above.

4.5.4.1.1 HSGW Treatment of Network and UE Initiated Deactivation of the Same Flow

Both the network and the UE may attempt to clean up the same packet filters at the same time.
This condition arises when the UE initiates deactivation of the packet filters and the signaling
arrives at the PCRF nearly at the same time as the signaling from the application in the
network.

If the HSGW receives a request from the UE to clean up the packet filter, then the HSGW
triggers UE requested packet filter clean up by sending a ‘Gateway Control and QoS Policy
Rules Request’ to the PCRF and waits for the response from the PCRF. If instead of
receiving a response to this message, the HSGW receives a ‘Gateway Control and QoS Rules
Provision’ message for the same packet filter from the PCRF, this is an indication that the
PCRF is initiating a packet filter clean up which results in the race condition, where both UE
and PCRF are trying to clean up the packet filter.

If the HSGW receives a ‘Gateway Control and QoS Rules Provision’ message from the PCRF
for a packet filter and if the HSGW had already sent a ‘Gateway Control and QoS Rules
Request’ message for the same packet filter, then the HSGW shall omit steps 2 – 6 in Figure
21 and shall acknowledge the request from the PCRF by sending a ‘Gateway Control and

The PCRF completes the UE requested packet filter clean up procedure by sending the
‘Gateway Control and QoS Rules Reply’ message.

To enable the above behavior, if the HSGW receives a request from the UE to release the
packet filter, then the HSGW shall unbind all the QoS rules that are mapped to the packet
filter and shall set the QoS rules to inactive state. If the QoS rules for a certain packet filter
are in the inactive state, and if the HSGW receives a request from the PCRF to release the
packet filter, then the HSGW shall not trigger a network initiated packet filter deletion.
4.5.4.1.2 UE Requested Radio Bearer State Modification

The UE requested bearer resource model allows for efficiencies at the eHRPD air interface by not requiring the deletion of bearers at the radio level and from the eAN/ePCF to the HSGW. Instead, radio reservations can be placed in the Reservation Off state. An example is shown in Figure 23.

**Figure 23** UE Requested Radio Bearer State Modification

1. Upon completion of the use of a bearer with specific QoS, e.g., a VoIP bearer, the UE sends a request to the eAN to set the radio reservation for the bearer to the Off state, and the eAN acknowledges the change to the Off state.
2. The eAN/ePCF sends an A11-Registration Request message to the HSGW with an Active Stop indication to inform the HSGW of the idle state of the Flow ID.
3. The HSGW acknowledges the A11-Registration Request message.
4. The eAN/ePCF and HSGW maintain the A10 connection used for the QoS bearer. This bearer may be reused later for the same IP flow, e.g., for another VoIP call to the same IP address on the UE. Such reuse would involve only the setting of the radio reservation state to the On state, and the sending of Active Start Airlink Records to the HSGW.
5. The UE and HSGW maintain the TFTs for the QoS Bearer.
4.6 Policy and Charging

This section describes the functions associated with policy and charging which are part of EPC – eHRPD Connectivity and Interworking Architecture (see Figure 24).

Per TS 23.401 [22] and TS 23.402 [23], an EPS needs to support both PCEF and PCRF functionality to enable dynamic policy and charging control by means of installation of PCC rules based on user and service dimensions. However, an EPS may only support PCEF functionality in which case it shall support static policy and charging control.

The procedures defined in this specification assume that deployment of dynamic policy and charging control (PCC) will be consistent throughout the network.

All call flows in this specification, unless noted otherwise, assume the use of PCC.

NOTE: The local configuration of PCEF static policy and charging control functionality is not subject to standardization. The PCEF static policy and control functionality is not based on subscription information.

The HSGW network element implements the Bearer Binding and Event Reporting Function (BBERF) needed to interwork EPC with eHRPD (see Figure 24).

4.6.1 Application of 3GPP PCC to the HSGW

The BBERF in the HSGW performs bearer binding and event reporting as defined in TS 23.203 [20] and follows the framework defined in TS 23.402 [23] for QoS policy control. Full policy and charging enforcement functionality with service-aware end-user charging is located only in the P-GW. The BBERF communicates with the PCRF in the EPC using the Gxa interface as defined in TS 23.203 [20].
4.6.2 3GPP Gxa Interface (Diameter)

To enable its bearer binding and event reporting functions, the HSGW BBERF communicates with the PCRF using the Gxa reference point.

The Gxa reference point shall satisfy the following architectural principles of TS 23.402 [23]:

1. Gxa shall be based on an evolution of the Gx application specified in TS 29.212 [29].

2. Gxa shall support transfer of QoS parameters and related packet filters.

3. Gxa shall support transfer of control information.

The service level QoS parameters are conveyed in QoS rules and their definition and usage are discussed in TS 23.401 [22] and TS 23.402 [23]. The service level QoS parameters consist of:

- QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP) for both Guaranteed Bit-Rate and non-Guaranteed Bit Rate bearers.

- Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR) parameters for Guaranteed Bit Rate bearers.
### 4.6.2.1 Gxa 3GPP2 AVPs

The following defines the 3GPP2 Diameter AVPs used by Gxa.

#### 3GPP2-BSID AVP

The AVP 3GPP2-BSID (Code 5535/9010) is of type UTF8String and the data is formatted according to the 3GPP2 RADIUS VSA BSID defined in [5].

TS 29.212 [29] uses the 3GPP2 Diameter AVP 3GPP2-BSID.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Value Type</th>
<th>Shall</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP2-BSID</td>
<td>5535/9010</td>
<td>UTF8String</td>
<td>M,V</td>
<td>M</td>
<td>P</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: The AVP header bit denoted as ‘M’ indicates whether support of the AVP is required. The AVP header bit denoted as ‘V’ indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [63].

### 4.6.3 Charging

Accounting functionality is provided by the HSGW and the P-GW. The BBERF function in the HSGW shall collect accounting information for each UE i.e., the amount of data transmitted in uplink and downlink directions. The accounting related functionality provided by the HSGW is aligned with the accounting functionality defined for the S-GW in TS 23.401 [22]. The charging functions in the HSGW, with associated interfaces shall be supported as specified in TS 32.240 [37]. The behavior of the charging functions in eHRPD EPC domain, the reporting of the chargeable events, and creation of the CDRs shall be as specified in TS 32.240 [37] and TS 32.251 [38].

The P-GW provides charging functionality for each UE according to TS 23.203 [20].

### 4.6.4 Policy interworking During Handoffs

In the scenario where a handoff from E-UTRAN to eHRPD is performed some policy interaction may be needed between the HSGW and the EPC PCRF (see TS 23.402 [23]).

### 4.6.5 Priority and Conflict Resolution

Priority and conflict resolution follows the principles described in TS 23.203 [20].
### 4.6.6 Mapping between 3GPP QoS parameters and eHRPD QoS Parameters

An EPS bearer is the level of granularity for bearer level QoS control in the E-UTRAN/eHRPD interworking scenario. That is, SDFs mapped to the same EPS bearer receive the same bearer level packet forwarding treatment (e.g., scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different bearer level QoS to two SDFs thus requires that a separate EPS bearer is established for each SDF.

The bearer level packet forwarding treatment (e.g., scheduling and rate control) for 3GPP access is determined by QCI, GBR, MBR, UE-AMBR, and APN-AMBR, which are described in TS 23.401 [22].

The FlowProfileID for eHRPD networks identifies the QoS needs for an application flow. Each flow profile is identified by a unique FlowProfileID to facilitate proper processing within the network and mobile stations. The 16-bit FlowProfileID is composed of two fields: the FlowProfileID Type field (2 bits) and the FlowProfileID Level field (14 bits). The FlowProfileID Type specifies whether that identifier is defined as standard or proprietary.

The HSGW maintains a mapping of the 3GPP2 FlowProfileIDs into the 3GPP triple <QCI, GBR, MBR>. An example of this mapping is defined in Annex A. Whenever the FlowProfileID does not specify an MBR parameter, the MBR was assumed in the mapping table (Table 64) to be the same as the GBR. No QoS mapping recommendations are provided for FlowProfileIDs reserved for proprietary or future use.

This QoS mapping capability provides the policy interworking used during session establishment and E-UTRAN to eHRPD handoffs.
4.6.7 Application of 3GPP PCC to the eHRPD Access Network

By mapping the eHRPD QoS parameters to EPC QoS parameters, the HSGW can apply the 3GPP PCC rules in the eHRPD network.

For network initiated dedicated bearers, as shown in section 4.5.3, the PCRF sends the requested QCI parameters to the HSGW. The HSGW maps the requested QCI parameters to a set (one or more) of FlowProfileIDs (based on operator determined charging policy, etc.) that are sent to the UE. The GBR provided by the FlowProfileID(s) shall be at least as high as the GBR assigned by the PCRF.

For UE initiated bearer resource allocation, as shown in section 4.5.4.1, the UE provides requested FlowProfileIDs ordered first to last in the list from most preferred to least preferred. The HSGW shall use the most preferred FlowProfileID sent by the UE that is supported by operator policy for mapping to a single set of QCI parameters included in a request to the PCRF. If the PCC request is accepted, the HSGW shall reverse map this accepted single set of QCI parameters to a set (one or more) of FlowProfileIDs (based on operator determined charging policy, etc.) that is a subset of the list of FlowProfileIDs sent by the UE. The GBR provided by the FlowProfileID(s) shall be at least as high as the GBR assigned by the PCRF.

4.7 S103 Interface: S-GW – HSGW

The S103 (User Plane interface) between the Serving Gateway (S-GW) and HSGW supports the forwarding of downlink data during mobility from E-UTRAN to eHRPD. Signaling procedures on the S101 interface are used to set up tunnels on the S103 interface as described in TS 23.402 [23].

The S103 reference point shall support the following requirements:

- The S103 interface shall support the ability to tunnel traffic on a per-UE, per-PDN basis
- The S103 interface shall support Generic Routing Encapsulation (GRE) RFC 2784 [55] including the Key Field extension RFC 2890 [56]. The Key field value of each GRE packet header uniquely identifies the PDN connectivity that the GRE packet payload is associated with.

4.7.1 S103 Protocol Stack


4.7.2 S103 Procedures

The S103 interface is established to provide indirect data forwarding from the S-GW to the HSGW during handoff from E-UTRAN to eHRPD. For stage 3 details, see TS 29.276 [36].

During the handoff execution phase from E-UTRAN to eHRPD, the HSGW provides its own IP address for the eHRPD end of the S103 interface, as well as the GRE key(s) and the APNs associated with each of those GRE keys(s) for packet forwarding from the S-GW to the HSGW. This information is passed to the eAN/ePCF across the A11 interface, see section 8. The eAN/ePCF then forwards that information to the MME across the S101 interface, and the MME provides it to the S-GW. The S-GW uses the HSGW IP address and GRE key(s) for packet forwarding from the S-GW to the HSGW.
4.8 PPP/VSNCP Renegotiation

If a UE that is attached to one or more PDNs receives an LCP-Configure-Request from an HSGW (e.g., inter-HSGW handoff without context transfer occurs), the UE shall perform LCP negotiation and EAP-AKA’ authentication as specified in section 4.2. In addition, the UE shall also perform Handoff Attach to all the PDNs that it was previously connected to and wishes to remain connected to.

If a UE that is attached to one or more PDNs receives a VSNCP Configure-Request from an HSGW, the UE shall perform VSNCP negotiation for that PDN using Handoff Attach.

4.9 MUPSAP Support for eHRPD

MUPSAP (Multiple PDN Connections to A Single APN) allows the UE to setup more than one PDN connection with an APN. Each PDN connection is uniquely identified using PDN Identifier + User Context Identifier. This section defines the additional requirements for the UE and HSGW to support MUPSAP over eHRPD. See section 12 for MUPSAP support for handoff from E-UTRAN to eHRPD.

4.9.1 PDN Connection Setup and Teardown Procedure

If the UE wants to setup multiple PDN connections to an APN (MUPSAP), then the UE shall include the User Context Identifier configuration option in the VSNCP Configure-Request message for the first PDN connection for that APN. The UE should not attempt to setup additional PDN connections to that APN until the UE receives the VSNCP-Configure-Ack message from the HSGW. If the HSGW indicates that multiple connections to that APN are not supported, then the UE shall not attempt to setup additional PDN connections to that APN. If multiple connections to the same APN is supported, then for each of the PDN connections to that APN, the UE shall choose a unique value for the User Context Identifier.

If the UE has included the User Context Identifier configuration option in the VSNCP Configure-Request message, and if the HSGW supports MUPSAP, then the HSGW includes the PDN Connection ID in the Proxy Binding Update message as specified in TS 29.275 [35]. The HSGW shall choose a unique PDN Connection ID value for each of the User Context Identifiers received from the UE for the same APN. If the MUPSAP function is supported by the P-GW, then the received PDN Connection ID information element is included in the Proxy Binding Acknowledge message sent by the P-GW. Upon receiving the PDN Connection ID in the Proxy Binding Acknowledge message from the P-GW, the HSGW shall include the User Context Identifier configuration option in the VSNCP Configure-Ack message with the value set to the same value received in the VSNCP Configure-Ack message received from the UE. When the HSGW sends the VSNCP Configure-Request message to the UE, it shall include the User Context Identifier configuration option with the value set to the same value received in the VSNCP Configure-Request sent from the UE.

If the HSGW included the Address Allocation Cause configuration option in the VSNCP Configure-Ack message sent to the UE with the cause code set to “New PDN type due to network preference”, then the UE may request a new PDN connection to the same APN by sending a VSNCP Configure-Request message to the HSGW with the User Context Identifier configuration option set to a value that is not already in use, and with the PDN Type configuration option set as follows:

- If the PDN Type configuration option of VSNCP Configure-Ack message received from the HSGW is set to IPv4, then the UE should set the PDN Type configuration option of the new VSNCP Configure-Request message to IPv6.
- If the PDN Type configuration option of VSNCP Configure-Ack message received from the HSGW is set to IPv6, then the UE should set the PDN Type configuration option of the new VSNCP Configure-Request message to IPv4.

If the HSGW included the APN-AMBR configuration option in the VSNCP Configure-Request message for more than one PDN connection connecting to same APN, then the UE shall use the latest value of the APN-AMBR configuration option for that APN.

If the HSGW does not support MUPSAP, it shall not include the PDN Connection ID information element in the Proxy Binding Update message it sends to the P-GW. If the HSGW does not receive a PDN connection ID value in the Proxy Binding Acknowledge message sent by the P-GW, it shall not include the User Context Identifier configuration option in the VSNCP Configure-Ack message sent to the UE. In the case of S101 based pre-registration, if the HSGW had already included the User Context Identifier configuration option in the VSNCP Configure-Ack message sent to the UE, and if the HSGW determines at the time of handoff that the P-GW does not support MUPSAP, then the HSGW shall initiate termination of all PDN connections to that APN by sending VSNCP Terminate Request message to the UE.

To terminate a specific MUPSAP PDN connection, the UE or HSGW shall include the PDN Identifier and the User Context Identifier in the VSNCP Terminate-Request message. If the VSNCP Terminate-Request message does not include a User Context Identifier configuration option, it implies all PDN connections to the APN shall be removed. When multiple PDN connections to an APN are setup, and if the VSNP Extend Code is negotiated for the first PDN connection to that APN, then all subsequent PDN connections to that APN shall use the same VSNP Extend Code until all the PDN connections to that APN are torn down. If the VSNP Extend Code is not negotiated for the first PDN connection to that APN, then none of the subsequent PDN connections to that APN shall negotiate the VSNP Extend Code until all the PDN connections to that APN are torn down.

For optimized handoff from E-UTRAN to eHRPD, GRE tunnels between the S-GW and HSGW are established per UE per APN. For MUPSAP, the HSGW will distinguish the packets for different PDN connections to the same APN using the destination IP address of the packet.

### 4.9.2 Quality of Service - MUPSAP

The QoS setup procedure is performed for each of the MUPSAP PDN connections using the procedures specified in section 4.5.

Each of the service connections, (i.e., each concatenation of an RLP flow with an A8+A10 connection, between the UE and the HSGW) established for an APN may be shared by all the MUPSAP PDN connections for that APN for the same QoS.

### 4.10 Emergency Session Support

#### 4.10.1 Overview

This section provides an overview of the functionality for emergency bearer services. The specific functionality is described in the affected procedures and functions of this
specification. For discrepancies between this overview clause and the detailed procedure and function descriptions, the latter take precedence.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving eHRPD access network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and depending on local regulation, to UEs that are in limited service state. Receiving emergency services in limited service state does not require a subscription. Depending on local regulation and an operator's policy, the HSGW may allow or reject an emergency attach request for UEs in limited service state. Four different behaviours of emergency bearer support have been identified as follows:

a. **Valid UEs only.** No limited service state UEs are supported in the network. Only normal UEs that have a valid subscription, are authenticated and authorized for PS service in the attached location are allowed. Normal UEs should initiate a normal attach procedure (if not already attached to the network) and then perform a PDN Connection Request (ref. section 4.10.8.1) when an IMS emergency session is detected by the UE.

b. **Only UEs that are authenticated are allowed.** These UEs must have a valid IMSI. These UEs are authenticated and may be in limited service state due to being in a location that they are restricted from service. A UE that can not be authenticated will be rejected.

c. **IMSI required, authentication optional.** These UEs must have an IMSI. If authentication fails, the UE is granted access and the unauthenticated IMSI retained in the network for recording purposes. The MEID is used in the network as the UE identifier. MEID only UEs will be rejected.

d. **All UEs are allowed.** Along with authenticated UEs, this includes UEs with an IMSI that can not be authenticated and UEs with only an MEID. The MEID is used in the network to identify the UE.

The HSGW shall not allow a UE that is emergency attached to the network to connect to PDNs other than the emergency PDN.

3GPP2 MEIDs and 3GPP IMEIs are taken from the same name space. Where 3GPP specifications require IMEI, the MEID of the UE shall be used in attachments to the eHRPD access network, since the value of the IMEI and the value of the MEID in the UE are exactly the same (ref. SC.R4002 [17]).

To provide emergency bearer services, the HSGW is configured with HSGW Emergency Configuration Data that are applied to all emergency bearer services that are established by an HSGW on UE request. The HSGW Emergency Configuration Data contain the emergency APN which is used to derive a P-GW, or the HSGW Emergency Configuration Data may also contain the statically configured P-GW for the emergency APN.

UEs that are in limited service state initiate the Attach procedure with indicating that the attach is to receive emergency services. The network supporting emergency services for UEs in limited service state provides emergency bearer services to each such UE, regardless whether the UE can be authenticated, has roaming or mobility restrictions or a valid subscription, depending on local regulation. The UEs in limited service state determine that the cell supports emergency services over eHRPD from a broadcast indicator in the AccessHashingChannelMask (ref. C.S0024 [10]). UEs that camp normally on a cell, i.e. without any conditions that result in limited service state, initiate the UE Requested PDN
Connectivity procedure to receive emergency bearer services. The UEs that camp normally on a cell are informed that the network supports emergency services by means of the VSNCP Configure-Request sent by the HSGW. Additionally, the eAN indicates emergency support over eHRPD as specified in C.S0087 [15].

For a UE that is Emergency Attached, normal network selection principles apply after the emergency PDN connection is disconnected.

For emergency bearer services any EPC functions, procedures and capabilities are provided according to TS 23.401 [22] except when specified differently in the following sections.

For emergency bearer services there is no support of inter-network mobility (i.e., inter-operator mobility) in this version of this specification.

When a network supports IMS emergency services, all HSGWs in that network shall have the same capability to support emergency bearer services.

The particular requirements for access to the EPC via an eHRPD access network in support of emergency accesses and emergency services in the case of handover from E-UTRAN to eHRPD are specified in TS 23.402 [23].

4.10.2 Architecture Reference Model for Emergency Services

The non-roaming architecture (Figure 1) and roaming architecture with the visited operator's application function (Figure 3) apply for emergency services. The other roaming architecture with services provided by the home network (Figure 2) do not apply for emergency services.

4.10.3 P-GW Selection Function (3GPP2 Accesses) for Emergency Services

In E-UTRAN, the MME selects a P-GW that is statically configured in the MME Emergency Configuration Data. In eHRPD, the HSGW selects a P-GW that is statically configured in the HSGW Emergency Configuration Data. In networks that support handoff between E-UTRAN and eHRPD, the HSGW shall have the same P-GW statically configured in the HSGW Emergency Configuration Data as is configured for the MME in the MME Emergency Configuration Data. The P-GW selection does not depend on subscriber information in the HSS, since emergency call support is a local, not subscribed service. The MME/HSGW Emergency Configuration Data contains the emergency APN which is used to derive a P-GW, or the MME/HSGW Emergency Configuration Data may also contain the statically configured P-GW for the emergency APN.

4.10.4 QoS for Emergency Services

Where local regulations require supporting calls from an unauthorized caller, the HSGW may not have subscription data. Additionally, the local network may want to provide IMS emergency call support differently than what is allowed by a UE subscription. Therefore, the initial QoS values used for establishing emergency bearer services are configured in the HSGW in the HSGW Emergency Configuration Data. If PCC is not deployed, the HSGW uses the ARP value that is reserved for emergency services, which the HSGW bases on the usage of the emergency APN.
### 4.10.5 PCC for Emergency Services

When dynamic PCC is used for UEs establishing emergency service, the procedures are as described in TS 23.203 [20]. When establishing emergency bearer services and dynamic policy is used, according to TS 23.402 [23] clause 4.10.4, the PCRF provides the HSGW with the QoS parameters, including an ARP value reserved for the emergency bearers to prioritize the bearers when performing admission control. Local configuration of static policy functions is also allowed and not subject to standardization.

All emergency call flows in this specification, unless otherwise specified, assume the use of PCC.

### 4.10.6 IP Address Allocation for Emergency Services

Emergency bearer service is provided by the serving network. The UE and network must have compatible IP address versions in order for the UE to obtain a local emergency PDN connection. IP address allocation in the serving network is provided per section 4.4 with the exception that the P-GW associated with the emergency APN shall support PDN type IPv4 and PDN type IPv6.

### 4.10.7 Handling of PDN Connections for Emergency Bearer Services

The default and dedicated IP flows of a PDN Connection associated with the emergency APN shall be dedicated for IMS emergency sessions and shall not allow any other type of traffic. The emergency bearer contexts shall not be changed to non-emergency bearer contexts and vice versa. The P-GW blocks any traffic that is not from or to addresses of network entities (e.g. P-CSCF) providing IMS emergency service. If PCC is not deployed, the list of allowed addresses may be configured in the HSGW by the operator.

When dynamic PCC is deployed, the procedures are as described in TS 23.203 [20]. If there is already an emergency P-GW connection, the UE shall not request another emergency PDN connection. The HSGW shall, for a given UE that already has an emergency PDN connection, reject any additional emergency PDN connection requests. The UE shall not request any bearer resource modification for the emergency PDN connection. The HSGW shall reject any UE requested bearer resource modification that is for the emergency PDN connection. The ARP reserved for emergency bearer service is only assigned to EPS bearers associated with an emergency PDN connection, and shall only be translated by the HSGW into FLOW_PRIORITY values associated with emergency services for service connections carrying traffic for an emergency PDN connection. When PCC is not used the HSGW provides static policy.

Note: MUPSAP for emergency PDN connections is not supported in this version of this specification.

### 4.10.8 PDN Connection Establishment Procedures for Emergency Services

This section defines the procedure for emergency PDN connection establishment during initial emergency PDN connection as well as for handoff from E-UTRAN to eHRPD. The procedure defined below is also applicable for inter-HSGW handoff without context transfer.

During an emergency call setup on an eHRPD network, the UE includes the ‘EmergencyIndication’ in the radio connection request sent to the eAN/ePCF either using the S101 tunnel or directly over the eHRPD air interface as specified in C.S0087 [15] / C.S0024 [10]. When the eAN/ePCF receives a radio connection request from the UE that includes an
‘EmergencyIndication’, the eAN/ePCF sends the ‘Emergency Service Indication’ to the HSGW using the A11-Registration Request message (ref. A.S0008 [1] / A.S0009 [2]).

Based on local regulation or operator policy, if the UE is required to be authenticated before an emergency PDN connection is allowed (ref. Section 4.10: (a) “Valid UEs only” and (b) “Only UEs that are authenticated are allowed”), then, following successful EPS authentication, the emergency PDN connection is initially established using the UE’s IMSI as the identity in the PBU. To preserve session continuity on handoff, the UE’s IMSI derived from EAP-AKA’ is used by the target HSGW as the identity when reconnecting the emergency PDN connection.

In the case where EPS authentication is not required by local regulation or operator policy (ref. Section 4.10, (c) “IMSI required, authentication optional”, (d) “All UEs are allowed”), either the UE’s IMEI/MEID or IMSI is used as the identity during initial emergency PDN connection establishment. To preserve IP session continuity during handoff, the identity that is used during the initial emergency PDN connection is also used as the identity on the target network.

During an emergency PDN connection establishment (either initial or handoff) on an eHRPD network, the UE and the HSGW shall follow the procedures defined below:

- The UE shall include Mobile Identity configuration option in the VSNCP Configure Request message sent to the HSGW, with the type of identity set as follows:
  - If a successful EPS authentication was performed prior to the initial emergency PDN connection, then the UE shall send the IMSI by setting the ‘Type of identity’ to ‘001’ (IMSI) as per section 10.5.1.4 of TS 24.008 [24].
  - Otherwise, the UE shall send the MEID by setting the ‘Type of identity’ to ‘010’ (IMEI) per section 10.5.1.4 of TS 24.008 [24].

- In S2a PMIPv6 signaling, the HSGW shall use the identity obtained in the Mobile Identity configuration option of the VSNCP-Configure Request message from the UE.
4.10.8.1 Already Authenticated UE Attach Procedure for Emergency Services

The UE requested emergency services PDN connectivity procedure for eHRPD is depicted in Figure 25. The procedure allows the UE to request connectivity to an emergency services PDN. The default bearer for the emergency services PDN shall reuse the best effort service connection. The emergency services PDN will also be assigned a new and unique PDN-ID by the UE. In this procedure, the UE is assumed to be already authenticated and in active mode via the eHRPD radio.

Figure 25  Already Authenticated UE Attach Procedure for Emergency Services

1. When the UE wants to establish connectivity to an emergency services PDN, it will send the VSNCP Configure-Request message (APN, PDN Address, PDN Type, Protocol Configuration Options, PDN-ID, Attach Type, Address Allocation Cause, IPv4 Default Router Address, and Emergency Indicator = 1, Mobile Identity with type of identity set to ‘IMSI’). The APN may be null. The Address Allocation Preference (contained within the Protocol Configuration Options) indicates whether the UE wants to perform the IPv4 address allocation during the execution of the procedure and PDN Type indicates that the UE is capable of supporting IPv4 and IPv6. The HSGW notes the inclusion of the Emergency Indicator with the value 1. If the UE supports NW Requested Bearer Control, then the UE includes the ‘MS Support of Network Requested Bearer Control indicator’ parameter in the Protocol Configuration Options.

2. The HSGW triggers the procedures for UE requested PDN connectivity described in TS 23.402 Section 6.2.1-1 Steps 4-10 inclusive (ref. TS 23.402 [23]). The Gateway Control Session is established only with the PCRF in the serving network, using the emergency QoS values in the HSGW Emergency Configuration Data. The APN supplied by the HSGW to the P-GW in the PMIP Binding Update shall be the emergency APN in the HSGW Emergency Configuration Data, and the APN supplied in the VSNCP Configure-Request may be ignored by the HSGW. This establishes the bindings at the P-GW and it updates the PCRF with the indication of the emergency services PDN connection.
3. After the HSGW receives the indication of the completion of PMIPv6 procedures, it will send the VSNCP Configure-Ack (APN=null APN, PDN Address, PCO, PDN-ID, Attach Type, Address Allocation Cause, and IPv4 Default Router Address, Emergency Indicator=1, Mobile Identity with type of identity set to ‘IMSI’) message to the UE. The Protocol Configuration Options parameter indicates the Selected Bearer Control Mode only if the UE included the MS Support of Network Requested Bearer Control indicator (BCM) parameter in the corresponding VSNCP Configure-Request message.

4. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID and the Emergency Services Supported Indicator configuration options. This message contains the APN-AMBR, if the APN-AMBR was received from the HSS/AAA.

5. The UE responds with a VSNCP Configure-Ack message. The UE includes APN-AMBR, if it received APN-AMBR in step 4, and if the UE supports APN-AMBR.

6. IPv4 address allocation may occur at this point using the procedure shown in section 4.4.5.2 steps 9-12 and section 4.4.5.3, steps 9-16, when the IPv4 address allocation is deferred.

7. IPv6 address allocation may occur at this point using the procedure shown in section 4.4.5.4 steps 9-11.
4.10.8.2 Not-Authenticated UE Attach Procedure for Emergency Services

PMIPv6 (see RFC 5213 [78] and TS 29.275 [35]) signaling is used to establish an S2a connection between the HSGW and the P-GW supporting the emergency PDN. The sample call flow in Figure 26 illustrates the establishment of the PMIPv6-based S2a connection when an unauthenticated UE attaches to the eHRPD access network for the purpose of receiving emergency services.

**Figure 26** Not-Authenticated UE Attach Procedure for Emergency Services
1. The UE and the eAN initiate eHRPD session establishment. During this procedure, the eAN determines that it connects with a UE. The UE indicates via radio level signaling that it is connecting to access emergency services.

2. The UE is ready to send data.

3. The ePCF recognizes that no A10 connection associated with the UE is available, and selects an HSGW. The ePCF sends an A11-Registration Request message to the HSGW to set up the main A10 connection, and optionally set up the Best Effort (BE) or QoS auxiliary connection. The A11-Registration Request message contains an indication that the UE is attaching to receive emergency services. The A11-Registration Request is validated and the HSGW accepts the connection by returning an A11-Registration Reply message.

4. The UE and HSGW perform LCP negotiation. The HSGW, noting that the UE is attaching for emergency services, chooses to skip EAP-AKA’ authentication based on operator policy.

Note: Authentication may be skipped or, if performed, NCP negotiation may proceed if authentication fails (to support the various levels of regulatory requirements).

5. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, PDN Type, APN, PDN Address with empty content, Protocol Configuration Options, Attach Type = “Initial Attach”, Emergency Indicator=1, and Mobile Identity with type of identity set to ‘IMEI’ and containing an MEID value. The Address Allocation Preference option contained in the Protocol Configuration Options indicates whether the UE wants to perform the IPv4 address allocation during the attach procedure or deferred IPv4 address allocation. PDN Type indicates the UE’s IP capability (IPv4, IPv6 or IPv4v6). Additional configuration options (e.g., IPv4 Default Router Address) are included depending upon the PDN Type. If the UE supports NW Requested Bearer Control, then the UE includes the option in the Protocol Configuration options parameter set to “MS/NW” mode. The APN value, if supplied in the VSNCP Configure-Request, shall be ignored by the HSGW.

6. The HSGW performs the Gateway Control Session Establishment procedure with the PCRF. The HSGW indicates the possible bearer control modes according to the UE capability provided in step 5 and its own capability. The HSGW includes the emergency APN and the emergency QoS values from the HSGW Emergency Configuration Data. The PCRF selects the bearer control mode to be used.

7. The HSGW sends a Proxy Binding Update to the P-GW in order to establish the connection to the emergency PDN. The HSGW uses an MEID-based NAI to identify the UE. The HSGW will use the emergency APN from the HSGW Emergency Configuration Data to choose the P-GW, and the APN supplied in the VSNCP Configure-Request is ignored by the HSGW.

8. The P-GW performs a PCRF interaction to establish the IP-CAN session. For details, see TS 23.203 [20].

9. The P-GW responds with a PBA message to the HSGW see TS 29.275 [35].

10. In case the QoS rules have changed, the PCRF updates the emergency services QoS rules at the HSGW by the exchange of Gateway Control and QoS Rules Provision/Ack messages, as specified in TS 23.203 [20].

11. The HSGW sends a VSNCP Configure-Ack (PDN-ID, APN=null APN, PDN Address, PCO, Attach Type, Address Allocation Cause, Emergency Indicator=1, and Mobile Identity with type of identity set to ‘IMEI’ and containing an MEID value) message to the UE over the main service connection. Note that the PDN Address Information may contain an IPv4 address for IPv4 and/or an IPv6 Interface Identifier for IPv6. Additional configuration options (e.g., IPv4 Default Router Address) are included if present in the VSNCP Configure-Request. The Protocol Configuration Options parameter may be included to indicate the Selected Bearer Control Mode, if the Protocol Configuration Options parameter was included by the UE in the corresponding VSNCP Configure-Request and indicated support for NW Requested Bearer Control.
12. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID and the Emergency Services Supported Indicator configuration options.

13. The UE responds with a VSNCP Configure-Ack message.

14. (optional) The UE can now issue a DHCPv4 DISCOVER (optionally with rapid commit option) message on the BE service connection provided the UE requested deferred IP address allocation in Step 5.

15. 15a. The UE may send a Router solicitation message.

15b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

16. The IP address allocation details are described in section 4.4.

Based on information stored at the UE or obtained from the network, the UE can start creating the required auxiliary connections (needed for the bearer transport) for a particular QoS flow. See section 9.3.

4.10.8.3 UE-Requested Emergency PDN Disconnection Procedure

The UE should not initiate termination of an emergency PDN connection. The network shall be responsible for termination of an emergency PDN connection.

Note that the UE can be implemented with an internal timer that would eventually cause clearing of the emergency PDN connection, to guard against the small possibility that the network initiated detach fails in some way, e.g., through undetected message loss.

4.10.8.4 UE Initiated Detach Procedure

The UE should not initiate detach from the network while an emergency PDN connection exists. This will allow a callback from the public safety access point (PSAP) to an emergency call.

Note that the UE can be implemented with an internal timer that would eventually cause clearing of the emergency PDN connection, to guard against the small possibility that the network initiated detach fails in some way, e.g., through undetected message loss.

4.10.8.5 Network Initiated Detach Procedure

The following sections describe the procedures for network initiated termination of emergency services.

If the UE is authenticated, the HSGW will have an STa/Pi* session to the 3GPP2 AAA Proxy. If that STa/Pi* session is terminated, the HSGW shall continue to maintain any emergency PDN connections and emergency bearers that the UE may have. The HSGW may delete non-emergency PDN connections.
4.10.8.5.1 PCRF Initiated Detach Procedure for Emergency Services

This section describes the message flow for the network initiated UE detach due to PCRF initiated release procedures. The UE is assumed to be attached only for emergency services. This call-flow depicts the usage of LCP-Terminate to release the PPP session.

Figure 27 PCRF Initiated Detach Procedure for Emergency Services

1. The PCRF initiates the Gateway Control Session Termination Procedure with the HSGW. The HSGW no longer applies QoS policy to service data flows for this UE for the emergency PDN and removes all context for the emergency PDN connection.

2. The HSGW sends an LCP Terminate-Request to the UE.

3. The UE sends an LCP Terminate-Ack to the HSGW to indicate that it received the request to terminate the PPP session.

4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN is needed in order to determine which PDN to deregister the UE from, as some P-GWs may support multiple PDNs.
5. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

6. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends a PBA message (MN NAI, APN, lifetime=0) to the HSGW.

7. The HSGW sends an A11-Registration Update message to initiate with the ePCF the release of all A10 connections for the UE. This step may occur immediately after step 3. The HSGW initiates STa session termination (Not shown in the figure).

8. The ePCF responds with an A11-Registration Acknowledge message.

9. The eAN may initiate HRPD session update. The UE may initiate HRPD session update any time after step 2.

10. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release all A10 connections.

11. The HSGW responds with A11-Registration Reply with lifetime zero.
4.10.8.5.2 P-GW Initiated Disconnect Procedure for Emergency PDN Connection

This section describes the network initiated emergency PDN disconnection procedure as per the P-GW indication or request.

1. The P-GW sends a PMIPv6 Binding Revocation Indication (BRI) message to the HSGW as defined in RFC 5846 [84] indicating a non-handover cause.
2. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of the emergency PDN with which the connection is to be terminated.
3. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to terminate a connection to the emergency PDN.
4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.
5. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].
6. The HSGW sends a PMIPv6 Binding Revocation Acknowledgement (BRA) message to the P-GW as defined in RFC 5846 [84].
7. The UE initiates session configuration procedure to delete any reservations associated exclusively with the closed emergency PDN connection. The UE may initiate this session configuration procedure any time after step 2.

8. The eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

9. The HSGW responds with A11-Registration Reply.

If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate LCP termination procedures.
4.10.9 Bearer Procedures for Emergency Services

This section describes the procedures for creation and deletion of emergency bearers.

4.10.9.1 UE Initiated Emergency Bearer Creation

The call flow in Figure 29 illustrates UE requested emergency bearer activation procedures.

1. The UE sends a Resv message to the HSGW with OpCode set to ‘QoS-Check’. The UE encapsulates the Resv message over the main service connection using VSNP and includes the PDN-ID to indicate to which PDN the additional bearer resource is linked. In this case, the PDN-ID indicates the emergency PDN. The message contains the UE requested FlowProfileIDs. The Transaction ID is dynamically
allocated by the UE for UE requested bearer resource activation procedure. In the example presented in the figure, Transaction ID is 1.

2. The HSGW maps the received FlowProfileID(s) into a single set of QCI/MBR/GBR parameters.

3. The HSGW uses Gateway Control and QoS Rules Request/Reply procedures to validate UE requested QoS with the hPCRF. If the HSGW is deployed in a roaming scenario, the message including QCI/MBR/GBR(s) and packet filter(s) is sent to the vPCRF which does not further pass it to the hPCRF, since this refers to an emergency bearer.

4. The HSGW maps the validated policy rules into appropriate FlowProfileID(s) that are being requested.

5. The HSGW sends a ResvConf message to the UE with OpCode set to ‘QoS-Check Conf’. The Resv message is an RSVP message transported over the main service connection. The ResvConf message contains the authorized FlowProfileIDs, which is the same or a subset of the UE requested FlowProfileIDs in step 1, and the same Transaction ID as in the Resv message sent in step 1. This step is used as an acknowledgment of the Resv message sent in step 1.

6. The UE performs the standard HRPD QoS establishment procedures defined in C.S0087 [15] / C.S0063 [13] using the authorized FlowProfileID list from step 5. There are two possible sequences that can occur at this step. If a new QoS link flow connection is needed to carry the new flow over the air interface, then the eAN will setup a new air interface link flow. If the eAN decides to carry the flow(s) on an existing link flow, it then reconfigures the parameters of that link flow.

7. If a new link flow is needed, a new A10 connection is also established. The eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, the Requested QoS information, and Granted QoS information for the flow. The A11 message includes the FLOW_ID. If a new QoS link flow is not needed, the eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, FLOW_ID, and the modified Granted QoS information for the existing connection (if required).

8. The UE sends a Resv message to the HSGW to associate the selected Reservation with the appropriate A10 connection and TFT. The message includes the Flow ID and associated packet filters for which the FlowProfileID(s) are authorized at step 5. This message can be sent in parallel with the start of the signalling in Step 6. The Transaction ID is different than that used in steps 1 and 5 to avoid having the HSGW view this message as a repetition of the message in step 1. The HSGW examines the QoS granted to the UE and compares it to the QoS authorized for the UE in step 5. If there is a discrepancy, the HSGW applies operator policy.

9. The HSGW acknowledges the Resv message with a ResvConf message.

10. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or eAN) may trigger the transition to the open state.

11. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an A11-Registration Request (Active Start) message to initiate the accounting for this bearer connection.

12. If the PCRF has indicated at step 3 that a particular priority (ARP value) is to be applied to this bearer, then anytime after step 8 the HSGW may use the A11-Session Update procedure to change the FLOW_PRIORITY of the emergency bearer.

13. Upon a successful negotiation of QoS, the HSGW sends the acknowledgement to the PCRF based on the QoS that was selected in step 2.

14. The IP CAN Session Modification Procedure may occur as the result of the Gateway Control and QoS Rules Request message, either to forward an Event Report to the P-GW (PCEF) or to issue revised PCC Rules and Event Triggers, or both an Event Report and a Rules and Triggers provision. If an indication that resources have been acquired is not required then this step may occur any time after step 3, above.
4.10.9.2 Network Initiated Emergency Bearer Creation

The following diagram illustrates network initiated emergency dedicated resource allocation operations for eHRPD which are triggered by the PCRF. The procedures shown include PCRF interactions described in TS 23.402 [23] and eHRPD specific procedures. The bearer to be established is assumed in this example to be related to the emergency PDN with which the UE has a current PDN connection.

On receiving the Gateway Control and QoS Rules Provisioning message from the PCRF, the HSGW decides that a new bearer needs to be activated, the HSGW uses this QoS policy to assign the bearer QoS, (i.e., it maps PCC QoS parameters to a set of eHRPD FlowProfileIDs). The HSGW follows this with the procedure shown in Figure 30 by sending an RSVP Resv message to the UE.

![Diagram of Network Initiated Dedicated Bearer Setup](image)

**Figure 30** Network Initiated Dedicated Bearer Setup

Both the roaming and non-roaming scenarios are depicted in Figure 30. In the roaming case for an emergency service, the vPCRF does not act as an intermediary with the hPCRF. Instead, the vPCRF directly sends the QoS Policy Rules to the HSGW in the vPLMN. The vPCRF receives the Acknowledgment from the HSGW. In the non-roaming case, the vPCRF is not involved.

1. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20] by sending a message with the QoS rules and Event Trigger information to the HSGW.
2. The HSGW uses the received QoS policy information to determine the bearer level QoS parameters required for the eHRPD bearer. The HSGW maps these parameters to the appropriate eHRPD FlowProfileID(s) (see C.R1001 [12]).

3. The HSGW sends an RSVP Resv message transported over the main service connection. As indicated in section 9, the RSVP Resv message encapsulation includes the PDN-ID of the PDN for which the bearer is being created. The RSVP Resv message includes the Uplink/Downlink packet filter, the QoS list, and a Transaction ID. See section 9.1.6.7.1 for parameter details.

4. The UE performs the standard QoS establishment procedures defined in C.S0024 [10] and in C.S0063 [13]. There are two possible sequences that can occur at this step. If a new QoS link flow connection is needed to carry the new flow over the air interface, then the eAN will setup a new air interface link flow. If the eAN decides to carry the flow(s) on an existing link flow, it then reconfigures the parameters of that link flow.

5. If a new link flow is needed, a new A10 connection is also established. The eAN/ePCF sends an A11-Registration Request message to the HSGW indicating the GRE key, the Requested QoS information, and the Granted QoS information for the flow. The Granted QoS information includes the FLOW_ID. If a new QoS link flow is not needed, the eAN sends an A11-Registration Request message to the HSGW indicating the GRE key, FLOW_ID, and the modified Granted QoS information for the existing connection (if required).

6. The UE sends an RSVP Resv message to the HSGW. The message includes the Flow ID for the bearer connection, and the same DL/UL TFT and Transaction ID received in step 3. This message can be sent in parallel with the start of the signaling in Step 4. The Transaction ID is used to associate the returned Flow ID with the new bearer connection. This message is also used as an acknowledgement to the RSVP Resv message in Step 3. The HSGW examines the QoS granted to the UE and compares it to the QoS authorized for the UE in step 2. If there is a discrepancy, the HSGW applies operator policy.

7. The HSGW acknowledges the delivery of the RSVP Resv message it received in Step 6 by sending a ResvConf message to the UE.

   If the HSGW needs to change the priority of the emergency bearer, it can use the A11-Session Update message to inform the eAN/ePCF of the new Flow_Priority (not shown in the figure).

8. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or eAN) may trigger the transition to the open state.

9. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an A11-Registration Request (Active Start) message to initiate the accounting for this bearer connection.

10. Any time after Step 6 the HSGW responds to the PCRF indicating its ability to enforce the rules provisioned to it in Step 1 and thus completing the Gateway Control and QoS Rules Provision Ack procedure started in step 1.


   NOTE: Step 11 may occur before step 2 or may be performed in parallel with steps 1 and 10 if acknowledgement of resource allocation is not required to update PCC rules in the PCEF. For details please refer to TS 23.203 [20].
4.10.9.3 UE Initiated Emergency Bearer Removal

The call flow in Figure 31 illustrates UE requested emergency bearer removal.

Figure 31 UE Initiated Emergency Bearer Removal


2. The eAN/ePCF sends an A11-Registration Request message to the HSGW with an ‘Active Stop’ indication. The A11 message includes the FLOW_ID. The HSGW responds with an A11-Registration Reply message.

3. The UE sends a Resv message to the HSGW with OpCode set to ‘Delete Existing TFT’. The UE encapsulates the Resv message over the main service connection using VSNP and includes the PDN-ID to indicate to which PDN the bearer resource is linked. The Transaction ID is dynamically allocated by the UE. In the example presented in the figure, the chosen Transaction ID is 1. Step 3 may occur at the same time as step 1.

4. The HSGW uses Gateway Control and QoS Rules Request/Reply procedures to notify the vPCRF that the bearer is being removed. The HSGW deletes the context for the emergency bearer.

5. The HSGW sends a ResvConf message to the UE to acknowledge the bearer removal.

6. The UE may choose to remove the Reservation.

7. The eAN/ePCF and the HSGW remove any unneeded A10 connections.

8. The IP CAN Session Modification Procedure may occur as the result of the Gateway Control and QoS Rules Request message. This step may occur any time after step 4.
4.10.9.4 Network Initiated Emergency Bearer Removal

This procedure applies to cases where the QoS rules provided by the PCRF to the HSGW result in a decision to release or modify one or more of the established emergency bearers.

Network initiated emergency bearer deactivation shall take into account the deactivation of both dedicated auxiliary service connections and the removal of emergency bearers from a PDN-ID multiplexed shared service connection. While removing an emergency bearer from a multiplexed shared service connection, it is necessary to retain the shared service connection for connectivity to other PDNs. A service connection is removed when the last Reservation associated with the service connection is removed.

This call flow assumes the PCRF initiated modification or release of an emergency bearer.

---

**Figure 32 PCRF Initiated Dedicated Bearer Deactivation**

1. The vPCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20] by sending a message with the QoS rules and Event Trigger information to the HSGW.

2. The HSGW sends a Resv message to the UE with OpCode set to ‘Initiate Delete Packet Filter from Existing TFT’ indicating the EPS bearer deletion. The message is indexed with the PDN-ID of the PDN for which the EPS bearer is being deleted.

3. The UE performs standard HRPD procedures to reconfigure the air interface in order to remove or modify the requested Reservation(s). If the last Reservation(s) associated with the link flow is removed, the link flow itself is also removed.
4. The eAN sends an A11-Registration Request message to the HSGW indicating the removed Flow ID(s). If the last Flow ID associated with the auxiliary A10 is removed, the auxiliary A10 itself will also be removed.

5. The UE sends a Resv message with OpCode set to ‘Delete Packet Filter from Existing TFT’ to indicate to the HSGW which flows have been removed. The TFT IE contains the list of flow identifiers for which filters have been deleted. The Transaction ID carried in this message shall be the same as the Transaction ID carried in the Resv message in step 2. This message is also used as an acknowledgement to the RSVP Resv message in Step 2.

6. The HSGW acknowledges a successful update of the IP flow mapping information by sending a ResvConf message to the UE.

7. The HSGW indicates to the vPCRF whether the requested QoS Policy Rules Provision could be enforced or not by sending a Gateway Control and QoS Rules Provision Acknowledgment message.


NOTE: Step 8 may occur before step 1 or performed in parallel with steps 1 and 7 if acknowledgement of resource de-allocation is not required to update PCC rules in the PCEF. For details please refer to TS 23.203 [20].
4.10.10 Handoff Procedures for Emergency Services

This section describes the procedures for handoff of emergency services.

In both optimized and non-optimized handoff, the UE will include the Emergency Indicator set to 1 in the VSNCP Configure-Request for the emergency PDN connection.

4.10.10.1 Optimized Handoff Pre-Registration for Emergency Services

The following flow describes the use of the S101 interface to tunnel eHRPD signaling between the UE and the eAN/ePCF to prepare to handoff emergency services from E-UTRAN to eHRPD.

**Figure 33** eHRPD Pre-registration via E-UTRAN
1. The UE is initially attached to the E-UTRAN. The UE acquires an IPv4 address and/or IPv6 prefix for the emergency PDN. Data flows between the UE and the P-GW through the eNodeB and the S-GW.

2. Based on a Radio Layer trigger, the UE decides to initiate a pre-registration procedure with potential target eHRPD access.

3. The UE initiates the establishment of a new session in the eHRPD system through the S101 tunnel.

4. RAN-level authentication is optional. If used, the UE establishes an AN-PPP connection with the eAN/ePCF and performs RAN-level authentication using the A12 interface. For details refer to A.S0022 [4]. If the UE does not have a valid A12 NAI, the UE uses the A12 emergency NAI for the A12 authentication, see X.S0060 [8]. By sending the challenge to the UE and receiving back the emergency NAI, the eAN will become aware of the emergency nature of the tunnelled attachment.

5. The eHRPD eAN/ePCF establishes the main A10 connection with the HSGW by exchanging A11-Registration Request/Registration Reply messages. The A11-Registration Request message contains the IMSI/MEID, an indication that the access is occurring through the S101 tunnel, and an indication that the access is for emergency services. For details refer to A.S0022 [4]. This information is used by the HSGW in step 7 to defer interaction with the P-GW. The UE and HSGW initiate the PPP connection establishment procedure.

6a-b. The UE may perform user authentication and authorization in the eHRPD access system using EAP-AKA’ if required by local regulation or operator policy and a valid IMSI is present. The EAP-AKA’ messages are transferred between the UE and HSGW over PPP. The EAP authenticator resides in the HSGW. The detailed EAP-AKA’ authentication flows are specified in Section 4.2. The 3GPP AAA server authenticates and authorizes the UE for access in the eHRPD system. The 3GPP AAA server queries the HSS and returns the subscription profile, and APN and P-GW address pair for each PDN connection to the eHRPD system in this step. The 3GPP AAA server also returns the NAI to be used to identify the UE in Proxy Binding Update message.

Note: Authentication may be skipped or, if performed, NCP negotiation may proceed if authentication fails (to support the various levels of regulatory requirements).

6c. If authentication is performed, the HSGW stores the information received from the 3GPP AAA/HSS server.

7. The UE exchanges VSNCP messages with the HSGW for the emergency PDN connection (see section 5.4.1 for details). The UE sets the Attach Type to “handoff” in the VSNCP Configure-Request message and includes the “Mobile Identity” configuration option, and the “Emergency Indicator” configuration option with the value 1. The APN supplied in the VSNCP Configure-Request may be ignored by the HSGW, since the UE indicates “emergency”.

If the UE has additional PDN connections on the E-UTRAN system that it wishes to also maintain on the eHRPD system, and if the UE has authenticated at step 6 above, then the UE follows the normal procedures shown in section 12.1.1 to create each of those PDN connections with the HSGW.

NOTE: The HSGW defers interaction with the P-GW until the UE arrives in eHRPD, at which time it sends a PBU to the P-GW to complete the PDN connection. For an emergency PDN connection, the HSGW obtains the address of the P-GW supporting the emergency PDN from the provisioned HSGW Emergency Configuration Data. For a normal PDN connection, the HSGW obtains the address of the P-GW via the STa/Pi* interface to the 3GPP2 AAA Proxy.

8. The network initiates resource reservation procedures to establish all dedicated bearers.

9. It may become necessary to modify the eHRPD radio session configuration between the UE and the eAN/ePCF. For example, this may be necessary as a result of moving under the coverage area of a new eAN/ePCF. This is accomplished by eHRPD signalling exchanges between the UE and the eAN/ePCF via S101 tunneling.
It is also possible that this procedure began as a normal optimized handoff pre-registration, and the UE then added the emergency PDN connection later. Adding the emergency PDN connection on eHRPD would be carried out as part of session maintenance, with the VSNCP Configure-Request carrying the “Emergency Indicator” configuration option with the value set to 1. Subsequently, the emergency bearers would also be added on eHRPD using tunneled signaling over the S101 interface.

10. If any bearer is added, modified, or deleted while the UE is operating on E-UTRAN, similar changes shall be made in the context between the UE and the HSGW. This is accomplished by signaling those changes between the UE and HSGW via S101 tunneling. Likewise, if the UE was authenticated at step 6, then if any PDN connection is added or deleted while the UE is operating on E-UTRAN, similar changes are made in the HSGW via the use of VSNCP.

Note: If the HSGW receives a VSNCP Configure-Request for a PDN connection for which it does not have a P-GW identity and if the UE was authenticated at step 6, then it obtains that information via an AAR/AAA exchange with the HSS/AAA. The exchanges of AAR/AAA messages are not shown in the figure.

11. If not already initiated, PCRF interactions due to session maintenance can be initiated by the PCRF or the HSGW. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20]. The HSGW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [20].
4.10.10.2 Optimized Handoff for Emergency Services

It is assumed that the UE has pre-registered with eHRPD for emergency services, that the PPP inactivity timer is still running, and that the HSGW has full context for the UE (except for PMIP binding).

**Figure 34** Active Mode Optimized Handoff E-UTRAN to eHRPD
1. 1a. E-UTRAN receives CDMA measurement reports from the UE and makes a HO decision.

   1b. UE sends an HRPD Connection Request message to the E-UTRAN to request an HRPD traffic channel. This request is forwarded to the MME. See TS 23.402 [23] for details. This Connection Request message includes an emergency indication.

   1c. The MME sends the P-GW address(es) and the associated APNs and the uplink GRE key(s) along with the HRPD Connection Request message to the eHRPD access node over the S101 tunnel.

   NOTE: The GRE keys (one for each APN) sent in step 1c are further sent in step 2a to the HSGW, and the HSGW uses them for uplink traffic towards the P-GW after the HO. The same keys are in use between the S-GW and P-GW before the HO. Using the same keys assures that the P-GW can associate the uplink data to the right UE, if the HSGW decides to send uplink data even before the PBA message is received in step 8b (note that the P-GW as defined in 23.402 [23] is equipped to receive data with the same GRE key even before updating the binding).

2. 2a. The eHRPD eAN/ePCF allocates the requested radio resources and sends an A11-Registration Request message to the HSGW. In this message the eAN/ePCF includes the P-GW address(es), the associated uplink GRE key(s) received in step 1c and the indicator that the UE is communicating via a tunnel (ref. Tunnel Mode indicator in A.S0022 [4]). This A11-Registration Request includes an emergency indication.

   2b. The HSGW responds with an A11-Registration Reply containing a forwarding address (i.e., HSGW IP address, GRE key per APN, and associated APN(s)).

3. In response to the HRPD Connection Request message received in step 1c, the eHRPD eAN/ePCF sends the HRPD Traffic Channel Assignment (TCA) message in an S101 message to the MME. The S101 message also carries the HSGW IP address, GRE key(s) for data forwarding, and associated APN(s).

4. 4a. The MME configures resources for indirect data forwarding and signals the HSGW IP address and GRE key(s) to the S-GW. The S-GW confirms data forwarding resources.

   4b. The MME forwards the HRPD TCA message embedded in the S101 message to the E-UTRAN which forwards it to the UE over the airlink.

5. E-UTRAN may return downlink IP packets back to the S-GW to be sent to the HSGW over the S103 interface. The HSGW will perform any necessary processing on the IP packets and forward them over the appropriate A10 connection to the eAN/ePCF.

6. 6a. L2 attach is completed (i.e., the UE acquires the eHRPD radio).

   6b. The UE sends a Traffic Channel Completion (TCC) message to the eHRPD eAN/ePCF.

7. 7a. The eHRPD eAN/ePCF sends an A11-Registration Request carrying an Active Start airlink record and the indicator that the UE is now operating on the eHRPD radio to the HSGW.

   7b. The HSGW responds to the eHRPD eAN/ePCF with an A11-Registration Reply.

8. 8a. Triggered by step 7a, the HSGW/MAG sends a PBU(s) to establish a PMIPv6 tunnel(s) with the P-GW(s) the UE is associated with.

   8b. The P-GW processes the PBU and updates the binding cache entry for the UE. The same IP address(es) or prefix(es) are assigned to the UE. The P-GW/LMA sends a PBA message to the HSGW/MAG, including the IP address(es)/prefix(es) allocated for the UE. The PMIPv6 tunnel is now setup.

   8c. The P-GW requires configuration for enforcing policy, the P-GW sends a Modify IP-CAN session message to the hPCRF. The P-GW has requested an IP-CAN session, the hPCRF responds to the P-GW with a Modify IP-CAN session Ack message. This message includes the Policy and Charging rules provisioned into the P-GW.

   Note: Steps 8a to 8c are repeated for each PDN connection that is to be established.
8d. The eHRPD eAN/ePCF signals handoff completion to the MME to confirm HO completion, and receives an acknowledgement.

9. L3 attach is completed and the UE can now send/receive packets to/from the eHRPD access network.

10. The E-UTRAN system, including eNodeB, MME, S-GW, and P-GW release resources, including sending a PMIPv6 BRI message from the P-GW to the S-GW as specified in TS 29.275 [35]. See also TS 23.402 [23].

11. If the UE had not completed PDN connection and bearer addition/deletion while on E-UTRAN, the UE completes those activities over the eHRPD radio. If the UE has authenticated during the pre-registration phase, and if any PDN connection is added or deleted while the UE is operating on E-UTRAN, similar changes are made in the HSGW via the use of VSNCP.

11a. If the UE has authenticated during the pre-registration phase, and if the HSGW receives a VSNCP Configure-Request for a PDN connection for which it does not have a P-GW identity, it obtains that information via an AAR/AAA exchange with the HSS/AAA. If the HSGW already has the corresponding P-GW IP address, or receives it from the HSS/AAA associated with the VSNCP Configure-Request message, the HSGW exchanges PBU/PBA messages with the P-GW. The exchanges of AAR/AAA and PBU/PBA messages are not shown in the figure.
4.10.10.3 Non-Optimized Handoff from E-UTRAN to eHRPD for Emergency Services

This procedure is used in the case there is no eHRPD session for the UE in the target eHRPD system. This scenario assumes that the UE is operating initially on E-UTRAN as an unauthenticated UE.

1. It is assumed that the UE does not have an existing eHRPD session with the eAN/ePCF (thus, the HSGW has no saved context for the UE). It is also assumed that the UE is operating initially on E-UTRAN as an unauthenticated UE. The UE does not use S101 to pre-register with eHRPD. When the UE attaches to eHRPD, it needs to go through full eHRPD session establishment and establish complete emergency context with the HSGW.

2. The UE is in E-UTRAN. Based on some trigger, the UE decides to perform cell re-selection to the eHRPD eAN. Note: the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network. The eNB may be involved in redirecting the UE to eHRPD.
3. The UE follows the steps 1 to 4 from the call flow in section 4.10.8.2 to establish an eHRPD session and a PPP session with the HSGW.

4. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, PDN Type, APN, PDN Address, Protocol Configuration Options, Attach Type = “Handover Attach”, and Emergency Indicator=1. The APN supplied in the VSNCP Configure-Request may be ignored by the HSGW, since the UE indicates “emergency”.

5. The HSGW performs the Gateway Control Session Establishment procedure with the PCRF (see TS 23.203 [20]). As part of this step, the PCRF sends the QoS rules and events to the HSGW.

6. The HSGW sends a Proxy Binding Update (using the UE identity as described in section 4.10.8) to the P-GW identified in the HSGW Emergency Configuration Data in order to update the registration see TS 29.275 [35].

7. The P-GW performs a PCRF interaction to retrieve the QoS policy parameters.

8. The P-GW responds with a PBA message to the HSGW see TS 29.275 [35].

9. The HSGW sends a VSNCP Configure-Ack (PDN-ID, APN, PDN Address, PCO, Attach Type, “Mobile Identity” configuration option, and and Emergency Indicator=1) message to the UE over the main service connection. The Protocol Configuration Options parameter may indicate the Selected Bearer Control Mode.

   NOTE: If dynamic policy is not supported, the Selected Bearer Control Mode is “MS-only”.

10. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID, Emergency Services Supported Indicator=1, and the IPv4 Default Router Address if an IPv4 address is to be assigned either immediately or deferred.

11. The UE responds with a VSNCP Configure-Ack message.

12. (optional) The UE can now issue a DHCPv4 Request (optionally with rapid commit option) message on the BE service connection provided the UE requested deferred IP address allocation in Step 8.

13. 13a. The UE may send a Router solicitation message.

   13b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

Step 14 is repeated as necessary until all bearers are established.

14. Bearers for the emergency PDN connection are re-established on eHRPD based on the Selected Bearer Control Mode:

   a.) If the Selected Bearer Control Mode is “MS-only”, the HSGW assumes that the UE will establish all bearers. The UE performs UE requested bearer resource allocation – section 4.10.9.1 for all bearers.

   b.) If the Selected Bearer Control Mode is “MS/NW”, the HSGW establishes all bearers. The HSGW performs network initiated dedicated bearer setup – section 4.10.9.2 for all bearers.
4.11 Header Compression

The UE and HSGW may perform header compression using the protocol types specified using the Compression Parameter configuration option (see section 9.1.4.1). The header compression for service connections using SO72 is not supported in this version of the specification. The UE shall not initiate either RAN based or HSGW based header compression when service option SO72 is used. The HSGW shall not initiate HSGW based header compression when service option SO72 is used.

The header compression protocol types are negotiated independently for forward link and reverse link. The header compression protocol negotiated via the VSNCP protocol may be used on the main service connection (SO59), and on any auxiliary service connection using SO64, when data from that PDN connection is placed on those service connections using the VSNP extend code capability.

The header compression for service connections using SO67 is performed according to the procedures of A.S0008 [1] / A.S0009 [2]. Such compression is independent of the header compression negotiation done via the VSNCP protocol.

The VSNP Extend Code (see section 9.1.5) shall be used when a header compression protocol is used over SO59 or SO64.

4.11.1 ROHC Support

If the UE and the HSGW support ROHC, the UE and HSGW shall support the RoHC Profile 0x0000 (uncompressed profile) on both forward and reverse links. The UE and HSGW may support other RoHC profiles as specified in RFC 3095 [58], RFC 3843 [68], RFC 4019 [71], RFC 4815 [75], RFC 4996 [77], and RFC 5225 [79] independently on the forward and reverse link. If multiple ROHC profile identifiers corresponding to the same profile type (for example, RTP profile) are supported by both UE and HSGW, the profile corresponding to the highest value supported by both UE and HSGW shall be used.

4.12 Improved Non-Optimized Handoff

This section describes a method to reduce the interval before user data can be sent between the UE and network following an E-UTRAN to eHRPD non-optimized active handoff.

A major component of the interval is the time it takes to setup the main A10 service connection, perform LCP and PPP, and authenticate the UE. This time is eliminated if the context created during execution of these procedures already exists in the UE and HSGW prior to handoff. This context is the same as the UE partial context described in section 9.1.9. Section 4.12.1 describes creation of the UE partial context.

UE partial context can be created directly over the eHRPD air interface or indirectly via the S101 interface. The process starts when the UE attaches directly or indirectly to eHRPD. It is the UE responsibility to choose when this happens. After the UE attaches to eHRPD, the main service connection is created. LCP is initiated and the HSGW and UE perform normal session setup through UE authentication, at which point the UE does not continue with NCP (i.e., it does not send VSNCP signaling to the HSGW). The HSGW then applies a timer to maintain the UE partial context in the HSGW for a period of time determined by the operator. Likewise, the UE maintains its internal context.
Support for and use of UE partial context is an operator decision.

### 4.12.1 UE Partial Context Establishment

The following call flow describes the steps that are performed to establish a UE partial context. This call flow depicts the steps performed when the UE is directly attached to eHRPD.

![Diagram of UE Partial Context Establishment on eHRPD without PMIP Tunnel]

**Figure 36** Partial Context Establishment on eHRPD without PMIP Tunnel

1. The UE decides to create a UE partial context.
2. The UE establishes an eHRPD air interface session with the eAN over the eHRPD air interface.
3. If RAN-level authentication is required, the UE establishes an AN-PPP connection with the eAN/ePCF and performs RAN-level authentication using the A12 interface.
4. The eHRPD eAN/ePCF establishes the main A10 connection with the HSGW by exchanging A11-RRQ/RRP messages. The HSGW initiates LCP and the UE and HSGW perform PPP connection establishment procedures.
5. 5a-b. The authentication and authorization procedure is performed using EAP-AKA’.
   5c. The HSGW stores the information received from the 3GPP AAA/HSS server.
   5d. The UE does not initiate PDN connection establishment. The UE and HSGW maintain the UE partial context and the HSGW starts a timer.
5 S2a Interface from the HSGW to the P-GW

5.1 Protocol Definition

The HSGW to P-GW interface carries control and bearer traffic between the two network elements. This interface is based on the 3GPP S2a reference point defined in TS 23.402 [23].

5.2 HSGW Requirements

The HSGW shall act as the Mobile Access Gateway (MAG) as specified in RFC 5213 [78] and in RFC 5844 [82]. The HSGW shall support Binding Revocation for IPv6 Mobility as defined in RFC 5846 [84] and GRE Key option for Proxy MIPv6 as RFC 5845 [83].

The HSGW shall use the NAI received from 3GPP AAA in the Permanent User Identity IE (Mobile-Node-Identifier AVP) upon successful authentication and authorization to populate the Mobile Node Identifier option in the PBU.

5.2.1 PMIPv6 Triggers

HSGW shall trigger PMIPv6 procedures as specified in this section.
5.2.1.1 PMIPv6 Registration Triggers

The HSGW shall trigger PMIPv6 registration procedures only if it determines that the UE is operating on the eHRPD radio. The HSGW determines that the UE is operating on the eHRPD radio when the “tunnel mode indicator” is set to 0 or no tunnel mode indicator is included in the last received A11-Registration Request message for the UE.

After the HSGW has determined that the UE is operating on the eHRPD radio, the HSGW triggers PMIPv6 registration as described below.

- When the HSGW receives a VSNCP Configure-Request from the UE that requests PDN connection establishment and the attach type is “Initial Attach” and the VSNCP Configure-Request does not include the Emergency Indicator configuration option or includes the Emergency Indicator configuration option with the value set to 0, the HSGW shall perform P-GW selection as per TS 23.402 [23] and then it shall trigger PMIPv6 registration for the corresponding PDN.

- When the HSGW receives a VSNCP Configure-Request from the UE that requests PDN connection establishment and the attach type is “Initial Attach” and the VSNCP Configure-Request includes the Emergency Indicator configuration option with the value set to 1, the HSGW shall select the emergency P-GW indicated in the HSGW Emergency Configuration Data (see section 4.10.1), and then it shall trigger PMIPv6 registration for the emergency PDN.

- When the HSGW receives a VSNCP Configure-Request from the UE that requests PDN connection establishment and the attach type is handover attach and the VSNCP Configure-Request does not include the Emergency Indicator configuration option or includes the Emergency Indicator configuration option with the value set to 0, the HSGW shall select the P-GW for the PDN connection indicated by the current HSS data (ref. TS 29.273 [34]) and then it shall trigger PMIPv6 registration for the corresponding PDN.

- When the HSGW receives a VSNCP Configure-Request from the UE that requests PDN connection establishment and the attach type is handover attach and the VSNCP Configure-Request includes the Emergency Indicator configuration option with the value set to 1, the HSGW shall select the emergency P-GW indicated in the HSGW Emergency Configuration Data (see section 4.10.1), and then it shall trigger PMIPv6 registration for the emergency PDN.

- When the HSGW receives an A11-Registration Request message with an Active Start airlink record for the UE that has one or more PDN contexts established in the HSGW, the HSGW shall trigger PMIPv6 registration for each PDN context setup that was requested by the UE and indicated by the current HSS data as being a current PDN connection if the PMIPv6 registration does not exist (ref. TS 29.273 [34]).

- When the HSGW receives a DHCPDISCOVER message (with or without Rapid Commit option), the HSGW shall trigger PMIPv6 registration only if it previously received a PBA message containing deferred IPv4 address assignment indicator and no IPv4 Address Acknowledgment Option. The HSGW also passes the DHCP message to the P-GW as specified in Section 4.4.4.

- When the HSGW receives a Hack message with context information TLVs as defined in Section 11.3.2, the HSGW shall trigger PMIPv6 registration for each PDN connection that was connected to the source HSGW as indicated in the context information.
The HSGW shall trigger PMIPv6 re-registration for PDN connection(s) as needed to prolong the lifetime of existing PMIPv6 session(s).

### 5.2.1.2 PMIPv6 De-registration Triggers

- When the HSGW receives a VSNCP Termination Request from the UE that requests PDN connection teardown, the HSGW shall perform PMIPv6 de-registration for the corresponding PDN.

- When the HSGW receives an indication from the PCRF requesting termination of a PDN connection, the HSGW shall perform PMIPv6 de-registration for the corresponding PDN.

- When the HSGW receives a BRI from the P-GW with the revocation trigger set to a non-handover value, the HSGW shall send VSNCP Terminate-Request to the UE. See section 9.1.4.6.

- When the main service connection is removed, the HSGW shall trigger PMIPv6 de-registration from all connected PDNs.

- When the HSGW receives an LCP Terminate-Request from the UE, the HSGW shall trigger PMIPv6 de-registration from all connected PDNs.

### 5.2.2 PMIPv6 Registration Process

The PMIPv6 registration process over S2a is described in TS 23.402 [23] and specified in TS 29.275 [35].

### 5.2.3 PMIPv6 Revocation Support

Upon receiving a PMIPv6 Binding Revocation Indication (BRI) message from the P-GW with revocation trigger = “Inter-MAG Handoff - same Access Types” (i.e., inter-HSGW handoff), the HSGW shall clear all UE session context (including LCP, CCP, Authentication, PDN context, and TFTs). If the HSGW supports inter-HSGW context transfer, the HSGW shall defer the UE session context clean up until inter-HSGW handoff is complete (see section 11.1.1). The HSGW responds to the BRI from the P-GW by sending a Binding Revocation Acknowledgement (BRA).

When the HSGW receives PMIPv6 Binding Revocation Indication (BRI) from the P-GW with revocation trigger = “Inter-MAG Handoff - different Access Types” (i.e., inter-technology handoff), the HSGW shall delete the PDN context and TFTs associated with the UE for that PDN connection, and then follow the procedures in section 9.1.8. However, in this release, the HSGW shall delete all PDN contexts and TFTs associated with the UE and then follow procedures in section 9.1.7.

### 5.3 P-GW Requirements

P-GW requirements are defined in TS 23.402 [23].

The P-GW supports the procedures of TS 29.275 [35].
5.4 Call Flows

5.4.1 S2a Connection Establishment with the Default PDN

PMIPv6 (see RFC 5213 [78] and TS 29.275 [35]) signaling is used to establish an S2a connection between the HSGW and the P-GW. The sample call flow in Figure 37 illustrates the establishment of the PMIPv6-based S2a connection when the UE attaches to the eHRPD access network for the first time.
**Figure 37** S2a Connection Establishment with the Default PDN

1. Session Establishment
2. UE is ready to send data.
3. Device Level Authentication
4. Location Update Procedure
5. A11-RRQ/RRP
6. PPP LCP Negotiation, EAP selected as authentication protocol
7. EAP-AKA' Authentication
8. VSNCP Configure-Request (PDN-ID, ...)
9. Gateway Control Session Setup
10. PMIP Binding Update
11. IP-CAN session establishment procedure
12. Update PDN GW address
13. PMIP Binding Ack
14. Gateway Control and QoS Rules Provision/ Ack
15. VSNCP Configure-Ack (PDN-ID, ...)
16. VSNCP Configure-Request (PDN-ID)
17. VSNCP Configure-Ack (PDN-ID)
18. DHCP Discover (Optional)
1. The UE and the eAN initiate eHRPD session establishment. During this procedure, the eAN
determines that it connects with a UE.

2. The UE is ready to send data.

3. (Optional) The UE and eAN perform device level authentication procedures.

4. (Optional) The UE may perform the eHRPD Location Update procedure.

5. The ePCF recognizes that no A10 connection associated with the UE is available, and selects
an HSGW. The ePCF sends an A11-Registration Request message to the HSGW to set up the
main A10 connection, and optionally set up the Best Effort (BE) auxiliary connection. The
A11-Registration Request is validated and the HSGW accepts the connection by returning an
A11-Registration Reply message.

6. The UE and HSGW perform LCP negotiation and select EAP-AKA’ as the authentication
protocol.

7. The authentication procedures are initiated and performed involving the UE, the HSGW, the
3GPP2 AAA Proxy and the 3GPP AAA Server. In the roaming case, there may be several
AAA proxies involved. The P-GW address is determined at this point. The AAA/HSS sends
subscription data to the HSGW. The Subscription Data contains the list of all APNs that the
UE is permitted to access and an indication about which of those APNs is the Default APN.
The subscription data also contains the NAI to be used to identify the UE in Proxy Binding
Update and Gateway Control Session Establishment messages. This information is cached at
the HSGW on behalf of the attaching UE. If the subscriber profile did not include an absolute
P-GW address a DNS look up may be performed to determine the P-GW address. At the end
of this step, the Authentication phase is complete. Also, the HSGW has received the
subscription profile of the UE from the HSS/AAA.

7a. The HSGW may send an A11-Session Update message to the eAN/ePCF to provide the
PMK, if the ePCF set the PMK Indicator to ‘1’ in the A11-Registration Request in step 5.

7b. The eAN/ePCF responds with an A11-Session Update Acknowledge message.

8. The UE sends a VSNCP Configure-Request message over the main service connection. The
information in the message includes a PDN-ID, PDN Type, APN, PDN Address with empty
content, Protocol Configuration Options, and Attach Type = “Initial Attach”. If the UE wants
to establish a MUPSAP connection to the APN and has not yet been informed that the HSGW
does not support MUPSAP for this APN, the User Context Identifier configuration option is
also included in the VSNCP Configure-Request message. The Address Allocation Preference
option contained in the Protocol Configuration Options indicates whether the UE wants to
perform the IPv4 address allocation during the attach procedure or deferred IPv4 address
allocation. PDN Type indicates the UE’s IP capability (IPv4, IPv6 or IPv4v6). Additional
configuration options (e.g., IPv4 Default Router Address) are included depending upon the
PDN Type. If the UE supports NW Requested Bearer Control, then the UE includes the
option in the Protocol Configuration options parameter set to “MS/NW” mode.

9. The HSGW may perform Gateway Control Session Establishment procedure with the PCRF.
If performed, the HSGW indicates the possible bearer control modes according to the UE
capability provided in step 8 and its own capability. The PCRF selects the bearer control
mode to be used.

10. The HSGW sends a Proxy Binding Update to the P-GW in order to establish the new
registration see TS 29.275 [35]. The HSGW uses the NAI received in step 7 to identify the
UE. If the VSNCP message in step 8 does not identify a requested APN, the HSGW will use
the default APN acquired from HSS/AAA during Authentication and Authorization
procedures to choose the P-GW. If the VSNCP message in step 8 identifies a requested APN
that is authorized to the user, the HSGW will use that APN to choose the P-GW. If the HSGW
supports MUPSAP and if the HSGW has received the User Context Identifier configuration
option in the VSNCP Configure-Request message in step 8, the HSGW includes the PDN Connection ID information element in the Proxy Binding Update message.

11. The P-GW performs a PCRF interaction to establish the IP-CAN session. For details, see TS 23.203 [20].

12. The selected P-GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection.

13. The P-GW responds with a PBA message to the HSGW see TS 29.275 [35]. If the P-GW supports MUPSAP and if the PDN Connection ID information element is included in the Proxy Binding Update message, it includes PDN Connection ID information element received in the Proxy Binding Update message.

14. In case the QoS rules have changed, the PCRF updates the QoS rules at the HSGW by the exchange of Gateway Control and QoS Rules Provision/Ack messages, as specified in TS 23.203 [20].

15. The HSGW sends a VSNCP Configure-Ack (PDN-ID, APN, PDN Address, PCO, Attach Type, and Address Allocation Cause) message to the UE over the main service connection. If the PBA message from the P-GW includes the PDN Connection ID information element, the HSGW includes the corresponding User Context Identifier configuration option in the VSNCP Configuration-Ack message. Note that the PDN Address Information may contain an IPv4 address for IPv4 and/or an IPv6 Interface Identifier for IPv6. Additional configuration options (e.g., IPv4 Default Router Address) are included if present in the Configure-Request. The Protocol Configuration Options parameter may be included to indicate the Selected Bearer Control Mode, if the Protocol Configuration Options parameter was included by the UE in the corresponding VSNCP Configure-Request and indicated support for NW Requested Bearer Control.

16. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID configuration option. The message includes the User Context Identifier configuration also if such configuration option has been accepted by the HSGW. This message contains the APN-AMBR if received from the HSS/AAA.

17. The UE responds with a VSNCP Configure-Ack message. The UE includes APN-AMBR, if it received APN-AMBR in step 16 and if the UE supports APN-AMBR.

18. (optional) The UE can now issue a DHCPv4 DISCOVER (optionally with rapid commit option) message on the BE service connection provided the UE requested deferred IP address allocation in Step 8.

19a. The UE may send a Router solicitation message.

19b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

20. The IP address allocation details are described in section 4.2.

Based on information stored at the UE or obtained from the network, the UE can start creating the required auxiliary connections (needed for the bearer transport) for a particular QoS flow per PDN. See section 9.3.

### 5.4.2 S2a Connection Release

See section 10 for call flows addressing PDN connection release.

### 5.4.3 S2a Additional PDN Connection Establishment

See section 9.3.1 for call flows addressing additional PDN connection establishment.
5.4.4 S2a Connection Movement at Handoff

See sections 11.1, 11.1.2, and 12.1.2 for call flows addressing PDN connection movement at handoff.

5.4.5 S2a Connection Release at De-Registration

See section 10 for call flows addressing PDN connection release at de-registration.
6 Interface between the HSGW and the AAA

The HSGW and 3GPP2-AAA-Proxy server utilize AAA protocols based on the Diameter Protocol specified in RFC 3588 [63]. The HSGW interfaces to the 3GPP2 AAA Proxy/Server over the Pi* reference point; and the 3GPP2 AAA Proxy/Server interfaces to the 3GPP AAA server over the STa reference point as defined by TS 23.402 [23].

6.1 HSGW and 3GPP2 AAA Proxy/Server

The Pi* reference point supports the STa Diameter Application as specified by TS 29.273 [34] and optionally, the Pi*3GPP2 Diameter Application as defined by this specification.

In this version of this specification, the PiLTE Interworking Diameter Application has been replaced by the Pi*3GPP2 Diameter Application.

Both the HSGW and the 3GPP2 AAA Proxy/Servers are required to support the STa Diameter Application and thus shall advertise support for the STa Diameter Application during the Diameter Capability Exchange procedure. The peers shall include the Vendor-Specific-Application-Id (VSA) in the Diameter Capability Exchange Request with the Vendor-Id attribute set to the SMI Network Management Private Enterprise Codes assigned to 3GPP (10415) and the Auth-Application-Id set to the STa Diameter Application ID of 16777250 as assigned by IANA.

An HSGW that supports the HSGW relocation procedures or the Subscriber QoS Profile Configuration Procedure may additionally advertise support for the Pi*3GPP2 Diameter Application during the Diameter Capability Exchange procedure.

A 3GPP2 AAA Proxy/Server that supports HSGW relocation procedures or the Subscriber QoS Profile Configuration Procedure may additionally advertise support for the Pi*3GPP2 Diameter Application during the Diameter Capability Exchange procedure.

The peers shall include the Vendor-Specific-Application-Id VSA in the Diameter Capability Exchange Request with the Vendor-Id attribute set to the SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535) and the Auth-Application-Id set to the assigned by IANA:

\[ \text{Pi*3GPP2 Diameter Application Identifier} = 16777298 \]

The Pi*3GPP2 Diameter Application Identifier as described in this specification shall be used if both the 3GPP2 AAA Proxy/Server and the HSGW support it.

In case the STa Diameter Application is used, the 3GPP2 AAA Proxy/Server shall proxy the messages between the HSGW and the 3GPP AAA server.
6.2 3GPP2 AAA Proxy/Server and 3GPP AAA Server

The STa interface supports the STa Diameter Application as specified by TS 29.273 [34] and is mandatory to use over the STa reference point.

The 3GPP2 AAA Proxy/Server shall advertise support for the STa Diameter Application during the Diameter Capability Exchange procedure by including the Vendor-Specific-Application-Id (VSA) in the Diameter Capability Exchange Request with the Vendor-Id attribute set to the SMI Network Management Private Enterprise Code assigned to 3GPP (10415) and the Auth-Application-Id set to the STa Diameter Application ID of 16777250 as assigned by IANA.

The 3GPP2 AAA Proxy/Server shall remove all attributes that are not supported by the 3GPP AAA STa Diameter Application before forwarding any 3GPP AAA STa commands to the 3GPP AAA Server. Specifically:

- If received by the 3GPP2 AAA Proxy/Server, the 3GPP2 AAA Proxy/Server shall remove the Supported-Features AVP with Vendor-ID AVP set to the 3GPP2 SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535).

Upon receiving 3GPP AAA STa Diameter Application commands, the 3GPP2 AAA Proxy/Server may modify the commands to align them with Pi*3GPP2 Diameter Application.

6.3 Pi*3GPP2 Diameter Application

The Pi*3GPP2 Diameter Application extends the STa Diameter Application by introducing the following commands (request/answer pairs) and AVPs required to support the inter-HSGW handoff procedure and Subscriber QoS Profile Configuration Procedure defined in this specification. The following table lists the commands and associated command codes:

<table>
<thead>
<tr>
<th>Command</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Location Request/Answer (ULR/ULA)</td>
<td>8388626</td>
</tr>
<tr>
<td>Cancel Location Request/Answer (CLR/CLA)</td>
<td>8388627</td>
</tr>
<tr>
<td>Query Profile Request/Answer (QPR/QPA)</td>
<td>8388630</td>
</tr>
</tbody>
</table>

The Pi*3GPP2 Diameter Application reuses the remaining commands and AVPs of the 3GPP AAA STa Diameter Application as defined in this specification and in TS 29.273 [34].

The Update Location Request/Answer (ULR/ULA) and the Query Profile Request/Answer (QPR/QPA) command pair are implemented by using a set of ‘features’, with each feature being specified by the use of Supported-Features AVP. Unique settings of the Feature-List-ID and Feature-List sub AVP pair are used to indicate support for a specific feature, with each bit in the Feature-List sub AVP being independent of the others. All command pairs are specified in the ABNF format. The following features are specified for the Pi*3GPP2 Diameter Application:

- Subscriber QoS Profile Configuration (SubQoSConfig)
HSGW Relocation (HSGWReloc)

Pi*3GPP2 Diameter Application is defined between the HSGW and the 3GPP2 AAA Proxy/Server as the peer entities. An operator may choose to extend Pi*3GPP2 Diameter Application between the HSGW and the 3GPP2 AAA Proxy/Server in the home domain. In the latter case, the 3GPP2 AAA Proxy/Server shall act as a proxy agent as specified in RFC3588 [63].

The Pi*3GPP2 Diameter Application utilizes the Supported-Features AVP in QPR/QPA and ULR/ULA request/answer pairs as follows:

- The Supported-Features AVP ‘M’ bit shall be set in the ‘Request’ commands.
- The Vendor-Id sub AVP shall be set to the 3GPP2 SMI Network Management Private Enterprise Code assigned to 3GPP2 (5535).
- The Feature-List-ID sub AVP value shall be set to ‘1’ “Query Group”.
- The Feature-List sub AVP shall have the bits set as specified in Table 2 below:
Table 2  Features of Feature-List-ID = “Query Group” Defined for the 
Pi*3GPP2 Diameter Application

<table>
<thead>
<tr>
<th>Feature bit</th>
<th>Feature</th>
<th>M/O</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SubQoSConfig</td>
<td>M</td>
<td>Subscriber QoS Profile Configuration Procedure. This feature allows the configuration of Subscriber QoS Profile in the eHRPD system. The Subscriber QoS Profile is obtained from the 3GPP2 AAA Proxy/Server in the home domain. If both the HSGW and the 3GPP2 AAA Proxy/Server support the Pi*3GPP2 Diameter Application, the HSGW initiates obtaining Subscriber QoS Profile information from the 3GPP2 AAA Proxy/Server in the home domain by sending the Query Profile Request (QPR) command. If the HSGW does not already know if the 3GPP2 AAA Proxy/Server supports the ‘SubQoSConfig’ feature, the HSGW includes the Supported-Features AVP in the QPR command with Feature-List sub AVP bit ‘0’ set to ‘1’ indicating support for SubQoSConfig feature. The 3GPP2 AAA Proxy/Server responds with Query Profile Answer (QPA) command that includes the complete set of features supported by it in the Supported-Features AVP. If the 3GPP2 AAA Proxy/Server supports the Subscriber QoS Profile Configuration procedure and has the Subscriber QoS Profile available, on successful processing of the QPR command, the 3GPP2 AAA Proxy/Server returns the Subscriber QoS Profile information also in the QPA command with the DIAMETER_SUCCESS result code.</td>
</tr>
<tr>
<td>1</td>
<td>HSGWReloc</td>
<td>M</td>
<td>HSGW Relocation Procedure. This feature allows the HSGW to update AT’s location information at the 3GPP2 AAA Proxy/Server. The procedure is invoked by the HSGW and is used to inform the 3GPP2 AAA Proxy/Server about the identity of the HSGW currently serving the user. If both the HSGW and the 3GPP2 AAA Proxy/Server support the Pi*3GPP2 Diameter Application, the HSGW initiates HSGW Relocation procedure by sending the Update Location Request (ULR) command. If the HSGW does not already know if the 3GPP2 AAA Proxy/Server supports the ‘HSGWReloc’ feature, the HSGW includes the Supported-Features AVP in the ULR command with Feature-List sub AVP bit ‘1’ set to ‘1’ indicating support for HSGWReloc feature. The 3GPP2 AAA Proxy/Server responds with Update Location Answer (ULA) command that includes the complete set of features supported by it in the Supported-Features AVP. If the 3GPP2 AAA Proxy/Server supports the HSGW Relocation procedure, on successful processing of the ULR command it updates the identity of the HSGW currently serving the AT. The 3GPP2 AAA Proxy/Server then initiates Cancel Location Request/Answer (CLR/CLA) procedures with the previously serving HSGW and returns Update Location Answer (ULA) command to the serving HSGW.</td>
</tr>
<tr>
<td>2-31</td>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Feature bit:** The number of the bit within the Supported-Features AVP, set to "1" if the corresponding feature is supported.

**Feature:** A short name that can be used to refer to the bit and to the feature.

**M/O:** Defines if the implementation of the feature is mandatory ("M") or optional ("O") by the 3GPP2 AAA Proxy/Server.

**Description:** A textual description of the feature.
6.3.1 Inter-HSGW handoff procedure

The following commands are used for the Inter-HSGW handoff procedure.

6.3.1.1 Update Location Request (ULR) command

The (ULR) command, indicated by the Command-Code field set to 8388626 and the "R" bit set in the Command Flags field, is sent from the HSGW to the 3GPP2 AAA Proxy/Server.

Message Format

< Update Location Request> ::= < Diameter Header: 8388626, REQ, PXY, 16777298 >
< Session-Id >
{Auth-Application-Id}
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[ Destination-Host ]
{ Destination-Realm }
{ User-Name }
{ RAT-Type }
* [ Supported-Features ]
* [ AVP ]
* [ Proxy-Info ]
* [ Route-Record ]

6.3.1.2 Update Location Answer (ULA) command

The Update Location Answer (ULA) command, indicated by the Command-Code field set to 8388626 and the 'R' bit cleared in the Command Flags field, is sent from the 3GPP2 AAA Proxy/Server to the HSGW.

Message Format

< -Update Location Answer> ::= < Diameter Header: 8388626, PXY, 16777298 >
< Session-Id >
{Auth-Application-Id}
[ Result-Code ]
[ Experimental-Result ]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
* [ Supported-Features ]
* [ AVP ]
* [ Failed-AVP ]
* [ Proxy-Info ]
* [ Route-Record ]

6.3.1.3 Cancel Location Request (CLR) command

The Cancel Location Request (CLR) command, indicated by the Command-Code field set to 8388627 and the "R" bit set in the Command Flags field, is sent from the 3GPP2 AAA Proxy/Server to the HSGW.
Message Format

< Cancel Location Request> ::= < Diameter Header: 8388627, REQ, PXY, 16777298 >
  < Session-Id >
  { Auth-Application-Id }
  { Origin-Host }
  { Origin-Realm }
  { Destination-Host }
  { Destination-Realm }
  { User-Name }
  { 3GPP2-Cancellation-Type }
  * [ AVP ]
  * [ Proxy-Info ]
  * [ Route-Record ]

6.3.1.4 Cancel Location Answer(CLA) command

The Cancel Location Answer(CLA) command, indicated by the Command-Code field set to 8388627 and the "R" bit cleared in the Command Flags field, is sent from the HSGW to the 3GPP2 AAA Proxy/Server.

< Cancel Location Answer> ::= < Diameter Header: 8388627, PXY, 16777298 >
  < Session-Id >
  { Auth-Application-Id }
  [ Result-Code ]
  [ Experimental-Result ]
  { Origin-Host }
  { Origin-Realm }
  * [ AVP ]
  * [ Failed-AVP ]
  * [ Proxy-Info ]
  * [ Route-Record ]
6.3.1.5 Inter-HSGW handoff procedure AVPs

The Inter-HSGW handoff procedure uses the following AVPs:

| 3GPP2-Cancellation-Type | 5535/56 |

6.3.1.5.1 3GPP2-Cancellation-Type

The 3GPP2-Cancellation-Type AVP is of type Enumerated and indicates the type of cancellation. The following values are defined:

HSGW LOCATION UPDATE PROCEDURE (0)

This value is used when the Cancel Location Request is sent to the source HSGW due to a received Update Location Request message from the target HSGW.
### 6.3.2 Subscriber QoS Profile Configuration Procedure

The following commands are used for the Subscriber QoS Profile Configuration procedure.

#### 6.3.2.1 Query Profile Request (QPR) command

The Query Profile Request (QPR) command, indicated by the Command-Code field set to 8388630 and the "R" bit set in the Command Flags field, is sent from the HSGW to the 3GPP2 AAA Proxy/Server.

Message Format

```
< Query Profile Request> ::= < Diameter Header: 8388630, REQ, PXY, 16777298>
   < Session-Id >
   {Vendor-Specific-Application-Id}
   {Auth-Session-State}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Host}
   {Destination-Realm}
   {User-Name}
   *[Supported-Features]
   * [AVP]
   * [Proxy-Info]
   * [Route-Record]
```
### 6.3.2.2 Query Profile Answer (QPA) command

The Query Profile Answer (QPA) command, indicated by the Command-Code field set to 8388630 and the "R" bit cleared in the Command Flags field, is sent from the 3GPP2 AAA Proxy/Server to the HSGW.

**Message Format**

```
< Query Profile Answer> ::= < Diameter Header: 8388630, PXY, 16777298>
   < Session-Id >
   {Vendor-Specific-Application-Id}
   [Result-Code]
   [Experimental-Result]
   {Auth-Session-State}
   {Origin-Host}
   {Origin-Realm}
   {User-Name}
   * [Redirect-Host]
   * [Supported-Features]
   {Service-Option-Profile}
   [Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort-Traffic]
   [Authorized-Flow-Profile-IDs-for-the-User]
   [Inter-User-Priority]
   [Max-Per-Flow-Priority-for-the-User]
   * [ AVP ]
   * [ Failed-AVP ]
   * [ Proxy-Info ]
   * [ Route-Record ]
```
7  **Gxa Interface between the HSGW and the PCRF**

This section describes the functions associated with policy which are part of E-UTRAN – eHRPD Connectivity and Interworking Architecture.

### 7.1 Protocol Definition

The HSGW to PCRF interface exchanges policy information between the two network elements. This interface is based on the 3GPP Gxa reference point defined in TS 23.402 [23].

The Gxa interface is based on an evolution of the Gx application specified in 3GPP 29.212 [29].

### 7.2 Stage 2 Flows

The protocol supported on the Gxa interface shall be Diameter. The Stage 2 procedures are specified in TS 23.203 [20]. The HSGW shall implement the following procedures from TS 23.203 [20]:

- Gateway Control Session Establishment
- Gateway Control Session Termination
- Gateway Control and QoS Rules Request
- Gateway Control and QoS Rules Provision

See TS 23.203 [20] for the details of these procedures.
### 7.2.1 Initial Attachment over S2a

The HSGW and P-GW access the PCRF to obtain the policy rules associated with the subscriber. The sample call flow diagram illustrates the procedure for obtaining policy rules when the UE powers-on in an eHRPD access and attaches to the EPS via the S2a interface. This procedure is based on similar procedure described in TS 23.402 [23].

---

**Figure 38 Initial attachment over S2a**

The operational interaction steps between the gateways and the PCRF in the procedure in Figure 38 only occur if dynamic policy provisioning is deployed. Otherwise policy rules may be statically configured with the gateways.

1. The S2a attach procedure per section 5.4.1, steps 1-8 is executed.
2. The HSGW initiates the Gateway Control Session Establishment Procedure with the hPCRF, as specified in TS 23.203 [20] by sending a Gateway Control Session Establishment message to the hPCRF. The HSGW provides the information to the hPCRF to correctly associate it with the IP-CAN session being established and also to convey subscription related parameters to the hPCRF. The HSGW also indicates the possible bearer control modes to the hPCRF according to the UE capability and its own capability. See TS 23.203 [20] for details on the parameters sent with this message.
3. The hPCRF sends an Acknowledge Gateway Control Session Establishment to the HSGW. The hPCRF may include the following information: QoS Rules, Event Triggers, and selected bearer control mode. The QoS policy rules are employed by the HSGW to perform Bearer Binding. The Event Triggers indicate events that require the HSGW to report to the hPCRF. See TS 23.203 [20] for more details.
4. The S2a attach procedure per section 5.4.1, steps 10-13 is executed.
5. In case the QoS rules have changed, the hPCRF updates the QoS rules at the HSGW by sending a Gateway Control and QoS Rules Provision message to the HSGW. This message will include QoS Rules and Event Triggers. See TS 23.203 [20] for more details.
6. The HSGW sends a Gateway Control and QoS Rules Provision Ack (Result) message to the hPCRF. The Result information element indicates whether the indicated QoS Rules could be implemented.

7. The S2a attach procedure per section 5.4.1, steps 15-20 is executed.
   This procedure applies to the non-roaming, roaming, and local breakout cases. For the roaming and local breakout cases, the vPCRF forwards messages between the HSGW and the hPCRF.

### 7.3 Gxa Reference Point – Stage 3

The Gxa reference point is located between the Policy and Charging Rules Function (PCRF) and the HSGW Bearer Binding and Event Reporting Function (BBERF). The Gxa reference point is used for:

- Provisioning, update and removal of QoS rules from the PCRF to the BBERF.
- Transmission of traffic plane events from the BBERF to the PCRF.
- Transmission of events reported by the PCEF (P-GW) to the BBERF via the PCRF.

The stage 3 information for the Gxa reference point is defined in TS 29.212 [29].

Signaling flows related to the Gxa interface are specified in TS 29.213 [30].
8  A11 Interface between the HSGW and the eAN/ePCF

The interface between the HSGW and eAN/ePCF is shown in Figure 1 for bearer (A10) and signaling (A11). The A10/A11 interfaces are specified by A.S0022 [4].

Flows showing the use of A11 messages for inter-eAN handoff are found in A.S0022 [4].

A message flow illustrating the use of A11 messages for pre-registration as used for E-UTRAN to eHRPD handoff is shown in section 12.1.

A message flow illustrating the use of A11 messages for handoff as used for E-UTRAN to eHRPD handoff is shown in section 12.1.2.

Flows showing the use of A11 messages for the initial attachment are found in A.S0022 [4].
9 Interface between the HSGW and the UE

The HSGW and the UE use the PPP protocol with vendor extensions (see RFC 3772 [67]) for signaling and user data transport over the main service connection. Auxiliary service connections provide transport for user bearers.

The UE-HSGW interface is made up of the main service connection and a number of auxiliary service connections. The main service connection and auxiliary service connections are logical connections established between UE and HSGW. As with the legacy system the auxiliary service connections may be setup to offer different grades of service to the user traffic through the RAN. Additionally, auxiliary service connections may be associated exclusively with traffic of a single PDN connection. The main service connection, packet framed auxiliary service connections using SO72, and auxiliary service connections with HDLC-like framing can be shared by more than one PDN connection. To accomplish this, a per-PDN indication (PDN identifier) is used to differentiate the traffic over these service connections.

The main service connection is used to provide a direct path between the UE and the HSGW for the exchange of connection management messages, EAP-AKA’ messages for access authentication, the exchange of bearer flow mapping information and the creation of per-PDN connections. The “Initial Attach” and “Detach” signaling take place using the PPP protocol (VSNCP) over the main service connection. The main service connection also supports IP traffic multiplexed from multiple PDNs.

When the UE attaches to the eHRPD eAN/ePCF, whether directly on the eHRPD radio interface or via S101 tunneling, and completes radio interface session configuration, the main service connection is established by the network for that UE. A BE auxiliary service connection may also be established.

- The main service connection is mapped over RLP-0 (see C.R1001 [11], C.S0063 [13] and C.S0087 [14]). This is done without the need for the UE to send a reservation request air interface message to the eAN/ePCF. The service option type used for setting up the main A10 connection is SO59. The HSGW shall discover the service option type from an extension received from the eAN/ePCF at the time service connection is established.

- The default auxiliary service connection for “best effort” bearer traffic may be configured (see C.R1001 [11], C.S0063 [13] and C.S0087 [14]). This is done without the need for the UE to send a reservation request air interface message to the eAN/ePCF. This default auxiliary “best effort” service connection, when established, is signaled to the HSGW on an A11-Registration Request message indicating service option 72 (IP packet framing, PDN multiplexing).

The 8-bit ReservationLabel (see C.S0063 [13]) is divided into two fields except for the 0xFF and 0xFE Reservations. The upper four bits identify the PDN. The lower four bits identify the IP flow uniquely for a certain PDN. The PDN identifier is selected by the UE for each additional PDN with which the UE chooses to connect, and is signaled to the HSGW at the time of PDN connection establishment.

The eAN uses the PDN-ID field of the ReservationLabel (Flow-ID) to determine whether the new reservation being requested can be added to an existing RLP flow. The eAN can only configure one auxiliary service connection of packet-based framing with the PDN-Mux protocol ID and uses it for BE traffic. The eAN may also configure auxiliary service connections that support HDLC-like framing (SO64) and packet framing (SO72) with PDN-
Mux. IP traffic from multiple PDNs with similar QoS can be multiplexed on auxiliary service connections of packet-based framing. The eAN is permitted to map IP traffic from multiple PDNs onto the main service connection. The eAN/ePCF signals the mapping of multiple Flow-IDs to the main service connection to the HSGW using the A11-Registration Request message, and the packets for those multiple Flow-IDs are differentiated using the PDN-ID within the VSNP header (see section 9.1.5). The eAN can map reservations with similar QoS from different PDNs onto the same auxiliary service connection of octet-based framing, and the packets for those multiple Flow-IDs are differentiated using the PDN-ID inserted just prior to the first octet of the IP packet.

After the UE moves from legacy HRPD to eHRPD, or vice versa, and when the data session is established, then the UE shall renegotiate PPP.

### 9.1 Main Service Connection between the UE and the HSGW

The evolved HRPD system enables the establishment of a PPP-based main service connection between the UE and the HSGW.

#### 9.1.1 Establishment of a Main Service Connection

In the evolved HRPD system the main service connection is configured to use octet-based HDLC-like framing. A PPP connection is established between the UE and the HSGW. The PPP-based main service connection provides a framework for subscription authentication, PDN connection configuration, IP packet transport, and QoS management.

During eHRPD session configuration, the eAN/ePCF will have determined that the UE will be operating in evolved mode, as defined in C.S0087 [15]. Upon subsequent connection establishment after successful HRPD session negotiation, eAN/ePCF will attach the UE to an HSGW. The HSGW and UE will then begin eHRPD procedures over PPP.

#### 9.1.2 HSGW-UE Link Layer Encapsulation

The messages which need to be exchanged across the main service connection include:

- EAP messages for authentication
- VSNCP signaling messages for establishment of PDN connectivity
- RSVP signaling messages over VSNP for establishment of TFTs and QoS
- User IP packets are also carried over the main service connection per section 9.1.5

The encapsulation format for messages sent over the main service connection is provided in RFC 3748 [66] with the exceptions discussed in sections 9.1.4 and 9.1.5.
9.1.3 PPP-Based Main Service Connection

PPP shall be used as the data link layer protocol between UE and HSGW for the main service connection. PPP shall be used as a signaling protocol framework for EAP, VSNCP, and RSVP messages using VSNP. It shall be also used for transport of IP packets over the main service connection using VSNP.

The messages supported in the VSNCP application are described in section 9.1.4.

The messages supported in the RSVP application are described in section 9.1.6.

Note: The default MRU value is 1500 octets; however, since the VSNP protocol adds an extra octet, an MRU value of at least 1501 can be considered to avoid fragmentation.

9.1.4 3GPP2 Vendor Specific Network Control Protocol (VSNCP) Packet for PDN Connectivity

The VSNCP packet format as defined in RFC 3772 [67] shall be used for PDN Connection procedures with the exceptions defined in this specification. A VSNCP message shall contain configuration options for a single PDN. The 3GPP2 VSNCP packet format is shown in Table 3.

VSNCP packets shall use 3GPP2 Organizationally Unique Identifier (OUI) value 0xCF0002.

<table>
<thead>
<tr>
<th>Code Identifier Length</th>
<th>OUI</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Code 1 through 7 (VSNCP Configure-Request, VSNCP Configure-Ack, VSNCP Configure-Nak, VSNCP Configure-Reject, VSNCP Terminate-Request, VSNCP Terminate-Ack, and VSNCP Code-Reject) as defined in RFC 3772 [67].

Note: Code ’3’ (VSNCP Configure-Nak) is not specified for the 3GPP2 VSNCP protocol. The UE/HSGW receiving a 3GPP2 VSNCP packet with Code field set to ’3’ shall respond with a 3GPP2 VSNCP Code-Reject (Code ’6’) packet.

Identifier As defined in RFC 3772 [67] and RFC 1661 [43].

Length As defined in RFC 3772 [67] and RFC 1661 [43].

OUI 0xCF0002

Data Zero or more configuration options as defined in the following sections.
9.1.4.1 3GPP2 VSNCP Configuration Options

Configuration options shall be encoded as specified in RFC 1661 [43]. Table 4 lists all the configuration options required for 3GPP2 VSNCP. A received configuration option that is unrecognized shall be ignored. The UE and the HSGW shall not encrypt any of the Configuration Options included in the VSNCP signaling.

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Type (decimal)</th>
<th>Configuration Option Length (octets)</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDN Identifier</td>
<td>01</td>
<td>3</td>
<td>PDN Identifier is a 1 octet identifier selected by the UE for a PDN. Valid values are from 0 to 14. The value 15 is reserved for future use. This option shall be present as the first configuration option in all 3GPP2 VSNCP packets.</td>
</tr>
<tr>
<td>Access point name</td>
<td>02</td>
<td>2-102</td>
<td>Value field of the Access Point Name IE as defined in TS 24.008 clause 10.5.6.1 [24], with the exception that an APN identifier may have zero length as specified in section 9.1.4.2.</td>
</tr>
<tr>
<td>PDN Type</td>
<td>03</td>
<td>3</td>
<td>Valid values are 1 – IPv4, 2 – IPv6, 3 – IPv4/IPv6 Value portion of the PDN Type IE as defined in 9.9.4.10 of TS 24.301 [25].</td>
</tr>
<tr>
<td>PDN address</td>
<td>04</td>
<td>3-15</td>
<td>Value portion of the “PDN Address” IE as defined in Section 9.9.4.9 of TS 24.301 [25]. In addition to the coding in TS 24.301, on the VSNCP Configure-Request message sent by the UE for initial attach to an APN, the PDN type field of the PDN Address option shall be set to ‘000’ and the Length field of the PDN Address option set to 3, with no IPv4 or IPv6 address information included.</td>
</tr>
<tr>
<td>Protocol configuration options</td>
<td>05</td>
<td>3-253</td>
<td>Value portion of the Protocol Configuration option value as defined in Section 9.9.4.11 of TS 24.301 [25] and in Section 10.5.6.3 of TS 24.008 [24].</td>
</tr>
<tr>
<td>Error Code</td>
<td>06</td>
<td>3</td>
<td>Error Code is used in Configure-Reject message when a PDN connection attempt is unsuccessful. See Table 5 for the supported error code values.</td>
</tr>
<tr>
<td>Attach Type</td>
<td>07</td>
<td>3</td>
<td>Valid values are 1 – “Initial Attach” to a PDN, 3 – “Handover” attach to a PDN.</td>
</tr>
<tr>
<td>IPv4 Default Router Address</td>
<td>08</td>
<td>6</td>
<td>Encoded as a 4-octet IPv4 address. Includes the IPv4 Default Router address assigned by the P-GW for the PDN connection.</td>
</tr>
<tr>
<td>Address Allocation Cause</td>
<td>09</td>
<td>3</td>
<td>See Table 6 for the supported Address Allocation Cause values.</td>
</tr>
<tr>
<td>Configuration Option</td>
<td>Type (decimal)</td>
<td>Configuration Option Length (octets)</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>APN-AMBR</td>
<td>10</td>
<td>4-8</td>
<td>APN Aggregate Maximum Bit Rate. Encoded as the value field (octets 3-end) of the APN-AMBR as specified in sub clause 9.9.4.2 of TS 24.301 [25].</td>
</tr>
<tr>
<td>IPv6 HSGW Link Local Address IID</td>
<td>11</td>
<td>10</td>
<td>Encoded as an 8-octet IPv6 interface identifier of the HSGW link local address.</td>
</tr>
<tr>
<td>User Context Identifier</td>
<td>12</td>
<td>3</td>
<td>User Context Identifier is a 4-bit identifier selected by the UE for each of the PDN connections to the same APN. Valid values are from 0 to 14. The value 15 is reserved for future use.</td>
</tr>
<tr>
<td>Emergency Indicator</td>
<td>13</td>
<td>3</td>
<td>Valid values are 1 – “emergency services request” 0 – “non-emergency services request” The absence of this configuration option implies “non-emergency services request”</td>
</tr>
<tr>
<td>Emergency Services Supported Indicator</td>
<td>14</td>
<td>3</td>
<td>Valid values are 1- “emergency services are supported” 0 – “emergency services are not supported” The absence of this configuration option does not imply either support or non-support of emergency services.</td>
</tr>
<tr>
<td>VSNP Extend Code Support</td>
<td>15</td>
<td>3</td>
<td>Indication whether the sender supports sending the VSNP Extend Code as defined in section 9.1.5. Valid values are 0 – Sender does not support VSNP Extend Code, 1 – Sender supports VSNP Extend Code. The absence of this configuration option implies that the VSNP Extend Code capability is not supported.</td>
</tr>
<tr>
<td>Compression Parameters</td>
<td>16</td>
<td>&gt;=4</td>
<td>This option indicates the protocol types supported by the sender. Allowed IP-Compression-protocol types are: o 0x0003 – ROHC over PPP. Coding of the specific parameters shall follow Robust Header Compression (ROHC) Option as defined in RFC 3241 [59], except for Type, Length and IP-Compression-Protocol fields. o Other values are reserved. This configuration option may only be included in a message if the VSNP Extend Code Support option is also included and set to the value 1. Multiple instances of this option may occur in the same message, but may not contain the same protocol type.</td>
</tr>
<tr>
<td>Default APN Indication</td>
<td>17</td>
<td>3</td>
<td>Valid values are: 0- “The requested APN is not the default APN” 1- “The requested APN is the default APN”</td>
</tr>
<tr>
<td>Reconnect Indication</td>
<td>18</td>
<td>3</td>
<td>This option indicates whether or not the UE is allowed to reconnect to the APN associated with the PDN connection being terminated. Valid values are: • 1 – Reconnect to this APN not allowed • All other values reserved</td>
</tr>
</tbody>
</table>
### Configuration Option Type (decimal) Configuration Option Length (octets) Value

| Mobile Identity | 19 | 3-11 | Value portion of the “Mobile Identity” IE as defined in Section 10.5.1.4 of [TS 24.008] [25]. The type of identity shall be set to ‘001’ (IMSI) or ‘010’ (IMEI). |

#### Table 5  Error Code values

<table>
<thead>
<tr>
<th>Value – General Description</th>
<th>Explanation of Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - General Error</td>
<td>Used when there is no other specific error code available to report the failure.</td>
</tr>
<tr>
<td>1 - Unauthorized APN</td>
<td>Requested APN is not authorized for this user.</td>
</tr>
<tr>
<td>2 - PDN Limit Exceeded</td>
<td>Number of PDN for this connection has exceeded the maximum allowed limit.</td>
</tr>
<tr>
<td>3 - No P-GW Available</td>
<td>No P-GW address available to establish the PDN connection.</td>
</tr>
<tr>
<td>4 - P-GW Unreachable</td>
<td>P-GW is not reachable or not responding.</td>
</tr>
<tr>
<td>5 - P-GW Reject</td>
<td>PDN connection attempt rejected by P-GW.</td>
</tr>
<tr>
<td>6 - Insufficient Parameters</td>
<td>Request does not have sufficient parameters to proceed.</td>
</tr>
<tr>
<td>7 - Resource Unavailable</td>
<td>HSGW does not have sufficient resource to proceed with the request.</td>
</tr>
<tr>
<td>8 - Admin Prohibited</td>
<td>PDN connection request is administratively prohibited at the HSGW.</td>
</tr>
<tr>
<td>9 - PDN-ID Already In Use</td>
<td>The PDN-ID received in a VSNCP Configure-Request is already in use for a PDN connection.</td>
</tr>
<tr>
<td>10 - Subscription Limitation</td>
<td>The “PDN Type” option received from the UE in a VSNCP Configure-Request does not indicate support for any IP address type allowed by the subscription data for the APN.</td>
</tr>
<tr>
<td>11 - PDN connection already exists for this APN</td>
<td>A PDN connection has previously been created for the APN specified in the VSNCP Configure-Request message.</td>
</tr>
<tr>
<td>12 - Emergency services not supported</td>
<td>This network does not support emergency services.</td>
</tr>
<tr>
<td>13 – Reconnect to this APN not allowed</td>
<td>Reconnect to this APN is not allowed.</td>
</tr>
</tbody>
</table>

#### Table 6  Address Allocation Cause values

<table>
<thead>
<tr>
<th>Value (decimal)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Null value – used on VSNCP Configure-Request sent by the UE to initiate attachment or handover.</td>
</tr>
<tr>
<td>255</td>
<td>Success.</td>
</tr>
<tr>
<td>xx</td>
<td>All values supported in TS 29.275 clause 12.1.1.3 [35].</td>
</tr>
</tbody>
</table>
### 9.1.4.1.1 Configuration Option Data Format

This section specifies the data format for the VSNCP Configuration Options specified in Table 4.

**Table 7 Configuration Option Data Format**

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Length</td>
<td>Configuration Option Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Option Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Type**: As specified in Table 4.
- **Length**: This field shall contain the length in octets for the VSNCP Configuration Option including the Type and Length fields.
- **Configuration Option Data**: As specified in Table 4.

### 9.1.4.2 3GPP2 VSNCP Configure-Request

The UE shall send this message to the HSGW to initiate a new PDN connection. When the UE sends this message, the following configuration options are mandatory.

- PDN Identifier (PDN-ID)
- Access Point Name (APN)
- PDN Type
- PDN Address
- Attach Type

The following additional configuration options are mandatory when the UE sends this message to setup multiple PDN connections with an APN.

- User Context Identifier

The PDN Address configuration option shall have a value 0, if the Attach Type is “Initial Attach”. If the Attach Type is “Handoff”, IP address(es) assigned for the PDN shall be set in the value field.

For default APN connection setup, if the default APN is not known to the UE, then the UE shall set the APN using a zero length APN Network Identifier as the APN name (see TS 23.003 [19]). When the HSGW receives a VSNCP Configure-Request message indicating a zero length APN, then the HSGW shall set the APN in the PBU message to the default APN value that is contained in the subscription data for the user, unless the HSGW also receives the Emergency Indicator configuration option with the value set to 1. If the HSGW receives a VSNCP Configure-Request message with the Emergency Indicator configuration option with the value set to 1, then the HSGW shall set the APN in the PBU message to the emergency APN value contained in the HSGW Emergency Configuration Data, and the APN supplied in the VSNCP Configure-Request is ignored by the HSGW.
A UE shall indicate its supported bearer control mode capabilities in the PCO of the VSNCP Configure-Request message when it attaches to an APN; see TS 24.008 [24]. The HSGW forwards the BCM value to the PCRF along with the HSGW capabilities, and the PCRF decides what BCM will be used, i.e., “MS-only”, or “MS/NW”, based on the capabilities of the UE and the HSGW. The HSGW shall indicate the result in the VSNCP Configure-Ack message. The UE shall use the BCM value returned to it.

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 (TS 24.008 [24]) of the PCO option, when sent in the 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 in the additional parameter list (TS 24.008 [24]) of the PCO option, when sent in the VSNCP Configure-Request message from the UE to the HSGW. In addition the UE may also include other parameters defined in the Protocol Configuration Options (TS 24.008 [24]), for example, username and password for authentication with an external AAA server may be included.

If the PDN Type is IPv4 or IPv4v6, the UE shall include the IPv4 Default Router Address Configuration Option. If the Attach Type is Initial, the value shall be set to 0.0.0.0. If the Attach Type is Handoff and the UE has the currently assigned IPv4 default router address, the value shall be set to the IPv4 address currently assigned as the IPv4 default router address. If the Attach Type is Handoff and the UE does not have the currently assigned IPv4 default router address, the IPv4 default router address shall be set to 0.0.0.0. If the PDN Type is IPv6 or IPv4v6, and if the Attach Type option is “Handoff”, and if the UE is operating in the tunneled mode, then the UE shall include the IPv6 HSGW Link Local Address IID option and shall set the value to all zeros.

The HSGW sets the Handoff Indicator value in the PBU message as follows:

In all cases of re-registration, the HSGW shall set the Handoff Indicator to 5, otherwise:

- If the Attach Type received from the UE is “Initial Attach”, the HSGW shall set the Handoff Indicator to 1.
- If Attach Type received from the UE is “handover” and if context transfer occurs for the UE using the H1 interface, the serving HSGW shall set the Handoff Indicator to 3.
- If Attach Type received from the UE is “handover” and if context transfer does not occur using the H1 interface, the serving HSGW shall set the Handoff Indicator to either 2 or 3.

If the UE is creating this PDN connection to access emergency services, then the UE shall include the Emergency Indicator configuration option with the value set to 1. In addition, the UE shall also include Mobile Identity configuration option in the VSNCP Configure Request message. If the UE is not creating this PDN connection to access emergency services, then the UE may include the Emergency Indicator configuration option with the value set to 0.

If the UE wants to use the VSNP Extend Code capability in the reverse link, it shall include the VSNP Extend Code Support configuration option in the VSNCP Configure-Request with the data field set to 0x01.

If the UE includes the VSNP Extend Code Support option, the UE may include an instance of the Compression Parameters option for each compression protocol type it wants to use in the reverse link.
During PDN connection setup, the HSGW shall send this message to the UE. The HSGW shall send VSNCP Configure-Request only after receiving VSNCP Configure-Request from the UE. When the HSGW sends this message, the following configuration options are mandatory.

PDN Identifier (This value is copied from the corresponding VSNCP Configure-Request from the UE.)

If the HSGW supports Default APN Configuration option, and if the PDN connection requested by the UE corresponds to the default APN, then the HSGW shall include the Default APN Configuration option in the VSNCP Configure-Request message sent by the HSGW with the value set to ‘1’.

If the UE had included User Context Identifier configuration option in the VSNCP Configure-Request message, and if the HSGW had accepted the User Context Identifier configuration option sent by the UE, the following additional fields are mandatory when the HSGW sends VSNCP Configure-Request message to the UE

User Context Identifier (This value is copied from the corresponding VSNCP Configure-Request from the UE.)

If the HSGW supports emergency services, then the HSGW shall include the Emergency Service Support Indicator configuration option with the value set to 1. If the HSGW does not support emergency services, then the HSGW shall either not include the Emergency Service Support Indicator configuration option, or shall include the Emergency Service Support Indicator configuration option with the value set to 0.

If the HSGW wants to use the VSNP Extend Code capability in the forward link, it shall include the VSNP Extend Code Support configuration option in the VSNCP Configure-Request with the data field set to 0x01.

If the HSGW includes the VSNP Extend Code Support option, the HSGW may include an instance of the Compression Parameters option for each compression protocol type it wants to use in the forward link.

The UE/HSGW shall ignore unrecognized configuration options present in the VSNCP Configure-Request. The VSNCP Configure-Reject message shall not be sent for such requests, if the UE/HSGW can proceed with the PDN connection attempt with available configuration options in the request. The UE/HSGW shall not include those unrecognized parameters in the VSNCP Configure-Ack message sent in response to the VSNCP Configure-Request. The configuration options that are sent by the UE/HSGW in the VSNCP Configure-Request and not received back in the VSNCP Configure-Ack shall be considered not supported by the other side.

If the HSGW or the UE wants to change any values in the configuration options that are received in VSNCP Configure-Request, then the HSGW or UE shall send VSNCP Configure-Ack with the modified value in the configuration option.

Note: In this version of this specification, there are no configuration options that the UE is allowed to change.
9.1.4.3 3GPP2 VSNCP Configure-Ack

The HSGW uses this message to respond to a VSNCP Configure-Request message from the UE, if the PDN connection attempt is successful. The HSGW shall include all acceptable configuration options present in the corresponding VSNCP Configure-Request message in the VSNCP Configure-Ack message. The "PDN Address" option shall be included and shall contain the IPv4 address (if the UE indicated that it wants to obtain the IPv4 address during PDN connection setup procedures) and/or IPv6 IID assigned to the UE for the PDN by P-GW. For the case where the UE requested and was granted deferred IP address allocation the IPv4 address field shall be set to 0.0.0.0. The UE shall use the IPv6 prefix received in the Router Advertisement to create an IPv6 address per clause 4.7.1 in TS 23.402 [23].

If the HSGW successfully connects to the default APN, it shall include the APN name of the default APN in the Access Point Name configuration option, unless the HSGW also receives the Emergency Indicator configuration option with the value set to 1. If the HSGW receives a VSNCP Configure-Request message with the Emergency Indicator configuration option with the value set to 1, then the HSGW shall set the APN configuration option in the VSNCP Configure-Ack to the null APN. If the HSGW successfully connects to the emergency APN, then the HSGW shall include the Emergency Indicator configuration option with the value set to 1 in the VSNCP-Configure-Ack message.

If the UE included the VSNP Extend Code Support option in the VSNCP Configure-Request, and if the HSGW accepts the use of VSNP Extend Code in the reverse link, then the HSGW shall include the VSNP Extend Code Support option in the VSNCP Configure-Ack message with the data field of the option set to 1. Otherwise the HSGW shall either not include the VSNP Extend Code configuration option in the VSNCP Configure-Ack message, or shall include the VSNP Extend Code configuration option in the VSNCP Configure-Ack message with the value set to 0.

If the UE included one or more instances of the Compression Parameters option in the VSNCP Configure-Request for the reverse link, and if the HSGW supports compression on the reverse link, then the HSGW shall include corresponding instances of the Compression Parameters option for all compression types that it accepts for the reverse link in the VSNCP Configure-Ack message. Otherwise, the HSGW shall not include the Compression Parameters configuration option in the VSNCP Configure-Ack message.

If the UE included the IPv4 Default Router Address Configuration Option in the VSNCP Configure-Request message and if deferred IPv4 address allocation is used, the HSGW shall set the value of the IPv4 Default Router Address Configuration Option to 0.0.0.0. If the P-GW returned an IPv4 default router address, the HSGW shall set the value of the IPv4 Default Router Address Configuration Option to the returned address.

If the UE included the IPv4 Default Router Address Configuration Option set to 0.0.0.0 in the VSNCP Configure-Request message with Attach Type = Handover and the UE is performing pre-registration over the S101 tunnel, the HSGW shall set the value of the IPv4 Default Router Address Configuration Option to the pre-configured value in the HSGW.

If the UE included the IPv6 HSGW Link Local Address IID option and if the Attach Type option is “Handoff", and if the Tunnel Mode Indicator is set to 1 in the last received A11-Registration Request message for the UE, then the HSGW shall include the IPv6 HSGW Link Local Address IID option in the VSNCP Configure-Ack message and shall set the value to the interface ID of the HSGW link local address.
If the UE included the User Context Identifier configuration option in the VSNCP Configure-
Request, and if the network supports MUPSAP, then the HSGW shall include the User
Context Identifier configuration option in the VSNCP Configure-Ack message. Otherwise the
HSGW shall not include User Context Identifier configuration option in the VSNCP
Configure-Ack message.

The HSGW shall fill in the requested parameters in the VSNCP Configure-Ack message
based on the PBA message received from the P-GW. The HSGW shall indicate the bearer
control mode selected by the PCRF using the Selected Bearer Control Mode in the PCO
option only if the UE included the MS Support of Network Requested Bearer Control
indicator in the PCO option in the corresponding VSNCP Configure-Request message.

Since the HSGW does not send a PBU message to the P-GW during pre-registration
procedures over S101, if the HSGW receives a VSNCP Configure-Request message from the
UE over the S101 interface with the ‘Attach Type’ set to ‘Handoff’, the HSGW shall include
in the VSNCP Configure-Ack message parameters based on the communication with the
PCRF and based on local configuration. Upon receiving the VSNCP Configure-Ack
message, the UE shall only update parameters for which new values are received and keep
other parameters unchanged.

If the HSGW included the VSNP Extend Code Support option in the VSNCP Configure-
Request, and if the UE accepts the use of VSNP Extend Code in the forward link, then the UE
shall include the VSNP Extend Code Support option in the VSNCP Configure-Ack message
with the data field of the option set to 1.

If the HSGW included one or more instances of the Compression Parameters option in the
VSNCP Configure-Request for the forward link, and if the UE supports compression on the
forward link, then the UE shall include corresponding instances of the Compression
Parameters option for all compression types that it accepts for the forward link in the VSNCP
Configure-Ack message. Otherwise, the UE shall not include the Compression Parameters
configuration option in the VSNCP Configure-Ack message.

The UE/HSGW shall validate the Configuration Option values received in the VSNCP
Configure-Ack message. If the UE/HSGW finds the values not acceptable for the PDN
connection, it may decide to terminate the PDN connection.

9.1.4.4 3GPP2 VSNCP Configure-Nak

To reduce the number of messages required for PDN connection setup, this message is not
used in the 3GPP2 VSNCP procedure. Neither the UE nor the HSGW shall send this message
to the other.

9.1.4.5 3GPP2 VSNCP Configure-Reject

The HSGW shall use this message to respond to a PDN connection request from the UE if the
PDN connection establishment is unsuccessful, unacceptable configuration options are
included in the VSNCP Configure-Request, or the requested PDN is not authorized in the
UE’s subscription profile. The UE shall use this message to respond to a VSNCP Configure-
Request from the HSGW if unacceptable Configuration Options are included in the VSNCP
Configure-Request. The Options field is filled with a PDN Identifier as the first configuration
option and the unacceptable configuration options from the VSNCP Configure-Request
message. Recognizable and acceptable configuration options are not included in the
construction of the VSNCP Configure-Reject message except for the PDN Identifier as the
first configuration option. The configuration options that are included shall not be reordered or modified in any way as specified in RFC 1661 [43]. In addition, the following parameter shall indicate the reason for the failure.

Error Code

The HSGW may use all error codes specified in Table 5. The UE may use error codes 0 and 6 as specified in Table 5.

If the UE receives a VSNCP-Configure-Reject with the error code set to “Reconnection to this PDN is not allowed” then the UE shall not send VSNCP Configure-Request for that APN until after its next power-cycle.

9.1.4.6 3GPP2 VSNCP Terminate-Request

The UE and the HSGW use this message to initiate explicit PDN Connection release. The following configuration options are mandatory. If, while processing a VSNCP Configure-Request, the HSGW receives a PBA message from the P-GW with a Status field value indicating failure to complete the request PDN attach, the HSGW shall send a VSNCP Configure-Reject to the UE.

PDN Identifier

User Context Identifier, if the PDN connection is a MUPSAP PDN Connection

If the HSGW receives a PBA message from the P-GW with a Status field value indicating failure to extend the lifetime of the PMIP tunnel for an existing PDN connection, the HSGW shall send a VSNCP Terminate-Request message to the UE for this PDN connection. Upon sending or receiving the VSNCP Terminate-Request message requesting release of a PDN connection, the HSGW shall trigger PMIPv6 procedures to release the binding, if the binding exists. The UE and the HSGW shall release all the resources including TFTs associated with the PDN matching the PDN-ID in the message when this message is sent or received.

If the HSGW receives a 3GPP2-Reconnect-Indication mobility option in a BRI, the HSGW shall include a Reconnect Indication configuration option in the corresponding VSNCP Terminate-Request it sends to the UE. The HSGW shall set the value in the Reconnect Indication configuration option to match the reconnect indication received in the 3GPP2-Reconnect-Indication mobility option.

The HSGW shall ignore a VSNCP Terminate-Request message received from a UE to terminate the PDN connection to an emergency PDN.

If the UE receives a VSNCP Terminate-Request with a Reconnect Indication Configuration Option set to “Reconnect to this APN not allowed” then the UE shall not send VSNCP Configure-Request for that APN until after its next power-cycle.

9.1.4.7 3GPP2 VSNCP Terminate-Ack

The UE and the HSGW shall use this message to respond to a VSNCP Terminate-Request message. The following configuration options are mandatory.

PDN Identifier
User Context Identifier, if the PDN connection is a MUPSUP PDN Connection

9.1.4.8 3GPP2 VSNCP Code-Reject

This message is used as specified in RFC 1661 [43]. The following configuration options are mandatory.

PDN Identifier
User Context Identifier, if the PDN connection is a MUPSUP PDN Connection

9.1.5 3GPP2 Vendor Specific Network Protocol (VSNP) Packet Format

User packets over the main service connection and other auxiliary service connections with PPP HDLC framing for a PDN session are encapsulated using Vendor Specific Network Protocol (VSNP) as defined in RFC 3772 [67].

The VSNP packet format without the VSNP extend code shall be supported as shown in Table 8.

<table>
<thead>
<tr>
<th>Table 8 3GPP2 VSNP packet format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol 0x05b as defined in RFC 3772 [67].</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDN Identifier PDN Identifier of the PDN for which the user data is sent. The high order 4 bits of this field shall be set to ‘0000’. The low order 4 bits of this field shall contain the PDN-ID.</td>
</tr>
<tr>
<td>Data IPv4 or IPv6 datagrams.</td>
</tr>
</tbody>
</table>

The VSNP packet format using the VSNP extend code is shown in Table 9. Support of this format is optional. The UE shall send packets using the format specified in Table 9, if the VSNP extend code is negotiated (see section 9.1.4) for the reverse link. The HSGW shall send packets using the format specified in Table 9, if the VSNP extend code is negotiated (see section 9.1.4) for the forward link.

<table>
<thead>
<tr>
<th>Table 9 3GPP2 VSNP extended packet format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

1 If PPP PFC is negotiated (ref. RFC 1661 [44]), then only the least significant octet (0x5b) is sent.
Protocol 0x005b as defined in RFC 3772 [67].
Extend Code This field shall be set to one of the values given in Table 10.

Table 10 3GPP2 VSNP Extend Codes and Data Field Contents

<table>
<thead>
<tr>
<th>Binary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘0000’</td>
<td>The Data field contains a full IPv4 or IPv6 packet.</td>
</tr>
<tr>
<td>‘0011’</td>
<td>ROHC small-CID (corresponds to IANA protocol type 0x0003).</td>
</tr>
<tr>
<td>All others</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

PDN-ID PDN Identifier of the PDN for which the user data is sent.
Data The contents of this field are defined in Table 10.

The format specified in Table 9 applies to both the main service connection (SO59) and auxiliary service connections using SO64.
9.1.6 RSVP Protocol

The following RSVP messages (see RFC 2205 [50]) shall be used between the UE and the HSGW to support QoS establishment:

1. Resv message
2. ResvConf message
3. ResvErr message.

RSVP messages shall be carried over the main service connection using the VSNP protocol (see section 9.1.5) by setting the Protocol field to 0x005b (see RFC 3772 [67]). RSVP Resv messages shall contain the TFT Information Element that includes Packet Filter List and the QoS List (as required).

RSVP messages are associated with a PDN based upon the PDN Identifier contained in the VSNP header. In addition, the upper 4 bits of the Flow Identifier in this document form a field that identifies the PDN-ID. This convention does not apply for the Flow-IDs 0xFF and 0xFE flows which are defined in detail in C.S0087 [15].

When generating a new Transaction ID value to be used in an RSVP message, the HSGW shall set the most significant bit of this field to ‘1’. When generating a new Transaction ID value, the UE shall set the most significant bit of this field to ‘0’.

All the RSVP messages used in this specification are sent over UDP with the Protocol ID of 17 with registered port number of 3455. All the messages (i.e., Resv, ResvErr, and ResvConf) shall be sent using the destination port of 3455 by both the HSGW and the UE. All the source port numbers may be set to any value.

For IPv6, the UE shall send the RSVP message to the Link Local IPv6 address of the HSGW and the HSGW shall send the RSVP message to the Link Local IPv6 address of the UE. The Link Local IPv6 address of the HSGW is the source address of the Router Advertisement message sent by the HSGWs (MAGs). The Link Local Address of the HSGW is set by the P-GW and does not change while the PDN connection is established, as per section 6.8 and 9.3 of RFC 5213 [78].

For IPv4, the UE shall use the IPv4 default router address obtained during the PDN connection setup as the destination address of the RSVP packets for that PDN. The HSGW sends the RSVP packets to the IPv4 address of the UE. The IPv4 default router address is set by the P-GW in the IPv4 Default-Router Address Option in the corresponding PBA message for a given UE (see RFC 5213 [78]), and it does not change while the PDN connection is established. The HSGW shall set its address to the IPv4 default router address received in the PBA message.

A UE that receives both an IPv4 address and an IPv6 address for a given PDN may choose either the IPv4 default router address or the Link Local IPv6 address of the HSGW as the destination address for RSVP signaling.
9.1.6.1 Requirements for QoS Updates

9.1.6.1.1 HSGW Requirements

During an inter-HSGW handoff with context transfer, if the QoS policy received from the SHSGW during the context transfer does not match with the QoS policy obtained from the PCRF, and if the selected Bearer Control Mode is “MS/NW”, then the T-HSGW shall perform the network initiated QoS setup procedures to update the QoS flows for unmatched flows based on the QoS policy received from the PCRF.

After a successful PPP renegotiation, if the selected Bearer Control Mode is “MS/NW”, then the HSGW shall perform the network initiated QoS setup procedures to setup the QoS flows for all the established flows based on the QoS policy received from the PCRF.

During handoff from E-UTRAN to eHRPD, including pre-registration, if the selected Bearer Control Mode is “MS/NW”, then the HSGW shall perform the network initiated QoS setup procedures to establish QoS flows based on the QoS policy received from the PCRF using the network initiated the QoS setup procedure described in section 9.1.6.3.

9.1.6.1.2 UE Requirements

Upon a successful PPP renegotiation, if the selected Bearer Control Mode is set to ‘MS only mode’, then the UE shall setup the QoS for all the flows that were active prior to the PPP renegotiation and the UE wishes to maintain as active.

During handoff from E-UTRAN to eHRPD, including pre-registration, if the selected Bearer Control Mode is set to “MS only mode”, then the UE should establish the QoS for all the flows are established on E-UTRAN using UE initiated the QoS setup procedure described in section 9.1.6.2.

9.1.6.2 UE Initiated QoS with PCC

To support the UE initiated QoS with PCC, the HSGW and UE shall perform the following procedures.

The UE shall send a Resv message to the HSGW containing the requested QoS List and associated packet filters with the Operation Code set to QoS-Check in the TFT. If the HSGW can not parse the TFT for any reason, e.g., poorly formatted TFT, invalid PDN-ID, or an unauthorized IPv4 address/IPv6 Prefix is included in the TFT, the HSGW shall send a ResvErr message as specified in Chapter 4 B.3 in X.S0011 [6].

If the UE receives a ResvErr message (ref. section 9.1.6.6) from the HSGW with the error code set to “NW initiated QoS in progress for all the flows”, then the UE shall wait for the Network to set up the QoS for all the flows in the TFT. If the UE receives a ResvErr message from the HSGW with the error code set to a value other than “NW initiated QoS in progress for all the flows”, then the UE shall assume that processing of all requested IE Data contained in the 3GPP2 Object was unsuccessful. When the ‘X’ bit in the TFT Error IE is set, it indicates the inclusion of index of the Flow Identifier that caused the failure.

If the Resv message received from the UE is valid, for each IP flow included in the Resv message the HSGW shall convert the FlowProfileID(s) to a single set of 3GPP QoS
parameters and perform authorization of the requested QoS per TS 29.212 [29]. If there are multiple FlowProfileIDs sent by the UE, the HSGW shall consider the first in the list as the one most preferred by the UE. If the network is setting up the QoS for all the flows in the TFT that the UE is requesting to setup, then the HSGW shall send a ResvErr message (ref. section 9.1.6.6) with the error code set to ‘NW initiated QoS in progress for all the flows’.

Once the HSGW has received authorization for the QoS per the PCC mechanisms, it shall respond to the UE request by sending a ResvConf message using the same Transaction ID as received in the Resv message, and the Operation Code set to QoS-Check Confirm. The ResvConf message shall include a set (one or more) of authorized FlowProfileIDs (based on operator determined charging rules, etc.) and associated packet filters for each authorized Flow Identifier in the QoS list. The authorized FlowProfileIDs in the QoS List shall be the same or a subset of the FlowProfileIDs in the Resv message sent by the UE. If UE Initiated QoS for the flow is not authorized, the HSGW shall set the R_QoS_SUB_BLOB_LEN for that Flow Identifier to zero and shall set the Result Code to the value “UE Initiated QoS is not authorized”. If the network decides to modify the evaluation precedence value of one or more packet filters that are sent by the UE in the Resv message with the Operation Code set to “QoS Check”, then the HSGW shall include those packet filters with the modified evaluation precedence values in the ResvConf message with the Operation Code set to “QoS Check Confirm”. In the ResvConf message with the Operation Code set to “QoS Check Confirm”, the HSGW should not modify the packet filters that were requested by the UE in the Resv message with the Operation Code set to “QoS Check”\(^1\). If the network is setting up the QoS for a flow in the TFT that the UE is also requesting to setup, then the HSGW shall set the R_QoS_SUB_BLOB_LEN for that Flow Identifier to zero and shall set the Result Code to the value “NW initiated QoS in progress for this flow”. The UE shall not include this flow in the subsequent Resv message.

The UE may send the Resv message a configurable number of times until a ResvConf or ResvErr message is received from the HSGW with the same Transaction ID, or until expiry of a configurable timer. The Resv and ResvConf message format is the same as the Resv and ResvConf message formats specified in Annex B in X.S0011 [6] except for 3GPP2 Object as specified in this section.

Upon receiving the ResvConf message from the HSGW, for each Flow Identifier that has a non-empty FlowProfileID list associated with it, the UE shall use the authorized FLOW_PRIORITY, associated packet filters and FlowProfileID list to start UE initiated QoS procedures as specified in C.S0063 [13]. The UE shall then set up the TFTs as specified in Annex B in X.S0011 [6] using the same Flow ID(s) with the modified evaluation precedence in QoS-Check procedures and a different Transaction ID on the Resv message.

After the TFT has been created, if the QoS list and/or associated packet filters are to be modified (i.e., add or replace), then the UE shall send a Resv message to the HSGW containing the modified QoS list and associated packet filters with the Operation Code set to QoS-Check in the TFT. After the QoS-Check procedure is successfully completed, the UE shall modify the TFTs as specified in Annex B in X.S0011 [6] using the same Flow ID(s) used in the QoS-Check procedures and a different Transaction ID on the Resv message. For each Flow ID that has been modified with a different FlowProfileID(s), the UE shall request modification by the eAN with the new FlowProfileID(s) as specified in C.S0063 [13].

\(^1\) E-UTRAN allows the network to modify the requested packet filters; however, such modification of packet filters is not supported in this version of this specification.
9.1.6.3 Network Initiated QoS with PCC

For network initiated QoS setup, the RSVP Resv messages are sent from the HSGW to the UE. The destination address of the RSVP Resv signaling messages sent from the HSGW is the address of the UE. This specification does not require the HSGW to send or receive the PATH message. The HSGW shall be able to send Resv messages without receiving a corresponding PATH message from the UE.

For Network Initiated QoS, three types of operations are supported:

1. Initiate flow request with QoS specified.

2. Initiate the deletion of ‘all’ packet filters for TFTs specified in the list of flow identifiers.

3. Initiate the modifications of packet filters/QoS for TFTs specified in the list of flow identifiers.

For network initiated flow request, the HSGW shall send an RSVP Resv message with the ‘Initiate Flow Request’ operation code to the UE. Upon successfully receiving such a Resv message the UE shall respond with a Resv message with the same Transaction ID and same packet filters as received from the HSGW and set the operation code to ‘Add packet filters to existing TFT’ if the TFT already exists; otherwise the UE shall send ‘Create New TFT’, as specified in X.S0011 [6]. For successful operation, the HSGW shall respond with a ResvConf message.

For network initiated delete of all packet filters, the HSGW shall send an RSVP Resv message with ‘Initiate Delete Packet Filters from Existing TFT’ operation code to the UE. Upon successfully receiving such a Resv message the UE shall respond with a Resv message with the same Transaction ID and operation code set to ‘Delete Packet Filters from Existing TFT’, as specified in X.S0011 [6]. For successful operation, the HSGW shall respond with a ResvConf message.

For network initiated modifications of packet filters/QoS, the HSGW shall send ‘Initiate Replace packet filters in existing TFT’ operation code to the UE. Upon successfully receiving such a Resv message the UE shall respond with a Resv message with the same Transaction ID and same packet filters as received form the HSGW and set operation code to ‘Replace packet filters in existing TFT’, as specified in X.S0011 [6]. For successful operation, the HSGW shall respond with a ResvConf message.

For network initiated flow request or network modifications of packet filters/QoS, if the UE supports one or more FlowProfileIDs associated with a Flow Identifier, the UE shall include the Flow Identifier and associated packet filters in the Resv message. The UE may use a subset of QoS FlowProfileIDs specified in the QoS list to request QoS Setup or modifications.

Upon receiving a Resv message from the HSGW, if the UE can not parse the TFT for any reason, e.g., poorly formatted TFT, or if the HSGW includes an invalid IPv4 address/IPv6 Prefix in the TFT, or if the UE supports none of QoS FlowProfileIDs specified in the QoS List (if included) the UE shall send a ResvErr message.

If the HSGW receives a ResvErr message from the UE, the HSGW shall assume that processing of all requested IE Data contained in the 3GPP2 Object was unsuccessful. When
the ‘X’ bit in the TFT Error IE is set, it indicates inclusion of the index of the Flow Identifier that caused the failure.

Error handling of the Resv messages by the UE and the HSGW is as specified for other operation codes in this specification.

The HSGW may send the Resv message a configurable number of times until a Resv message or ResvErr message is received from the UE with the same Transaction ID, or until expiry of a configurable timer. Upon receiving the Resv message from the UE, the HSGW shall send either a ResvConf or a ResvErr message to the UE.

9.1.6.4 Resv Message

Resv message is specified in Annex B.1 of X.S0011-004 [6]. The 3GPP2 OBJECT in Resv messages sent from the HSGW to the UE for network initiated QoS and from the UE to the HSGW for UE initiated QoS-Check operation is specified in the section 9.1.6.7.1.

9.1.6.5 ResvConf Message

The format of the ResvConf Message shall follow Annex B.2 of X.S0011-004 [6] except for the UE initiated QoS-Check operation. The format of the ResvConf Message for the UE initiated QoS containing the QoS-Check Confirm operation code shall be the same as the Resv Message. The 3GPP2 OBJECT in ResvConf messages sent from the HSGW to the UE for UE initiated QoS-Check confirm operation is specified in the section 9.1.6.7.1.
9.1.6.6 ResvErr Message

ResvErr message is specified in Annex B.3 of X.S0011-004 [6].

The TFT Error Code values defined in Table 11 shall be supported in addition to those defined in Annex B.3 of X.S0011-004 [6].

<table>
<thead>
<tr>
<th>TFT Error Code</th>
<th>Description</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000000</td>
<td>Unsuccessful TFT processing</td>
<td>Sent from the UE to the HSGW in a ResvErr message for network initiated QoS to indicate that the UE could not parse the TFT for any reason, e.g., poorly formatted TFT.</td>
</tr>
<tr>
<td>10000001</td>
<td>Invalid IP address</td>
<td>Sent from the UE to the HSGW in a ResvErr message for network initiated QoS to indicate that the HSGW used an invalid UE IP address/prefix in a Resv message sent from the HSGW to the UE.</td>
</tr>
<tr>
<td>10000010</td>
<td>FlowProfileIDs not supported by the UE</td>
<td>Sent from the UE to the HSGW in a ResvErr message for network initiated QoS to indicate that the UE supports none of the FlowProfileIDs specified in the QoS list.</td>
</tr>
<tr>
<td>10000011</td>
<td>Invalid PDN-ID in TFT</td>
<td>A Flow-ID contained in an RSVP message indicates a PDN-ID that is different than the PDN-ID identified in the VSNP header used in delivery of the RSVP message. This code may be sent by either the UE or the HSGW.</td>
</tr>
<tr>
<td>10000100</td>
<td>QoS-Check procedure needs to be performed</td>
<td>Sent from the HSGW to the UE to indicate that the UE needs to perform the QoS-Check procedure for the QoS and associated Packet Filters(s).</td>
</tr>
<tr>
<td>10000101</td>
<td>NW initiated QoS in progress for all the flows</td>
<td>Sent from the HSGW to the UE to indicate that the Network is setting up the QoS for the flows that the UE is trying to setup.</td>
</tr>
<tr>
<td>10000110</td>
<td>Evaluation precedence contention for NW initiated QoS</td>
<td>Sent from the UE to the HSGW in a ResvErr message for network initiated QoS to indicate Contention in the evaluation precedence.</td>
</tr>
</tbody>
</table>
9.1.6.7 Reliable Delivery of RSVP Messages

The HSGW and UE shall follow the requirements of X.S0011 for reliable delivery of RSVP messages. In addition, the HSGW shall include the RESV_CONFIRM object in the Resv message and send it to the UE. The HSGW may send the Resv message a configurable number of times until a Resv message is received from the UE with the same Transaction ID. If the HSGW retransmits the Resv message, the HSGW shall use the same Transaction ID.

9.1.6.7.1 3GPP2 OBJECT

The 3GPP2 OBJECT shall appear in Resv messages sent between the HSGW and the UE and shall appear in ResvConf messages sent from the HSGW to the UE for the QoS-Check confirm operation. The 3GPP2 OBJECT shall contain the following information element:

TFT

The HSGW or UE shall include at least one TFT Information Elements (IE) into the 3GPP2 OBJECT; the IEs may be repeated. The 3GPP2 OBJECT shall be formatted per the IANA assigned numbering scheme. The format of the 3GPP2 OBJECT is shown in Table 12:

<table>
<thead>
<tr>
<th>Table 12 3GPP2 OBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1</td>
</tr>
<tr>
<td>Length 3GPP2 Class C-Type</td>
</tr>
<tr>
<td>Transaction ID</td>
</tr>
<tr>
<td>IE List</td>
</tr>
<tr>
<td>Padding as necessary</td>
</tr>
</tbody>
</table>

Length: Length of the 3GPP2 OBJECT includes all octets, including the Length field. Length in octets and shall always be a multiple of 4 octets.

3GPP2 Class: 231

C-Type: 1

Transaction ID: This field shall be set in Resv messages to a 32 bit unique number which is used for matching a Resv message with the response (i.e., Resv message, ResvConf message, or ResvErr message).

This field shall be set in Resv, ResvConf and ResvErr messages to the same value that was received in the Resv message for which the Resv, ResvConf or ResvErr message is a response.
IE List: IE List shall include one or more IEs. The format of an IE List is as follows.

Table 13 3GPP2 OBJECT- IE List

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Length</th>
<th>IE Type #</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE Data</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IE Data</th>
<th>Padding</th>
</tr>
</thead>
</table>

Length: Length is the length in octets of the IE Data (including the length and IE Type fields), and shall always be a multiple of two octets.

IE Type #: A number used to identify the Information Element.

Table 14 3GPP2 OBJECT- IE Type #

<table>
<thead>
<tr>
<th>IE Type #</th>
<th>IE Type# value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTIPv4</td>
<td>0</td>
</tr>
<tr>
<td>TFTIPv6</td>
<td>2</td>
</tr>
</tbody>
</table>

IE Data: This field is specified in section 9.1.6.7.1.1. Only one IE Data shall be included in each IE.
9.1.6.7.1.1 Traffic Flow Template (TFT, IE Type # 0 and 2)

The HSGW shall set the value of the IP address (Destination IP address/Prefix if the D field is
set to ‘00’ or the source IP address/Prefix if the D field is set to ‘01’) in the packet filter list to
be the same as the value of UE IPv4 address field or the UE IPv6 address field if the UE’s IP
address/prefix is included in the packet filter list. When comparing IPv6 addresses, only the
prefix shall be compared.

The IE Data field is sent in the Resv message (for network initiated QoS or for the UE
initiated QoS-Check operation) or the ResvConf message (for the UE initiated QoS-Check
confirm operation) and has the following format:

<table>
<thead>
<tr>
<th>Table 15</th>
<th>TFT IPv4 IE Type# = 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1</td>
<td>1 2 3 4 5 6 7 8 9 0 1</td>
</tr>
<tr>
<td>D</td>
<td>Reserved</td>
</tr>
<tr>
<td>Packet filter list</td>
<td>QoS List</td>
</tr>
<tr>
<td>Number of packet filters with modified precedence</td>
<td>Packet filter list with modified precedence</td>
</tr>
<tr>
<td>Packet filter list with modified precedence</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 16</th>
<th>TFT IPv6 IE Type# = 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1</td>
<td>1 2 3 4 5 6 7 8 9 0 1</td>
</tr>
<tr>
<td>D</td>
<td>Reserved</td>
</tr>
<tr>
<td>Packet filter list</td>
<td>QoS List</td>
</tr>
<tr>
<td>Number of packet filters with modified precedence</td>
<td>Packet filter list with modified precedence</td>
</tr>
<tr>
<td>Packet filter list with modified precedence</td>
<td></td>
</tr>
</tbody>
</table>

The TFT is coded with the following fields. When the HSGW includes a TFT in a ResvConf
message in response to a UE initiated QoS-Check procedure, the HSGW shall set each field in
the TFT to be the same as the UE requested in the Resv message except for the TFT
Operation Code field which is set to the value “QoS-Check Confirm” and number of packet
filters is set to ‘0’. The Result Code field (in QoS List) shall be present only in the ResvConf message that has the TFT Operation Code field set to the value “QoS-Check Confirm”.

UE IP Address: The UE IP address is used to identify the TFT. For IE Type \# = 0, the UE IP address applies to IPv4, and for IE Type \# = 2, the UE IP address applies to IPv6. Specifically, this field shall be set as follows:

- For IPv4, it shall be set to the UE’s IPv4 address.
- For IPv6, the 64 most significant bits shall be set to the UE’s prefix and the 64 least significant bits shall be set to all zeros.

D: This field shall be set as follows:

- ‘00’ if this TFT is sent for the Forward Direction
- ‘01’ if this TFT is sent for the Reverse Direction
- ‘10’ and ‘11’ are reserved values.

NS: The Non-Specific bit. This bit indicates the type of FLOW ID-to-A10 connection mapping requested for the associated TFT. When set, it indicates that the FLOW ID-to-A10 connection mapping shall be indicated by the RAN in A11 signaling. For eHRPD, the NS bit shall always be set to ‘1’.

SR_ID: When the NS bit is set to ‘1’, the SR_ID field shall be set to ‘000’. This is always the case for eHRPD.

P: The P (Persistency) bit is set to ‘1’ to indicate that the HSGW will keep the TFT even if the A10 connection is not established or disconnected at the HSGW or flow ID to A10 connection mapping information is not yet received at the HSGW from the RAN. For eHRPD this bit shall always be set to ‘1’.

TFT Operation Code: The TFT operation code indicates an operation to be performed. Table 17 indicates TFT Operation Codes that are used in addition to the TFT Operation Codes specified in X.S0011 [6].
Table 17  TFT OpCodes

<table>
<thead>
<tr>
<th>OpCode</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000110</td>
<td>QoS-Check</td>
<td>Sent from the UE to the HSGW in a Resv message for UE initiated QoS-Check operation. The UE checks with the HSGW on whether requested QoS is authorized by the network.</td>
</tr>
<tr>
<td>10000000</td>
<td>Initiate Flow Request</td>
<td>Sent from the HSGW to the UE in a Resv message for network initiated QoS. The HSGW requests the UE to initiate a new flow with QoS. The QoS values are specified by the FlowProfileIDs in the QoS List in the same Resv message. The flow ID included in the TFT shall have the upper 4-bits set to the PDN-ID and the lower 4-bits set to a unique temporary flow identifier associated with the Transaction ID. The UE shall replace the temporary flow identifier with a unique flow identifier in the remainder of the network initiated QoS procedure.</td>
</tr>
<tr>
<td>10000001</td>
<td>QoS-Check Confirm</td>
<td>Sent from the HSGW to the UE in ResvConf message for UE initiated QoS-Check confirm operation. The HSGW responds to the UE with the authorized QoS for the session.</td>
</tr>
<tr>
<td>10000010</td>
<td>Initiate Delete Packet Filter from Existing TFT</td>
<td>Sent from the HSGW to the UE to request that the UE initiate the procedure to delete all Packet Filters from the TFTs given by the list of Flow Identifiers included in the list.</td>
</tr>
<tr>
<td>10000011</td>
<td>Initiate Replace packet filters in existing TFT</td>
<td>Sent from the HSGW to the UE to request that the UE initiate procedure to replace packet filters from existing TFTs. The TFTs are identified in the list of flow identifiers included in this message.</td>
</tr>
</tbody>
</table>

Number of Packet Filters: The HSGW shall set this field to zero in the ResvConf message when the TFT Operation Code is “QoS-Check Confirm”. Otherwise, the field shall be set as defined in X.S0011-004 [6].

Packet Filter List: The packet filter list contains a variable number of packet filters. It shall be encoded same as defined in X.S0011-004 [6] except as defined below:

For “QoS-Check Confirm” operations, the packet filter list shall be empty.

For “Initiate Delete Packet Filter from Existing TFT”, the packet filter list shall contain a variable number of Flow Identifiers given in the number of packet filters field. In this case, the packet filter evaluation precedence, length, and contents are not included, only the Flow Identifiers are included. See Figure B-6, X.S0011-004 [6].

For “Initiate Flow request” and “Initiate Replace Packet Filters in Existing TFT” Replace Packet Filters in Existing TFT the packet filter list shall contain a variable number of Flow Identifiers, along with the packet filter contents. See Figure B-7, X.S0011-004 [6].
Flow Identifier in the packet filter list shall be set as follows:

Flow Identifier (8 bits):

The upper 4 bits of Flow Identifier shall include the PDN-ID. The lower 4 bits of Flow Identifier shall identify each reservation that is requested to be added or deleted.

For the TFT operation code set to “Initiate Flow Request”, the lower 4 bits of Flow Identifier shall be set to a unique temporary flow identifier associated with the Transaction ID. The UE shall replace the temporary flow identifier with a unique flow identifier in the remainder of the network initiated QoS procedure. The same FLOW_ID value may be used in the forward and reverse directions.

For the TFT operation code set to “Initiate Delete Packet Filter from Existing TFT” and “Initiate Replace Packet Filter in Existing TFT”, the lower 4 bits of Flow Identifier shall be set to the flow identifier associated with the flow for which packet filter are to be deleted or modified respectively.

QoS List: QoS List shall not be included in IE Data field for the “Initiate Delete Packet Filter from Existing TFT” operation code. QoS List shall only be included in IE Data field for the “QoS-Check”, “QoS-Check Confirm”, “Initiate Flow Request”, and “Initiate Replace Packet Filters in Existing TFT” operation codes.

The QoS List, if present, shall contain a variable number of Flow Identifiers and associated R_QOS_SUB_BLOB fields. Table 18 shows the format of the QoS List.

Table 18  QoS List Layout

<table>
<thead>
<tr>
<th>MSB</th>
<th>LSB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS List Length (MSB)</td>
<td>QoS List Length (LSB)</td>
</tr>
<tr>
<td>Flow Identifier 1</td>
<td>Flow Identifier 2</td>
</tr>
<tr>
<td>R_QOS_SUB_BLOB_LEN 1</td>
<td>R_QOS_SUB_BLOB_LEN 2</td>
</tr>
<tr>
<td>R_QOS_SUB_BLOB 1</td>
<td>R_QOS_SUB_BLOB 2</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Result Code 1</td>
<td>Result Code 2</td>
</tr>
<tr>
<td>Flow Identifier N</td>
<td>Flow Identifier N</td>
</tr>
<tr>
<td>R_QOS_SUB_BLOB_LEN N</td>
<td>R_QOS_SUB_BLOB N</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Result Code N</td>
<td>Result Code N</td>
</tr>
</tbody>
</table>
Each QoS List is of variable length and consists of the following fields:

**QoS List Length (16 bits):**

The QoS List Length field contains the binary coded representation of the length (in octets) of the QoS List. Its value includes the QoS List Length field and the QoS list contents.

**Flow Identifier (8 bits):**

The Flow Identifier field is used to identify each reservation to or from an UE and shall be unique within the UE across different reservations. The same Flow Identifier value may be used in the forward and reverse directions.

Flow Identifier shall be set as follows:

The upper 4 bits of Flow Identifier shall include the PDN-ID. The lower 4 bits of Flow Identifier shall identify each reservation that is requested to be added or deleted.

For the TFT operation code set to “QoS-Check”, the UE shall set the lower 4 bits of Flow Identifier to a flow identifier associated with the Transaction ID. In the resulting ResvConf message with operation “QoS-Check Confirm”, the HSGW shall return the same Flow Identifier value as received from the UE.

For TFT operation code set to “Initiate Flow Request”, the HSGW shall set the Flow Identifier to a unique temporary value associated with the Flow Identifier in the packet filter list. This temporary Flow Identifier shall be set to the same value as used in the Packet Filter List.

For TFT operation code set to “Initiate Replace Packet Filters in Existing TFT”, the HSGW shall set the Flow Identifier to the flow identifier associated with the flow for which packet filters are to be replaced. This Flow Identifier shall be set to the same value as used in the Packet Filter List.

**R_QoS_SUB_BLOB_LEN (1 octet):**

This field shall be set to the length, in octets, of the R_QoS_SUB_BLOB field.

**R_QoS_SUB_BLOB (multiple octets):**

This field shall be set according to Annex E.1 of X.S0011-004 [6]. The VERBOSE field shall be set to ‘0’. The FlowProfileIDs are listed in this parameter in descending order of precedence.

QoS_ATTRIBUTE_SET_ID shall not be set to ‘000000’. QoS_ATTRIBUTE_SET_IDs in the ResvConf message with operation code set to “QoS-Check Confirm” shall be set independently from the QoS_ATTRIBUTE_SET_IDs in the Resv message with the Operation Code set to “QoS Check”.

The HSGW shall set FLOW_PRIORITY based on local policy (e.g., persistent value).

**Result Code (1 octet):**

This field is only included in the ResvConf message when the TFT Operation Code field is set to “QoS-Check Confirm”, and is not present otherwise. The Result Code indicates whether the QoS list check
requested by the UE was successful. The result codes, descriptions and the reasons are described in Table 19.

Table 19  Result Code Values

<table>
<thead>
<tr>
<th>Result Code</th>
<th>Description</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>Successful</td>
<td>The HSGW uses this code if the HSGW includes one or more authorized FlowProfileIDs associated with the corresponding Flow Identifier.</td>
</tr>
<tr>
<td>00000001</td>
<td>UE Initiated QoS is not authorized</td>
<td>The HSGW includes this code if the value of R_QoS_SUB_BLOB_LEN field associated with the corresponding Flow Identifier is set to zero and the UE initiated QoS is not authorized. The UE may fall back to the best effort for the flow.</td>
</tr>
<tr>
<td>00000010</td>
<td>NW initiated QoS in progress for this flow</td>
<td>The Network is setting up the QoS for this flow that the UE is trying to setup.</td>
</tr>
<tr>
<td>00000011</td>
<td>Requested FlowProfileIDs failed mapping</td>
<td>The HSGW uses this code if none of the FlowProfileIDs sent by the UE maps to a valid QCI/MBR/GBR. Upon receipt of this error code, the UE may choose to resubmit the QoS request, e.g., using a different set of FlowProfileIDs.</td>
</tr>
<tr>
<td>Others</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

Number of packet filters with modified precedence:  If the network modifies the precedence value of one or more packet filters that are requested by the UE in the Resv message with the TFT Operation Code set to “QoS Check”, then the HSGW shall set this field to the number of packet filters that have a modified precedence in the ResvConf message when the TFT Operation Code is “QoS-Check Confirm”. Otherwise, the HSGW shall set this field to 0.

Packet filter list with modified precedence:  If the HSGW sends ResvConf message to the UE with the TFT Operation Code set to “QoS-Check Confirm”, then the HSGW shall include ‘Number of packet filters with modified precedence’ occurrences of this field. Except for the following parameter, this field shall be encoded the same as the packet filter defined in X.S0011-004 [6] for TFT create/add/modify operations.

Flow Identifier (8 bits):  The upper 4 bits of Flow Identifier shall include the PDN-ID. The lower 4 bits of Flow Identifier shall identify each reservation.

9.1.7  Always On Service in eHRPD

The HSGW shall support the Always On service for each PPP session in the eHRPD system. An Always On UE is a UE that uses Always On service.
9.1.7.1 UE Requirements - Always On Service

Always On UEs shall send the 3GPP2 vendor specific Version/Capability packet with the C4 bit of the MS capabilities set to ‘1’. The 3GPP2 vendor specific Version/Capability packet is specified in section 8 of X.S0011-002 [6].

9.1.7.2 HSGW Requirements - Always On Service

If the HSGW receives the 3GPP2 vendor specific Version/Capability packet with the C4 bit of the MS capabilities set to ‘1’, then the HSGW shall treat the UE as an Always On UE. The 3GPP2 vendor specific Version/Capability packet is specified in section 8 of X.S0011-002-D [6]. If the HSGW does not receive the 3GPP2 vendor specific Version/Capability packet, or if the C4 bit of the MS capabilities is set to ‘0’, then the HSGW shall treat the UE as a non-Always On UE.

The HSGW shall follow the procedures for PPP Link Maintenance as specified in section 9.1.8.

9.1.8 PPP Link Maintenance

This section specifies how the UE and the HSGW determine the status of the PPP link and maintain the PPP session when the UE is connected to the HSGW directly over the eHRPD air interface or indirectly via the S101 interface.

9.1.8.1 HSGW Requirements - PPP Link Maintenance

For each PPP session, the HSGW shall support a PPP inactivity timer. The HSGW shall not implement a PPP session timer.

The PPP inactivity timer is a 4-octet unsigned integer which is locally provisioned in the HSGW. The value of this timer represents the maximum number of consecutive seconds that a PPP session can remain idle before the HSGW starts performing the PPP link status determination.

The HSGW shall set the default value of 86,400 seconds (24 hours) for the PPP inactivity timer for all PPP sessions. The HSGW may set the PPP inactivity timer to a non default value.

After entering the LCP Opened state, the HSGW shall send the 3GPP2 vendor specific MAX PPP Inactivity Timer packet (see RFC 2153 [49]) to the UE over the main service connection. The format of the 3GPP2 vendor specific MAX PPP Inactivity Timer packet shall be as defined in section 3.2.1.10 of X.S0011-002 [6]. The MAX PPP Inactivity Timer value shall be equal to

\[
\text{[PPP inactivity timer} + \text{Echo\_Reply\_Timeout timer} \times (\text{Echo\_Request\_Retries} + 1)\text{]}\]

for the PPP session. If the HSGW has determined that the UE is an Always On UE, the HSGW should resend the MAX PPP Inactivity Timer packet a configurable number of times if no response from the UE is received. If the HSGW has determined that the UE is a non-Always On UE, the HSGW need not resend the MAX PPP Inactivity Timer packet.

If the HSGW determines that the value in the MAX PPP Inactivity Timer packet previously sent to the UE should be changed, the HSGW shall send a revised 3GPP2 vendor specific MAX PPP Inactivity Timer packet as described in the preceding paragraph.
If the PPP inactivity timer is not running, then the HSGW shall start the PPP inactivity timer for the PPP session upon entering the VSNCP Opened state for a PDN connection. While the PPP inactivity timer is running, if the HSGW sends or receives any packet to or from the UE, the HSGW shall reset the PPP inactivity timer to its full value.

If the PPP inactivity timer expires, the HSGW shall perform the following:

- If the HSGW has determined that the UE is an Always On UE, the HSGW shall perform the PPP Link Status Determination procedure as specified in section 9.1.8.3.

- If the HSGW has determined that the UE is a non-Always On UE, then the HSGW shall not perform the PPP Link Status Determination procedure. Instead, the HSGW shall perform the following:
  - If the HSGW received a MAX PPP Inactivity response packet from the UE, the HSGW shall perform context maintenance as described in section 9.1.9.
  - Otherwise, the HSGW shall release all context(s) and all A10/A11 resources associated with the UE.

### 9.1.8.2 UE Requirements - PPP Link Maintenance

An Always On UE shall support a MAX PPP Inactivity Timer. When an Always On UE receives the Max PPP Inactivity Timer packet from the HSGW, the UE shall perform the following:

- Send the MAX PPP Inactivity Timer response packet to the HSGW. The format of the MAX PPP Inactivity Timer response packet is defined in section 3.2.1.10 of X.S0011-002 [6].

- Set its MAX PPP Inactivity Timer to the value in the MAX PPP Inactivity Timer packet.

A non-Always On UE should support a MAX PPP Inactivity Timer. When a non-Always On UE receives the MAX PPP Inactivity Timer packet from the HSGW, if the UE supports a MAX PPP Inactivity Timer, the UE shall perform the following:

- Send the MAX PPP Inactivity Timer response packet to the HSGW. The format of the MAX PPP Inactivity Timer response packet is defined in section 3.2.1.10 in X.S0011-002 [6].

- Set its MAX PPP Inactivity Timer to the value in the MAX PPP Inactivity Timer packet.

If the MAX PPP Inactivity Timer is not running and if the UE supports Max PPP Inactivity Timer, then the UE shall start the MAX PPP Inactivity Timer for the PPP session upon entering the VSNCP Opened state for a PDN connection. While the MAX PPP Inactivity Timer is running, if the UE sends or receives an LCP Echo-Request or any other packet to or from the HSGW, the UE shall reset its MAX PPP Inactivity Timer to its full value.

Upon the expiry of MAX PPP Inactivity Timer, the UE shall release all the VSNCP contexts and maintain partial context (which includes the LCP, CCP, and authentication context).
9.1.8.3 PPP Link Status Determination

When the UE is connected to the HSGW over the eHRPD air interface, the PPP Link Status Determination procedure is performed over the eHRPD air interface. When the UE is connected to the HSGW using the S101 interface, the PPP Link Status Determination procedure is performed over the S101 interface.

Upon expiration of the PPP inactivity timer, the HSGW shall send an LCP Echo-Request message (see RFC 1661 [44]) over the main service connection, and start the Echo-Reply-Timeout timer for the PPP session. It shall also initialize the Echo-Request-Retries counter to a configurable integer value.

Upon receipt of an LCP Echo-Reply message, an LCP Code-Reject (see RFC 1661 [44]), or any other packet, the HSGW shall stop and reset the Echo-Reply-Timeout timer, reset the Echo-Request-Retries counter, and reset the PPP inactivity timer to its full value.

Upon expiration of the Echo-Reply-Timeout timer and if the Echo-Request-Retries counter value is greater than zero, the HSGW shall send an LCP Echo-Request message, decrement the Echo-Request-Retries counter by one, and start the Echo-Reply-Timeout timer. Upon expiration of the Echo-Reply-Timeout timer and when the Echo-Request-Retries counter value is equal to zero, the HSGW shall perform the following:

- If the HSGW has received a MAX PPP Inactivity Timer response packet from the UE, the HSGW shall perform context maintenance as described in section 9.1.9.
- Otherwise, the HSGW shall release all context(s) and all A10/A11 resources associated with the UE.

9.1.9 HSGW Requirements for UE Context Maintenance

The HSGW uses the UE Context Maintenance timer to track and maintain the UE partial context.

The HSGW shall implement a configurable UE Context Maintenance timer. The UE Context Maintenance timer is a 4-octet unsigned integer which is locally provisioned in the HSGW. The value of this timer represents the maximum number of consecutive seconds that a partial UE session context (which includes the LCP, CCP, authentication and A10 session context for a given UE) is maintained by the HSGW. The value 0 indicates that the UE Context Maintenance timer is not used and consequently the UE partial context is not maintained.

If the UE Context Maintenance timer has a value other than 0, and if any of the following conditions is met, the HSGW shall release all context(s) associated with the UE except for the LCP, CCP, A10/A11, and authentication contexts and the HSGW shall start the UE Context Maintenance timer:

- The HSGW receives a PMIPv6 Binding Revocation Indication (BRI) message from the P-GW with the Revocation Trigger field set to “Inter-MAG Handover-different Access Types” for the UE session.
- The HSGW determines that it cannot communicate with an Always On UE after PPP link status determination fails at the HSGW (see 9.1.8).

When the HSGW starts the UE Context Maintenance timer, it shall stop the PPP inactivity timer.
If the HSGW receives a request for one or more PDN Connection(s) from the UE (using VSNCP Configure-Request) directly over the eHRPD air interface or indirectly via the S101 interface and if the UE Context Maintenance timer is running, then the HSGW shall stop the UE Context Maintenance timer and re-start the PPP inactivity timer.

If the UE context maintenance timer expires or if the authentication context becomes invalid due to e.g., MSK lifetime expiration, the HSGW shall release all context(s) and all A10/A11 resources associated with the UE.

9.1.10 Version Indication

The UE and the HSGW should send the 3GPP2 vendor specific Version/Capability packet, as per X.S0011-002-D [6]. If the 3GPP2 vendor specific Version/Capability packet is not exchanged, then the UE and the HSGW shall assume the X.S0011 features and functions used in this specification operate according to X.S0011-D [6].

Note: In the future it may be necessary to introduce a way to refer to different versions of X.S0057 when new features are introduced in X.S0057 based on the same version of X.S0011.

9.1.11 Capability Indication

The UE and HSGW shall use the 3GPP2 vendor specific Version/Capability packet, as per X.S0011-002 [6] to indicate the capabilities listed in the table below. The 3GPP2 vendor specific Version/Capability packet is specified in section 8 of X.S0011-002 [6].

Table 20 and Table 21 are extensions of Table 8 and Table 9 of X.S0011 [6].

<table>
<thead>
<tr>
<th>Bit</th>
<th>MS Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C8</td>
<td>Stale PDN Handling</td>
<td>Set to 1 if MS supports Stale PDN Handling</td>
</tr>
<tr>
<td>C9</td>
<td>IPCP NAK Handling</td>
<td>Set to 1 if MS supports receipt of IPCP Configure-NAK in the PCO in a VSNCP Configure-Ack</td>
</tr>
<tr>
<td>C10 to C23</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit</th>
<th>PDSN Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C10</td>
<td>Stale PDN Handling</td>
<td>Set to 1 if PDSN supports Stale PDN Handling</td>
</tr>
<tr>
<td>C11 to C23</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

9.1.12 IPCP Handling

IPCP messages (ref. RFC 1332 [45]) are contained in the PCO element in VSNCP messages between the UE and the HSGW. The PCO is transferred to/from the Proxy Binding Update/Acknowledgement messages that are sent between the HSGW and the P-GW on the S2a interface.

To avoid two round-trip IPCP message exchanges, if the UE sets bit C9 (IPCP Nak Handling) in the MS Capabilities in the 3GPP2 vendor specific Version/Capability packet, the HSGW may not convert IPCP Configure-Nak messages to IPCP Configure-Ack messages for the UE.
Otherwise, the HSGW should convert the IPCP Configure-Nak to an IPCP Configure-Ack when, for example, a DNS address is included in the IPCP Configure-Nak.

9.2 Auxiliary Service Connections between the UE and the HSGW

In the evolved HRPD system multiple auxiliary service connections\(^1\) may be used for:

1. Distinguishing QoS characteristics of different IP flows.
2. Carrying BE traffic - In this case, BE traffic from all PDNs shall be multiplexed across that auxiliary service connection using PDN-Mux.
3. Separating non-BE traffic according to PDN domains.
4. Carrying multiplexed non-BE traffic over an SO64 service connection using VSNP.
5. Carrying multiplexed non-BE traffic over an SO72 service connection using PDN-Mux.
6. Carrying non-multiplexed non-BE traffic over an SO67 service connection.

In the reverse direction, IP flows are mapped by the UE onto the appropriate link flows for forwarding to the eAN. If a BE auxiliary service connection is established, the BE IP flows for all PDNs shall be combined onto the same link flow that is associated with the BE auxiliary service connection in the reverse direction, and will include a PDN identifier that identifies the PDN that is the final destination for the traffic. The PDN identifier is inserted by PDN-Mux that is served by the link flow that carries BE traffic. The PDN Mux is associated to the link flow by a successful negotiation of protocol ID 0x08 between a UE and an eAN. This default auxiliary A10 “best effort” service connection is signaled to the HSGW on an A11-Registration Request message indicating service option 72 (IP packet framing, PDN multiplexing). Similarly in the forward direction the HSGW shall combine BE traffic from all PDNs onto the BE auxiliary service connection, if one is established using a PDN identifier to identify the source PDN. Otherwise, if a BE auxiliary service connection is not established, the main service connection is used to carry BE traffic using the VSNP protocol.

The auxiliary service connections are illustrated in Figure 39.

\(^1\) In the legacy HRPD system multiple service connections between the PDSN and AT are established to satisfy the QoS characteristics of different IP flows.
Figure 39  Auxiliary service connections

Figure 39 provides an illustrative example of a UE connecting to three different PDNs. IP flows 1 and 2 are combined over a single link flow and separated by a PDN identifier header that indicates to which PDN each flow corresponds. IP flow #3 is shown as being mapped to a dedicated link flow which is associated by the HSGW with PDN-1. Similarly IP Flows #4 and #5 are associated with PDN-2 and PDN-3 respectively and are used for the transport of different grades of VoIP traffic.

9.2.1 PDN Identifier Description

A PDN identifier (PDN-ID) shall be a value selected by the UE and mapped to a packet data network to which the UE is attached. The association of the PDN-ID to the Packet Data Network (PDN) shall be indicated to the HSGW using the VSNCP Configure-Request message. The PDN-ID identifies the PDN in various subsequent operations. In particular, it identifies the associated PDN for IP packets that are multiplexed across a service connection. The PDN-ID is associated with an APN used by the UE.
9.3 Use of the VSNCP Protocol

9.3.1 UE Requested PDN Connectivity

The UE requested PDN connectivity procedure for eHRPD is depicted in Figure 40. The procedure allows the UE to request connectivity to a new PDN. The default bearer for the new PDN shall reuse the best effort service connection. The new PDN will also be assigned a new and unique PDN-ID by the UE. In this procedure, the UE is assumed to be in active mode via the eHRPD radio. Proxy Mobile IP is used on the PMIP-based S2a interface.

1. When the UE wants to establish connectivity to a PDN, it will send the VSNCP Configure-Request message (APN, PDN Address, PDN Type, Protocol Configuration Options, Attach Type, Address Allocation Cause, and IPv4 Default Router Address). The Address Allocation Preference (contained within the Protocol Configuration Options) indicates whether the UE wants to perform the IPv4 address allocation during the execution of the procedure and PDN Type indicates that the UE is capable of supporting IPv4 and IPv6. The HSGW verifies that the APN provided by UE is allowed by subscription. If the UE supports NW Requested Bearer Control, then the UE includes the ‘MS Support of Network Requested Bearer Control indicator’ parameter in the Protocol Configuration Options.

2. The HSGW triggers the procedures for UE requested PDN connectivity described in TS 23.402 Section 6.2.1-1 Steps 4-10 inclusive (ref. TS 23.402 [23]). This establishes the bindings at the new P-GW and it updates the PCRF with the indication of the new connection.

3. After the HSGW receives the indication of the completion of PMIPv6 procedures, it will send the VSNCP Configure-Ack (APN, PDN Address, PCO, PDN-ID, Attach Type, Address Allocation Cause, and IPv4 Default Router Address) message to the UE. The Protocol Configuration Options parameter...
indicates the Selected Bearer Control Mode only if the UE included the MS Support of Network Requested Bearer Control indicator (BCM) parameter in the corresponding VSNCP Configure-Request message.

4. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID configuration option. This message contains the APN-AMBR, if the APN-AMBR was received from the HSS/AAA.

5. The UE responds with a VSNCP Configure-Ack message. The UE includes APN-AMBR, if it received APN-AMBR in step 4, and if the UE supports APN-AMBR.

6. IPv4 address allocation may occur at this point using the procedure shown in section 4.4.5.2 steps 9-12 and section 4.4.5.3, steps 9-16, when the IPv4 address allocation is deferred.

7. IPv6 address allocation may occur at this point using the procedure shown in section 4.4.5.4 steps 9-11.

9.4 Non-Optimized E-UTRAN to eHRPD Handoff Requirements

If the UE is attached to one or more PDNs in E-UTRAN, and if the mobile performs a handoff to eHRPD, then the UE shall perform handoff attach for each of the PDN connections it is allowed to and chooses to attach to over the eHRPD air interface.

The requirements for re-establishing the QoS is specified in section 9.1.6.1.

9.5 Stale PDN Handling

The procedure for handling stale PDN connection(s) is specified in this section. The UE and HSGW shall follow the procedures specified in this section if the C8 bit of the MS capabilities and if the C10 bit of the PDSN capabilities of 3GPP2 Vendor Specific Version/Capability packet are set to ‘1’.

If the UE or HSGW receives a packet for a PDN connection that is not active, then the receiver discards the packet and shall send the 3GPP2 Vendor Specific Extension of LCP-Echo-Request packet with the information element identifier set to ‘00000001’ (Active VSNCP Context Identifiers) as specified in section 9.6. If, after sending the 3GPP2 Vendor Specific Extension of LCP Echo-Request packet, the receiver continues to receive packets for the same PDN connection, it may resend the 3GPP2 Vendor Specific Extension of LCP Echo-Request packet.

Upon receiving a 3GPP2 Vendor Specific Extension of LCP-Echo-Request packet with the information element identifier set to ‘00000001’ (Active VSNCP Context Identifiers) as specified in section 9.5, then the receiver shall do the following:

- Send LCP-Echo-Reply as specified in RFC 1661 [44].
- If the receiver has one or more active PDN connection(s) that is/are not included in the 3GPP2 Vendor Specific Extension of LCP Echo-Request packet with the information element identifier set to ‘00000001’ (Active VSNCP Context Identifiers), then the receiver shall release the corresponding VSNCP context.
- If the receiver does not have a PDN connection associated with one or more PDN Identifier(s) included in the 3GPP2 Vendor Specific Extension of LCP Echo-Request packet with the information element identifier set to ‘00000001’ (Active VSNCP Context Identifiers), then the receiver shall release the corresponding VSNCP context.
Context Identifiers), then the receiver shall send a 3GPP2 Vendor Specific Extension of the LCP-Echo-Request packet with the information element identifier set to '00000001' (Active VSNCP Context Identifiers), as specified in section 9.6.

If the UE has gone out of coverage for a period of time, then the UE may send a 3GPP2 Vendor Specific Extension of the LCP-Echo-Request packet with the information element identifier set to '00000001' (Active VSNCP Context Identifiers) after returning to service coverage.

9.6 3GPP2 Vendor Specific Extension for LCP Echo-Request packet

If the UE and HSGW both indicate support for 3GPP2 Vendor Specific Extension for LCP Echo-Request in the 3GPP2 vendor specific Version/Capability packet exchange, then the UE and the HSGW shall support the LCP Echo-Request packet using the packet format specified in RFC 1661 [45] with the additional vendor specific extension as defined in Table 22:

<table>
<thead>
<tr>
<th>Table 22  LCP Echo-Request packet format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Code</td>
</tr>
<tr>
<td>Magic-Number</td>
</tr>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

Code As defined in RFC 1661 [45].

Identifier As defined in RFC 1661 [45].

Length As defined in RFC 1661 [45].

Magic-Number As defined in RFC 1661 [45].

Data Zero or more information elements as defined in 9.6.1.
9.6.1 Information Elements for LCP Echo-Request packet

If the sender sets the data field of the LCP Echo-Request, then the sender shall set the data field of LCP Echo-Request packet to the 3GPP2 Vendor Specific Information Element Structure as specified in this section.

<table>
<thead>
<tr>
<th>Table 23</th>
<th>3GPP2 Vendor Specific Information Element Structure for the LCP Echo-Request packet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSB</td>
</tr>
<tr>
<td></td>
<td>Information Element Identifier</td>
</tr>
<tr>
<td></td>
<td>Information Element Length</td>
</tr>
</tbody>
</table>

Information Element Identifier (1 octet):

The sender sets this field to the type of 3GPP2 Vendor Specific Information Element Structure in LCP Echo-Request packet:

<table>
<thead>
<tr>
<th>Table 24</th>
<th>Information Element Identifier for 3GPP2 Vendor Specific Information Element Structure in the LCP Echo-Request packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Element Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>00000001</td>
<td>Active VSNCP Context Identifiers</td>
</tr>
<tr>
<td>Others</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

Information Element Length (1 octet):

The sender sets this field to the number of octets contained in the Information Element Value field.

Information Element Value (Information Element Length octets)

The sender sets this field as follows:

If the Information Element Identifier is set to ‘00000001’ (Active VSNCP Context Identifiers), then the sender shall set this field to a list of active VSNCP Context Identifiers. Each field is one octet long, with the upper four bits set to the PDN Identifier and the lower four bits set to User Context identifier. If there is no User Context-identifier option associated with the VSNCP context, then the User Context-identifier field shall be set to ‘0000’.
10 Session Release Call Flows

This section provides the message flows for the different session release scenarios.

10.1 UE Initiated Release procedures

10.1.1 UE-Requested PDN Disconnection Procedure

The procedures for UE-requested PDN disconnect are based on the procedures in Clause 6.4.1 in TS23.402 [23]. The eHRPD radio specific portion of this procedure is described in C.S0087 [15].

![Diagram of UE Initiated PDN Disconnection Procedure]

**Figure 41  UE Initiated PDN Disconnection Procedure**

1. The UE sends a VSNCP Terminate-Request to the HSGW. The request contains the PDN-ID of the PDN with which the UE is closing the connection.

2. The HSGW sends a VSNCP Terminate-Ack to the UE to indicate that it received the request to terminate a connection to a PDN.

3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for the associated PDN for this UE.
4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN is needed in order to determine which PDN to deregister the UE from, as some P-GWs may support multiple PDNs.

5. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection in a Session Termination Request message.

6. The HSS/AAA responds with a Session Termination Answer message.

7. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

8. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends PBA message (MN NAI, APN, lifetime=0) to the HSGW.

   If all PDN connections with the UE are terminated, the HSGW initiates STa session termination (Not shown in the figure).

9. The UE initiates session configuration procedure to delete any reservations associated exclusively with the terminated PDN connections.

10. If the radio interface is modified by step 9, the eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

11. If step 10 occurs, the HSGW responds with A11-Registration Reply.

   If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate detach procedures.
10.1.2 UE-Initiated Detach Procedure

This section describes the message flows for the UE initiated detach procedure. The UE can initiate the detach procedure, for example, when the associated PPP session is terminated. This call-flow depicts the usage of LCP Terminate-Request/Ack to release the PPP session. The eHRPD radio specific portion of this procedure is described in C.S0087-0 [15].

**Figure 42  UE Initiated Detach Procedure**

1. The UE sends an LCP Terminate-Request message to the HSGW.
2. The HSGW sends an LCP Terminate-Ack to the UE to indicate that it received the request to terminate the PPP session.
Steps 3 to 8 are repeated for each APN to which the UE is attached and which is to be disconnected.

3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.

4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN is needed in order to determine which PDN to deregister the UE from, as some P-GWs may support multiple PDNs.

5. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection by sending a Session Termination Request.

6. The HSS/AAA responds with a Session Termination Answer.

7. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

8. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends a PBA message (MN NAI, APN, lifetime=0) to the MAG.

9. The HSGW sends Session Termination Request to 3GPP2 AAA Proxy/Server for releasing the Pi* and STa Diameter Sessions.

10. The 3GPP2 AAA Proxy/Server responds with a Session Termination Answer.

   Note: The 3GPP2 AAA Proxy/Server forwards the Session Termination Request to the 3GPP HSS/AAA and responds to the HSGW with Session Termination Answer on receiving the response from the 3GPP HSS/AAA.

11. The HSGW sends an A11-Registration Update message to initiate with the ePCF the release of all A10 connections for the UE. This step may occur immediately after Step 3.

12. The ePCF responds with an A11-Registration Acknowledge message.

13. The UE/eAN may initiate HRPD session update.

14. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release all A10 connections.

15. The HSGW responds with A11-Registration Reply with lifetime zero.
10.2 Network Initiated UE Detach

This section describes the message flows for the network initiated UE detach procedures.

10.2.1 HSS/AAA Initiated UE Detach

This section describes the message flows for the network initiated UE detach due to HSS or AAA initiated release procedures. The HSS can initiate the network initiated detach procedure, for example, when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, for example, upon instruction from OA&M or when the timer for re-authentication/re-authorization has expired. This call flow depicts the usage of the LCP Terminate-Request procedure to release the PPP session.

![Figure 43: HSS/AAA Initiated UE Detach Procedure](image-url)
1. The HSS/AAA sends an Abort Session Request (ASR) message to the HSGW to detach the UE from the network.

2. The HSGW sends an LCP Terminate-Request to the UE.

3. The UE sends an LCP Terminate-Ack to the HSGW to indicate that it received the request to terminate the PPP session.

   Steps 4 to 9 are repeated for each APN to which the UE is attached and which is to be disconnected.

4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE for the associated PDN.

5. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN is needed in order to determine which PDN to deregister the UE from, as some P-GWs may support multiple PDNs.

6. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection by sending a Session Termination Request.

7. The HSS/AAA responds with a Session Termination Answer.

8. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

9. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends a PBA message (MN NAI, APN, lifetime=0) to the HSGW.

10. The HSGW sends an A11-Registration Update message to initiate with the ePCF the release of all A10 connections for the UE. This step may occur immediately after Step 3.

11. The ePCF responds with an A11-Registration Acknowledge message.

12. The eAN may initiate HRPD session update. The UE may initiate HRPD session update any time after step 3.

13. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release all A10 connections.

14. The HSGW responds with A11-Registration Reply with lifetime zero.

15. The HSGW sends an Abort Session Answer (ASA) to the HSS/AAA.
10.2.2 HSGW Initiated UE Detach

This section describes the message flow for the network initiated UE detach due to HSGW initiated release procedures. The HSGW can initiate the network initiated detach procedure, for example, when the associated PPP session is terminated. This call-flow depicts the usage of LCP Terminate-Request/Ack to release the PPP session.

**Figure 44** HSGW Initiated UE Detach Procedure
1. The HSGW sends an LCP Terminate-Request to the UE.

2. The UE sends an LCP Terminate-Ack to the HSGW to indicate that it received the request to terminate the PPP session.

   Steps 3 to 8 are repeated for each APN to which the UE is attached and which is to be disconnected.

3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE for the associated PDN.

4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN is needed in order to determine which PDN to deregister the UE from, as some P-GWs may support multiple PDNs.

5. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection by sending a Session Termination Request.

6. The HSS/AAA responds with a Session Termination Answer.

7. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

8. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends a PBA message (MN NAI, APN, lifetime=0) to the HSGW.

9. The HSGW sends a Session Termination Request to 3GPP2 AAA Proxy/Server for releasing the Pi* and STa Diameter Sessions.

10. The 3GPP2 AAA Proxy/Server responds with a Session Termination Answer.

   Note: The 3GPP2 AAA Proxy/Server forwards the Session Termination Request to the 3GPP HSS/AAA and responds to the HSGW with Session Termination Answer on receiving the response from the 3GPP HSS/AAA.

11. The HSGW sends an A11-Registration Update message to initiate with the ePCF the release of all A10 connections for the UE. This step may occur immediately after step 3. The HSGW initiates STa session termination (Not shown in the figure).

12. The ePCF responds with an A11-Registration Acknowledge message.

13. The eAN may initiate HRPD session update. The UE may initiate HRPD session update any time after step 2.

14. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release all A10 connections.

15. The HSGW responds with A11-Registration Reply with lifetime zero.
10.3 Network Initiated PDN Disconnection

This section describes the message flows for the network initiated PDN disconnection procedure.

10.3.1 HSS/AAA Initiated PDN Disconnection

The HSS/AAA, e.g. to support user’s subscription update, can indicate to a P-GW to remove one or several PDN connections previously activated by the UE. This section describes the network initiated PDN disconnection procedure as per the HSS/AAA indication.

Figure 45 HSS/AAA Initiated PDN Disconnection Procedure

1. The HSS/AAA sends an Abort Session Request message to indicate to the P-GW to remove an existing PDN connection, refer to TS 29.273 [34].
2. The P-GW sends a PMIPv6 Binding Revocation Indication (BRI) message to the HSGW as defined in RFC 5846 [84] indicating a non-handoff cause.
3. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of the PDN with which the connection is to be terminated.
4. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to terminate a connection to a PDN.
5. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.
6. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

7. The HSGW sends a PMIPv6 Binding Revocation Acknowledgement (BRA) message to the HSGW as RFC 5846 [84].

8. The P-GW sends an Abort Session Answer message to the HSS/AAA

9. The UE initiates session configuration procedure to delete any reservations associated exclusively with the terminated PDN connections.

10. The eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

11. The HSGW responds with A11-Registration Reply.

If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate LCP termination procedures. If the HSGW finds that all PDN connections have been deleted, then the HSGW initiates STa session termination (not shown in the figure).
10.3.2 P-GW Initiated PDN Disconnection

This section describes the network initiated PDN disconnection procedure as per the P-GW indication or request.

1. The P-GW sends a PMIPv6 Binding Revocation Indication (BRI) message to the HSGW as defined in RFC 5846 [84] indicating a non-handover cause.

2. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of the PDN with which the connection is to be terminated.

3. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to terminate a connection to a PDN.

4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.

5. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].
6. The HSGW sends a PMIPv6 Binding Revocation Acknowledgement (BRA) message to the HSGW as defined in RFC 5846 [84].

7. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection in a Session Termination Request message.

8. The HSS/AAA responds with a Session Termination Answer message.

9. The UE initiates session configuration procedure to delete any reservations associated exclusively with the closed PDN connection.

10. The eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

11. The HSGW responds with A11-Registration Reply.

If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate LCP termination procedures. If the HSGW finds that all PDN connections have been deleted, then the HSGW initiates STa session termination (not shown in the figure).
10.3.3 HSGW Initiated PDN Disconnection

This section describes the network initiated PDN disconnection procedure as per the HSGW indication or request

1. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of the PDN with which the connection is to be terminated.

2. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to terminate a connection to a PDN.

3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.

4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero, indicating de-registration.

Figure 47 HSGW Initiated PDN Disconnection Procedure

- The UE
- eAN/ePCF
- HSGW
- P-GW
- V-PCRF
- H-PCRF
- HSS/AAA

1. VSNCP Terminate-Request (PDN-ID)
2. VSNCP Terminate-Ack (PDN-ID)
3. Gateway Control Session Termination Procedure
4. P-BU (Lifetime=0)
5. PCEF-initiated IP-CAN Session Termination Procedure
6. P-BA
7. Session Termination Request
8. Session Termination Answer
9. Air Interface Procedures
10. A11-Registration Request
11. A11-Registration Reply
5. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

6. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends PBA message (MN NAI, APN, lifetime=0) to the HSGW.

7. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection in a Session Termination Request message.

8. The HSS/AAA responds with a Session Termination Answer message.

Steps 9 through 11 can happen any time after step 2.

9. The UE initiates session configuration procedure to delete any reservations associated exclusively with the terminated PDN connection.

10. The eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

11. The HSGW responds with A11-Registration Reply.

If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate LCP termination procedures. If the HSGW finds that all PDN connections have been deleted, then the HSGW initiates STa session termination (not shown in the figure).
10.3.4 P-GW Initiated Resource Deactivation

This section describes network initiated PDN resource deactivation due to IP-CAN session modification/termination initiated by the PCRF (see TS 23.402 [23], TS 23.203 [20] and TS 29.213 [30]) or by the P-GW. These procedures also address the case of UE handover from eHRPD to E-UTRAN.

For the case of resource deactivation triggered by IP-CAN session modification/termination, the resources associated with the PDN connection in the P-GW as well as the resources in the eHRPD system are released. For the case of handover from eHRPD to E-UTRAN, the resources associated with the PDN connection in the P-GW are maintained, whereas the resources in the eHRPD system are released.

![Diagram](image)

**Figure 48 P-GW Initiated Resource Deactivation**

0. PDN GW initiated resource deactivation may be triggered due to IP CAN session modification/termination procedures, as defined in TS 23.402 [23], TS 23.203 [20] and TS 29.213 [30].

1. The P-GW sends a PMIPv6 Binding Revocation Indication (BRI) message to the HSGW as defined in RFC 5846 [84]. The BRI indicates the cause of disconnection, such as due to IP-CAN session modification/termination, or a handover cause resulting from UE handover from eHRPD to E-UTRAN.

2. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of the PDN with which the connection is to be terminated.

3. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to terminate a connection to a PDN.
4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20]. The HSGW no longer applies QoS policy to service data flows for this UE.

5. The HSGW sends a PMIPv6 Binding Revocation Acknowledgement (BRA) message to the HSGW as defined in RFC 5846 [84].

6. For the case of PDN connection termination due to IP-CAN session modification, the P-GW informs the HSS/AAA to remove the P-GW identity information and APN corresponding to the UE's PDN connection in a Session Termination Request message. For the case of handover from eHRPD to E-UTRAN, IP-CAN session in the P-GW is maintained and this step and the next step (step 7) are not performed.

7. The HSS/AAA responds with Session Termination Answer message.

8. The UE initiates session configuration procedure to delete any reservations associated with the closed PDN connection. This can happen anytime after step 3.

9. The eAN/ePCF sends an A11-Registration Request to update A10 connections mapping info to the HSGW.

10. The HSGW responds with A11-Registration Reply.

If the UE or HSGW finds that all PDN connections have been deleted, then either entity may initiate LCP termination procedures. If the HSGW finds that all PDN connections have been deleted, then the HSGW initiates STa session termination as well (not shown in the figure).
10.4 3GPP2 Mobile IPv6 Mobility Options

The P-GW may need to communicate additional information to the HSGW concerning termination or rejection of a PDN connection. For the termination case, the P-GW communicates this information in a Mobile IPv6 Mobility Option in the BRI. For the rejection case, the P-GW communicates this information in a Mobile IPv6 Mobility Option in the PBA message.

The following describes 3GPP2 Mobile IPv6 Mobility Options that carry information from the P-GW to the HSGW in the BRI or PBA message.

10.4.1 3GPP2-Reconnect-Indication

The 3GPP2-Reconnect-Indication IPv6 Mobility Option carries information to assist the UE in deciding whether to reconnect to the APN associated with this PDN connection. The format of the 3GPP2-Reconnect-Indication follows.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>8 octets.</td>
</tr>
<tr>
<td>5535</td>
<td>MO Sub-Type = 2</td>
</tr>
<tr>
<td>MO Data = reconnect indication</td>
<td></td>
</tr>
</tbody>
</table>

Type: 19
Length: 8 octets.
Vendor/Org-ID: 5535
MO Sub-Type: 2
MO Data: This field contains the reconnect indication from the P-GW. 1 = reconnect to this APN not allowed. All other values are reserved.
11 Inter-HSGW Mobility Procedures

This section defines inter-HSGW mobility procedures for eHRPD. A diagram of an eHRPD network during inter-HSGW context transfer is shown in Figure 49.

Two HSGWs are depicted in Figure 49, one marked S-HSGW for Source HSGW and the other marked T-HSGW for Target HSGW. The HSGW is a functional entity in the network that provides IP edge functionalities to the UE. The P-GW/LMA tunnels user data to/from the S-HSGW via S2a (PMIP-based) interface. During an inter-HSGW context transfer, a bearer plane interface (H2) is used to tunnel user data between the S-HSGW and the T-HSGW. The H2 tunnel is established after necessary context information is exchanged between the S-HSGW and the T-HSGW via the control plane interface (H1). Finally, the A10/A11 interface is used to tunnel data to/from the Target eAN/ePCF (T-eAN/ePCF) and the T-HSGW. The inter-HSGW context transfer procedures consist of three elements: H2 tunneling, H1 context transfer, and proxy Mobile IP binding update via the S2a interface.

When the UE moves to the serving area of a new eAN/ePCF and the eHRPD session is successfully transferred from the Source eAN/ePCF (S-eAN/ePCF) to the T-eAN/ePCF, if the S-HSGW is not reachable from the T-eAN/ePCF, then the T-ePCF selects a T-HSGW for the session. During the A10 session establishment, the T-ePCF sends the T-HSGW the S-HSGW’s H1 IP address information received from the S-eAN/ePCF. The T-HSGW initiates context transfer of the HSGW session state from the S-HSGW.
The unidirectional H2 tunnel (traffic flows from the S-HSGW to the T-HSGW) is established using the per-UE GRE keys that are allocated by the T-HSGW and exchanged between the T-HSGW and the S-HSGW as part of the H1 signaling. This GRE tunnel carries all the UE’s traffic from the S-HSGW to the T-HSGW. The detailed procedures for the H2 tunnel establishment, H1 context transfer, and release of the H2 tunnel are specified in the following sub-sections.

Each HSGW should only indicate that it supports the VSNP Extend Code field per 9.1.5 if all HSGWs to which it has an H1/H2 interface also support the VSNP Extend Code field.

If a target HSGW receives context from a source HSGW during inter-HSGW context transfer that includes VSNP Extend Code options negotiated with the UE that the target HSGW cannot support, then the target HSGW may choose to renegotiate the PDN connection (using VSNCP), may choose to close the PDN connection, or may choose to re-establish the PPP session with the UE.

If any of the following capabilities is supported by one HSGW, then all the HSGWs that participate in inter-HSGW context transfer with that HSGW shall also support that feature.
- MUPSAP
- Emergency call support
- VSNP Extend Code

11.1 Intra-eHRPD Handoff with HSGW Relocation using Context Transfer

This section describes inter-HSGW context transfer call flows for eHRPD.

11.1.1 Handoff when the UE is Active on the eHRPD Radio

Example call flows for inter-HSGW context transfer for eHRPD are illustrated in Figure 50. The signaling interface between the HSGWs is used for context transfer, such as UE’s IP address(es), TFTs, PPP state, etc. The data interface is used for uplink and downlink data transfer for the UE from S-HSGW to T-HSGW during handoff.

Figure 50 illustrates an example call flow for an eHRPD inter-HSGW context transfer when the UE is active on the eHRPD radio.
Figure 50  Inter-HSGW Context Transfer

The steps in Figure 50 are described below.
0. The UE has a session up and running with the P-GW via the source eAN/ePCF (S-eAN/ePCF) and source HSGW (S-HSGW).

1. An end-to-end data path between the UE and the correspondent node is established and the UE can send/receive packets to/from the network via the S-eAN/ePCF, S-HSGW and P-GW.

2. The UE and/or the S-eAN decide that the UE will move to the T-eAN.

3. The S-eAN and T-eAN cooperate using A13 or A16 signaling to move the eHRPD radio session context to the T-eAN, including the H1 address at the S-HSGW.

4. The T-eAN/ePCF sends an A11-Registration Request (RRQ) message to the T-HSGW to signal the handoff. The message includes the S-HSGW’s H1 IP address and MSID of the UE, and sets the A10 connections for the UE, etc. The T-eAN/ePCF sends this message anytime after step 3.

5. The T-HSGW accepts the connection and sends an A11-Registration Reply (RRP) message back to the T-eAN/ePCF with an accept indication.

6. Triggered by step 4, the T-HSGW sends a Handover Initiate (HI) message (see RFC 5949 [85]) including the MSID to the S-HSGW to request the session context, subscription context, etc. The message also contains the GRE key(s) that the T-HSGW wants to use for the uni-directional tunnel(s) (H2 tunnels) between S-HSGW and T-HSGW for data transfer. The GRE keys correspond to one GRE tunnel for forwarding the uplink data to the T-HSGW and one GRE tunnel for forwarding the downlink data to the T-HSGW.

7. The S-HSGW sends a Handover Ack (HAck) message to the T-HSGW with the session context information TLVs as defined in section 11.3.3. This message includes the following set of information at a minimum for each established PDN connection: MN-NAI, MN-LL-Identifier, UE’s IPv4 address(es)/IPv6 prefix(es), APNs, User Context Identifier if MUPSAP is in use, TFTs, P-GW IP address(es), policy context, compression context (e.g., ROHC context), User’s AAA profile with subscription information, PPP state, MSK Info, and MSK lifetime. Other information may be included if available. The relationship of each PDN-ID with APN, User Context Identifier if MUPSAP is in use, P-GW address, and GRE key for uplink traffic to the P-GW is included in the context that is transferred.

8. In this scenario, the HSGW and the 3GPP2 AAA Proxy perform the HSGW relocation procedure. Steps 8a to 8d are performed per section 11.3.5. Steps 8a to 8d are required only when the HSGW relocation procedure is performed.

8a The T-HSGW indicates to the 3GPP2 AAA Proxy that it is the new HRPD serving Gateway for this UE by sending a Update Location Request (ULR) message. The T-HSGW can initiate this step after step 7.

8b The 3GPP2 AAA Proxy removes the S-HSGW as the Gateway serving the UE. The 3GPP2 AAA Proxy informs the S-HSGW by sending a Cancel Location Request (CLR) command with the 3GPP2-Cancellation-Type AVP included with the cancellation type field is set to “HSGW Location Update Procedure”.

8c The S-HSGW acknowledges with a Cancel Location Answer (CLA) command.

8d The 3GPP2 AAA Proxy acknowledges that the T-HSGW is the serving Gateway for the UE by sending an Update Location Answer (ULA) command to the T-HSGW with a result code of success.

9. The S-HSGW extracts the downlink packets from the PMIPv6 tunnel from the P-GW and forwards the downlink packets to the T-HSGW over the downlink GRE tunnel.

9b. A PDN-ID is added in front of the packet and the packet is sent as received from the P-GW.

9c. The T-HSGW performs necessary packet processing operation for these downlink packets and forwards them to the T-eAN/ePCF. The downlink packets are forwarded to the T-eAN/ePCF through the T-HSGW and these packets are buffered until they can be delivered to the UE.
10. Triggered by step 8d, the T-HSGW sends a PBU to the P-GW to update the BCE for the UE with T-HSGW’s IP address as the new MAG.

11a. The uplink data packets that the UE is still sending over the S-eAN/ePCF are received at the S-HSGW.

11b. These packets are forwarded by the S-HSGW to the T-HSGW over the uplink H2 GRE tunnel. The S-HSGW does not perform any UL packet processing operation on these data packets (e.g., no HDLC and PPP de-framing of these UL packets received from the S-eAN/ePCF), except for any reassembly as specified in section 11.3.2. The S-HSGW also forwards any control plane packets, e.g., RSVP, DHCPv4 etc., from the UE that are sent over the S-eAN/ePCF to the T-HSGW. The S-HSGW adds an SRID in front of the A10 payload, after any necessary segment reassembly, and puts this as the payload of the uplink H2 GRE tunnel.

Note: The SRID will be the same after the Handoff for each service connection, and thus the T-HSGW will be able to correlate the traffic with a particular A10 based on the SRID it receives with the packet.

11c. The T-HSGW performs all necessary packet processing operations for these uplink packets. In this specification it is not required for the T-HSGW to wait for the PBA message as specified in RFC 5213 [78], therefore the HSGW forwards these packets to the P-GW. The UL packets are sent to the T-HSGW over the H2 UL GRE tunnel. The S-HSGW adds an SRID in front of the A10 payload and puts this as the payload of the H2 UL GRE tunnel.

12. The P-GW updates its BCE, switches the data path to the T-HSGW and returns a PBA message to the T-HSGW to indicate successful operation. Anytime after step 12, the P-GW may perform a Registration Revocation procedure with the S-HSGW with Revocation Trigger value “Inter-MAG handoff - same Access Types”.

13. The P-GW sends a BRI to the S-HSGW with Revocation Trigger value set to “Inter-MAG handoff - same Access Types”, and receives a BRA.

14. Now that the BCE is updated and the data-path is switched, the downlink data packets from the P-GW start flowing to the T-HSGW. The T-HSGW forwards them to the T-eAN/ePCF. The T-eAN/ePCF buffers them until they can be delivered to the UE.

15. The T-eAN/ePCF acquires the UE.

16. The T-eAN may begin transmitting data to the UE. The T-eAN/ePCF starts emptying its buffer and it delivers the buffered downlink packets to the UE.

17. The T-HSGW interacts with the PCRF (via the Gxa interface) to set up the policy associated with the bearer(s) of the UE. This step can happen anytime after step 8d.

18. Anytime after step 15, the T-eAN/ePCF sends an A11-Registration Request message to the T-HSGW which includes an Active Start Airlink record. This is to indicate that the air interface traffic channel is now established.

19. The T-HSGW sends an A11-Registration Reply message to the T-eAN/ePCF.

20. At this time, both uplink and downlink traffic for the UE are going through the target system. The UE can begin to send uplink packets as soon as step 15 happens. Also, the T-HSGW begins forwarding downlink data directly received from the P-GW anytime after step 12.

21. Any time after step 11 and after the T-HSGW detects that there has been no data for a configurable period of time over the H2 tunnel, the T-HSGW sends a HI message to tear down the forwarding tunnels between the S-HSGW and T-HSGW.

22. The S-HSGW sends a HAck message to acknowledge successful teardown of the forwarding tunnel(s). The S-HSGW deletes all context for the UE.

23. The P-GW interacts with the PCRF (via the Gx interface) to setup the policy associated with the new bearer(s). This can happen in parallel with the PMIPv6 tunnel set up (i.e., anytime after step 9).
24. 24a. After the T-eAN/ePCF has acquired the UE and is assured that access to the system by the UE would be directed to the T-eAN/ePCF, it sends an A16-Session Release Indication message to the S-eAN/ePCF. This message indicates that the session is now under control of the T-eAN/ePCF; hence the S-eAN/ePCF can terminate its connection with the S-HSGW and can purge the session associated with the UE. This step can happen any time after step 15.

24b. The S-eAN/ePCF sends an A16-Session Release Indication Ack message to the T-eAN/ePCF.

25. 25a. Any time after step 21, the S-HSGW sends an A11-Registration Update message to the S-eAN/ePCF to request tearing down the bearer connection with the S-eAN/ePCF.

25b. The S-eAN/ePCF sends an A11-Registration Ack message to the S-HSGW.

26. 26a. The S-eAN/ePCF sends an A11-Registration Request message (with lifetime=0) to the S-HSGW to tear down the bearer between with the S-eAN/ePCF.

26b. The S-HSGW sends A11-Registration Reply message to the S-eAN/ePCF to confirm the de-registration process.
11.1.2 Handoff when the UE is Dormant on the eHRPD Radio

This section describes inter-HSGW relocation with context transfer when the UE is dormant on the eHRPD radio interface.

![Diagram](image)

0. The UE has an active session up and running with the P-GW via the source eAN/ePCF (S-eAN/ePCF) and source HSGW (S-HSGW).

1. An end-to-end data path between the UE and the correspondent node is established and the UE can send/receive packets to/from the network via the S-eAN/ePCF, S-HSGW and P-GW.

2. The UE makes a transition from active to dormant state.

3. After crossing the mobility boundary (footprint) of the current serving eAN/ePCF, the UE requests a session to be established between the UE and the target eAN/ePCF. During this

**Figure 51** Handoff when the UE is Dormant on the eHRPD Radio
procedure, the target eAN/ePCF receives the UATI of an existing eHRPD session (if available). The UATI can be used as an identifier for the existing eHRPD session when the target eAN/ePCF attempts to retrieve the existing eHRPD session state information from the source eAN/ePCF.

4. 4a. The T-eAN/ePCF sends an A13-Session Information Request message to the S-eAN/ePCF to request the eHRPD session information for the UE. The A13-Session Information Request message shall include the UATI, the Security Layer Packet and the Sector ID of the serving cell.

4b. The S-eAN/ePCF validates the A13-Session Information Request and sends the requested eHRPD user session information to the T-eAN/ePCF in an A13-Session Information Response message.

4c. The T-eAN/ePCF sends an A13-Session Information Confirm to the S-eAN/ePCF to indicate that T-eAN/ePCF has received the eHRPD session information. Upon receipt of the A13-Session Information Confirm message the S-eAN/ePCF deletes the associated session information.

5. The T-eAN/ePCF sends A11-Registration Request message to the T-HSGW to signal the handoff. The request includes the S-HSGW’s H1 IP address and MSID of the UE, and sets the A10 connections for the UE, etc. The T-eAN/ePCF sends this message anytime after step 4a.

6. Triggered by step 5, the T-HSGW sends a Handover Initiate (HI) message, see RFC 5949 [85], including the MSID to the S-HSGW to request the session context, subscription context, etc. The message also contains the GRE key(s) that the T-HSGW wants to use for the uni-directional tunnel(s) between S-HSGW and T-HSGW for data transfer. The GRE keys correspond to one GRE tunnel for forwarding the uplink data to the T-HSGW and one GRE tunnel for forwarding the downlink data to the T-HSGW.

7. The S-HSGW sends a Handover Ack (HAck) message to the T-HSGW with the session context TLVs as defined in section 11.3.3. This message includes the following set of information at a minimum for each established PDN connection: MN-NAI, MN-LL-Identifier, UE’s IPv4 address(es)/IPv6 prefix(es), APNs, User Context Identifier if MUPSAP is in use, TFTs, P-GW IP address(es), policy context, compression context (e.g., ROHC context), User’s AAA profile with subscription information, PPP state, MSK Info, and MSK lifetime. Other information may be included if available. The relationship of each PDN-ID with APN, User Context Identifier if MUPSAP is in use, P-GW address, and GRE key for uplink traffic to the P-GW is included in the context that is transferred.

8. In this scenario, the HSGW and the 3GPP2 AAA Proxy perform the HSGW relocation procedure. Steps 8a to 8d are performed per section 11.3.5. Steps 8a to 8d are required only when the HSGW relocation procedure is performed.

8a. The T-HSGW indicates to the 3GPP2 AAA Proxy that it is the new serving Gateway for this UE by sending a Update Location Request (ULR) command. The T-HSGW can initiate this step after step 7.

8b. The 3GPP2 AAA Proxy removes the S-HSGW as the Gateway serving the UE. The 3GPP2 AAA Proxy informs the S-HSGW by sending a Cancel Location Request (CLR) command with the 3GPP2-Cancellation-Type AVP included with the cancellation type field is set to “HSGW Location Update Procedure”.

8c. The S-HSGW acknowledges with a Cancel Location Answer (CLA) command.

8d. The 3GPP2 AAA Proxy acknowledges that the T-HSGW is the serving Gateway for the UE by sending a Update Location Answer (ULA) command to the T-HSGW with code success.

9. The T-HSGW accepts the connection and sends an A11-Registration Reply Message back to the T-eAN/ePCF with an accept indication.

10. 10a. If any downlink data arrives at the S-HSGW during this procedure, the S-HSGW extracts the downlink packets from the PMIPv6 tunnel from the P-GW and forwards the downlink packets to the T-HSGW over the downlink GRE tunnel.
10b. A PDN-ID is added in front of the packet and the packet is sent as received from the P-GW.

10c. The T-HSGW performs necessary packet processing operation for these downlink packets and forwards them to the T-eAN/ePCF. The downlink packets are forwarded to the T-eAN/ePCF through the T-HSGW and these packets are buffered until they can be delivered to the UE. The T-eAN will use normal paging procedures to place the UE on a traffic channel and subsequently deliver the data. This is not shown in the figure.

11. Triggered by step 8d, the T-HSGW sends a PBU to the P-GW to update the BCE for the UE with T-HSGW’s IP address as the new MAG.

12. The P-GW/LMA updates its BCE, switches the data path to the T-HSGW (new MAG) and returns a PBA message to the T-HSGW to indicate successful operation. Anytime after this step, the P-GW may perform a Registration Revocation procedure with the S-HSGW with Revocation Trigger value “Inter-MAG handoff - same Access Types”.

13. The P-GW sends a BRI to the S-HSGW and receives a BRA.

14. Now that the BCE is updated and the data-path is switched, the downlink data packets from the P-GW start flowing to the T-HSGW. The T-HSGW forwards them to the T-eAN/ePCF. The T-eAN/ePCF buffers them until they can be delivered to the UE.

15. The T-HSGW interacts with the PCRF (via the Gxa interface) to set up the policy associated with the bearer(s) of the UE. This step can happen anytime after step 7.

16. After receipt of the PBA message (step 12) and after the T-HSGW detects that there has been no data for a configurable period of time over the H2 tunnel, the T-HSGW sends a HI message to tear down the forwarding tunnels between the S-HSGW and T-HSGW.

17. The S-HSGW sends a HACK message to acknowledge successful teardown of the forwarding tunnel(s). The S-HSGW deletes all context for the UE.

18. The P-GW interacts with the PCRF (via the Gx interface) to setup the policy associated with the new bearer(s). This can happen in parallel with the PMIPv6 tunnel set up (i.e., anytime after step 11).

19. 19a. Any time after step 6, the S-HSGW sends A11-Registration Update message to S-eAN/ePCF to request tearing down of the bearer connections with the S-eAN/ePCF.

19b. The S-eAN/ePCF sends an A11-Registration Ack message to the S-HSGW.

20. 20a. The S-eAN/ePCF sends an A11-Registration Request message (with lifetime=0) to the S-HSGW to tear down the bearer between with the S-eAN/ePCF.

20b. The S-HSGW sends an A11-Registration Reply message to the S-eAN/ePCF to confirm the de-registration process.
11.2 Intra-eHRPD Handoff with HSGW Relocation without Context Transfer

The UE performs handoff to a Target eAN (T-eAN) where the T-eAN selects a T-HSGW. Since there is no trust relationship between the T-HSGW and S-HSGW, in this example, the T-HSGW requires the UE to perform LCP, CCP, and attach procedures for the PDNs the UE is connected to. The UE shall set the Attach-Type in the VSNCP procedure to “handover” in this case.

Handoff without context transfer will occur if there is no H1/H2 connectivity to the source HSGW, or if for some reason the context transfer signaling exchange fails. This procedure may not be necessary in a network with reliable H1/H2 connectivity between all HSGWs.

---

**Figure 52** Intra-eHRPD Handoff with HSGW Relocation without Context Transfer
0. The UE has an active session up and running with the P-GW via the source eAN/ePCF (S-eAN/ePCF) and source HSGW (S-HSGW).

1. An end-to-end data path between the UE and the correspondent node is established and the UE can send/receive packets to/from the network via the S-eAN/ePCF, S-HSGW and P-GW.

2. The UE transitions from S-eAN/ePCF to target eAN/ePCF (T-eAN/ePCF). This could be an active handoff or a dormant handoff involving A16 or A13.

3. The eHRPD session is transferred from S-eAN/ePCF to T-eAN/ePCF.

4. Anytime after step 3, the T-eAN/ePCF sends an A11-Registration Request message to the T-HSGW to signal the handoff. The request includes the S-HSGW’s IP address, the MSID of the UE, the existing A10 connection information for the UE, etc.

5. The T-HSGW accepts the connection and sends an A11-Registration Reply Message back to the T-eAN/ePCF with an accept indication.

6. The assumption in this flow is that an H1 interface does not exist between the S-HSGW and T-HSGW. Therefore, since the T-HSGW does not have an authentication context for the UE, the T-HSGW sends an LCP Configure-Request to the UE.

6a. The UE, HSGW, and AAA Server continue the LCP negotiation procedures. EAP-AKA’ is executed as the authentication protocol. CCP negotiation is performed if needed.

Steps 7-9 are repeated for each PDN connection that the UE had on the S-HSGW.

7. The UE and the eHRPD network perform the steps for PDN bearer establishment. These steps are described in step 8 to 17 in Section 5.4.1. The following changes are required to the flow in Section 5.4.1:

   i. Step 8 in Section 5.4.1: the VSNCP Configure-Request message has the Attach Type set to ‘Handover’ to indicate to the network that the UE has previously established state with the EPC network. The UE sets the IP address to the previously assigned IP address(es) in the PDN Address Option.

8. The P-GW sends a PMIPv6 Binding Revocation Indication to the S-HSGW and receives an acknowledgement. The Revocation Trigger value is “Inter-MAG handoff - same Access Types”.

9. If the Selected Bearer Control Mode of the PCO option is set to is ‘Network only mode’ or “MS/NW”, then the network initiates QoS update procedures to setup all dedicated bearers on the T-HSGW for that PDN connection. Otherwise, the UE performs the UE initiated QoS update procedures for that PDN connection.

10. 10a. The S-HSGW sends a Session Termination Request to the HSS/AAA per TS 29.273 [34].

   10b. The HSS/AAA sends a Session Termination Answer to the S-HSGW.

11. 11a. The S-HSGW sends an A11-Registration Update message to S-eAN/ePCF to request tearing down of the bearer connections with the S-eAN/ePCF. This step may occur any time after step 8.

   11b. The S-eAN/ePCF sends an A11-Registration Ack message to the S-HSGW.

12. 12a. The S-eAN/ePCF sends an A11-Registration Request message with lifetime=0 to the S-HSGW to tear down the bearer with the S-eAN/ePCF.

   12b. The S-HSGW sends an A11-Registration Reply message to the S-eAN/ePCF to confirm the de-registration process.
11.3 Inter-HSGW Stage 3

11.3.1 Inter-HSGW Tunnel Establishment

The protocol and the structure of the messages used for inter-HSGW handoff is as per RFC 5949 [85]. For inter-HSGW handoff signaling purposes, the reactive handover procedure as described in RFC 5949 [85] applies. Also, the Mobility Header-based messages shall be used between the HSGWs. The TLVs specified in section 11.3.3 shall be used to carry the context parameters needed for eHRPD. It is assumed that the HSGWs perform context transfer of security material, i.e., MSK Info, only when there is mutual trust between the gateways.

In order to establish a per-UE unidirectional GRE H2 tunnel, the HSGW shall use GRE as defined in RFC 2784 [55], Key and Sequence Number Extensions to GRE as defined in RFC 2890 [56], and the GRE Key option defined in RFC 5845 [83] to exchange the required per-UE GRE keys when sending the HI message. In this specification, the T-HSGW shall include two instances of the GRE Key Option. The first instance shall contain the H2 GRE Key for the UE downlink traffic. The second instance shall contain the H2 GRE Key for the UE uplink traffic. These two GRE Keys are used for traffic going from the S-HSGW to the T-HSGW for the UE.

If segmentation is being used on an A10 connection between the S-ePCF and the S-HSGW, the S-HSGW shall reassemble the uplink PDU before sending the PDU over H2 to the T-HSGW.

For the details of encapsulation of the UE downlink and uplink traffic over the H2 GRE tunnel, see section 11.3.4.

11.3.2 HSGW Requirements

The S-HSGW shall set its MSK to either the value of the MSK received from the AAA or to the value of the MSK Info received from another HSGW.

The S-HSGW shall use the 128 most significant bits of the MSK (Sub-MSK) as the Master Session Key for the derivation of PMKs. The S-HSGW shall declare the remaining portion of the received MSK as the unused MSK information. The S-HSGW shall set the value of the MSK Lifetime Info TLV to the remaining lifetime of the authorized session.

The S-HSGW shall include the MSK Info TLV only if the unused portion of the MSK information is ≥ 128 bits, the Target HSGW is trusted, and the link between the HSGWs is secure (e.g., IPsec). At the inter-HSGW handoff, if the MSK Info TLV is included, the S-HSGW shall set the value of the MSK Info TLV to the unused portion of the MSK information. The T-HSGW shall set its MSK to the value of the MSK Info TLV and act as defined above.

If the lifetime of the received MSK Info is close to expiry, or if the length of the received MSK Info is equal to 128 bits, or if the MSK Info TLV is not received, the T-HSGW shall initiate the authentication as soon as possible to continue with the session. When the new MSK AVP is received from the AAA, the T-HSGW shall deprecate the current MSK value.
and replace it with the value received in the MSK AVP. The T-HSGW shall derive the new PMK from the new MSK as specified in section 4.2.2.3.

It is optional for the HSGW to support inter-HSGW handoff without context transfer. If the T-HSGW receives an A11-Registration Request and the T-HSGW cannot obtain a PPP context for the UE from the S-HSGW, then the T-HSGW shall send an LCP Configure-Request message to UE.

### 11.3.3 H1 Context Parameter TLVs

This section defines the TLVs that are needed for the transfer of context parameters between the S-HSGW and T-HSGW. The format of the context parameters TLVs is illustrated in Table 25.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>2 octets</td>
<td>Unsigned Integer. Identifies the Context Parameter TLV.</td>
</tr>
<tr>
<td>Length:</td>
<td>2 octets</td>
<td>Unsigned Integer. The length of the TLV in octets, including</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the length of the “Type” and “Length” fields.</td>
</tr>
<tr>
<td>Context Parameter Data:</td>
<td>variable</td>
<td>Structure and content of the Context Parameter carried in the TLV.</td>
</tr>
</tbody>
</table>

In the case of full context transfer, all the context parameters identified in this section shall be transferred from S-HSGW to the T-HSGW. In the case of partial context transfer, only the context parameters that are explicitly identified in each of the sub-sections shall be transferred from the S-HSGW to the T-HSGW.
11.3.3.1 User NAI

This TLV is of the following format. It carries the NAI of the user. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 26 User NAI TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NAI...</td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF01
Length: ≤ 74 octets
NAI: This NAI is associated with the user and is received from the 3GPP AAA upon successful EAP authentication in the Permanent User Identity IE (Mobile-Node-Identifier AVP). The format is specified in TS 23.003 [19].

11.3.3.2 User MSID

This TLV is of the following format. It carries the MSID of the user. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 27 User MSID TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>MSID</td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF02
Length: ≤ 22 octets
MSID: This is the MSID associated with the UE as received from the eAN via A11 messages. The format of this field is as per the Session Specific Extension defined in A.S0017-D [5].
11.3.3.3 LCP Info

This TLV contains the parameters negotiated via the LCP during PPP connection establishment between the HSGW and the UE. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 28 LCP Info TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>HP</th>
<th>UP</th>
<th>HA</th>
<th>UA</th>
<th>Reserved</th>
<th>HSGW-Magic Number</th>
<th>UE-Magic Number</th>
<th>HSGW-MRU</th>
<th>UE-MRU</th>
<th>HSGW-Auth-Proto</th>
<th>UE-Auth-Proto</th>
</tr>
</thead>
</table>

Type: 0xFF03
Length: 24 octets

HP-bit (HSGW PFC): When set, this bit indicates that the HSGW has negotiated PFC (see RFC 1661). Otherwise, it indicates that the HSGW has not negotiated PFC with the UE.

UP-bit (UE PFC): When set, this bit indicates that the UE has negotiated PFC (see RFC 1661 [46]). Otherwise, it indicates that the UE has not negotiated PFC with the HSGW.

HA-bit (HSGW ACFC): When set, this bit indicates that the HSGW has negotiated ACFC (see RFC 1661 [46]). Otherwise, it indicates that the HSGW has not negotiated ACFC with the UE.

UA-bit (UE ACFC): When set, this bit indicates that the UE has negotiated ACFC (see RFC 1661 [46]). Otherwise, it indicates that the UE has not negotiated ACFC with the HSGW.

Reserved: Reserved for future use. Set to all 0s.

HSGW-Magic Number: This field carries the Magic Number negotiated by the HSGW with the UE and is coded per the Magic Number definition in RFC 1661 [46].

UE-Magic Number: This field carries the Magic Number negotiated by the UE with the HSGW and is coded per the Magic Number definition in RFC 1661 [46].

HSGW-MRU: This field carries the Maximum-Receive-Unit negotiated by the HSGW with the UE and is coded per the MRU definition in RFC 1661 [46].

UE-MRU: This field carries the Maximum-Receive-Unit negotiated by the UE with the HSGW and is coded per the MRU definition in RFC 1661 [46].
HSGW-Auth-Proto: This field carries the Authentication-Protocol negotiated by the HSGW with the UE and is coded per the Auth-Proto definition in RFC 1661 [46].

UE-Auth-Proto: This field carries the Authentication-Protocol negotiated by the UE with the HSGW and is coded per the Auth-Proto definition in RFC 1661 [46].

### 11.3.3.4 CCP Info

This TLV contains the parameters negotiated via CCP during PPP connection establishment between the HSGW and the UE. These fields are defined in RFC 1962 [47]. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Type</td>
<td>Length</td>
<td></td>
</tr>
</tbody>
</table>

Table 29  CCP Info TLV

Type: 0xFF04
Length: 8 octets

HSGW-Comp-Proto: This field carries the CCP configuration option sent by the HSGW during CCP exchange with the UE.

UE-Comp-Proto: This field carries the CCP configuration option sent by the UE during CCP exchange with the HSGW.

### 11.3.3.5 VSNCP State and Common Info

This TLV contains the list of PDN IDs established with VSNCP. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Type</td>
<td>Length</td>
<td></td>
</tr>
</tbody>
</table>

Table 30  VSNCP State and Common Info TLV

Type: 0xFF05
Length ≥5 octets

List of PDN IDs: The list of 1 octet long PDN IDs for the UE. At least 1 PDN ID shall be present for the UE.
11.3.3.6 PDN Info

This TLV contains the PDN specific common info and shall be used only if MUPSAP is not supported at the S-HSGW. This TLV shall be repeated for each connected PDN at the S-HSGW. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

Table 31 PDN Info TLV

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDN ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF06
Length: ≤ 110 octets
PDN ID: This field carries the 1 octet PDN Identifier.
Reserved: Reserved for future use. Set to all 0s.
APN: This field carries the Access Point Name that is associated with the PDN Identifier. See TS 24.302 [26]. The HSGW shall inspect the APN. If it is the emergency APN, the HSGW shall note that the UE is involved in emergency services relative to this PDN ID.

11.3.3.7 PCO Info

This TLV contains the PCO for a given PDN connection. This TLV shall be repeated for each connected PDN at the S-HSGW. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

Table 32 PCO Info TLV

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDN ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF07
Length: ≤ 259 octets
PDN ID: This field carries the 1 octet PDN Identifier.
Reserved: Reserved for future use. Set to all 0s.
PCO: This field carries the value portion of the Protocol Configuration Options received from
the UE for the associated PDN Identifier. See TS 24.008 clause 10.5.6.3 [24].

11.3.3.8 PDN Related Address Info

This TLV contains the PDN Address and PDN Type fields for a given PDN connection at the
S-HSGW. It also contains the IPv6 link-local address and IPv4 default router addresses
assigned by the P-GW. This TLV shall be repeated for each connected PDN at the S-HSGW.
This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of
full context transfer.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PDN ID</th>
<th>PDN Type</th>
<th>DHCP</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Prefix

IPv6 Prefix

IPv6 IID

IPv6 IID

IPv6 LLA

IPv6 LLA

IPv6 LLA

IPv6 LLA

IPv4 Address

IPv4 Default Router Address

Table 33 PDN Address Info TLV

Type: 0xFF08
Length: = 48 octets

PDN ID: This field carries the 1 octet PDN Identifier.
PDN Type: This field carries the 1 octet PDN Type field. If the PDN Type field indicates that
the PDN is an IPv4 only PDN, the IPv6 Prefix and the IPv6 IID fields and the IPv6 LLA
fields are set to all 0s and the IPv4 Address field carries a non-zero PDN address. If the PDN
Type field indicates that the PDN is an IPv6 only PDN, the IPv6 Prefix and the IPv6 IID fields carry non-zero IPv6 prefix and Interface Identifier (IID) information of the PDN. In this case, the IPv4 Address field and IPv4 Default Router Address field are set to all 0s. If the PDN Type field indicates that the PDN is a dual stack PDN, the IPv6 Prefix and the IPv6 IID fields carry non-zero IPv6 prefix and Interface Identifier (IID) information of the PDN. If an IPv4 Address has been assigned, the IPv4 Address and IPv4 Default Router Address fields carry non-zero PDN Addresses.

DHCP-bit (1 bit): When set, this bit indicates that DHCPv4 is used to allocate the UE’s IPv4 address.

Reserved (15 bits): Reserved for future use. Set to all 0s.

IPv6 Prefix: This field (8 octets long) carries the IPv6 prefix associated with the PDN connection of the UE.

IPv6 IID: This field (8 octets long) carries the IPv6 interface identifier assigned to the UE.

IPv6 LLA: This field (16 octets long) carries the IPv6 link-local address assigned by the P-GW used by the HSGW on the access link shared with the UE.

IPv4 Address: This field (4 octets long) carries the IPv4 Address is assigned to the UE.

IPv4 Default Router Address: This field (4 octets long) carries the UE’s IPv4 default router address.
11.3.3.9 PMIPv6 Info

This TLV contains the parameters required by T-HSGW (new MAG) to perform PMIPv6 registration with the P-GW (LMA). This TLV is repeated for each of the connected PDNs for the UE. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Table 34 PMIPv6 Info TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>PDN ID</td>
</tr>
<tr>
<td>PMIPv6 UL GRE</td>
</tr>
<tr>
<td>LMA IPv6 Address</td>
</tr>
<tr>
<td>LMA IPv6 Address</td>
</tr>
<tr>
<td>LMA IPv6 Address</td>
</tr>
<tr>
<td>LMA IPv6 Address</td>
</tr>
<tr>
<td>LMA IPv4 Address</td>
</tr>
</tbody>
</table>

Type: 0xFF09
Length: = 28 octets

PDN ID: This field carries the 1 octet PDN Identifier.

TT-flag: This is the 2-bits MAG-LMA transport flag. When this flag is set to 01, it indicates that the LMA has an IPv4 interface only. In this case, the LMA IPv6 Address field is set to all 0s. When this flag is set to 10, it indicates that the LMA has an IPv6 interface only. In this case, the IPv4 Address field is set to all 0s. When this flag is set to 11, it indicates that the LMA has both IPv4 and IPv6 interfaces. In this case, both the IPv6 Address and the IPv4 Address fields carry non-zero values representing the IPv6 address and the IPv4 address of the LMA respectively. The value of 00 for this flag is reserved.

Reserved: Reserved for future use. Set to all 0s.

PMIPv6 uplink GRE: This field (4 octets long) carries the Uplink GRE key for the PMIPv6 tunnel for the corresponding PDN connection.

LMA IPv6 Address: This field (16 octets long) carries the IPv6 Address of the LMA (P-GW) for the corresponding PDN connection.

LMA IPv4 Address: This field (4 octets long) carries the IPv4 Address of the LMA (P-GW) for the corresponding PDN connection.
11.3.3.10 ROHC Configuration Info

This TLV contains the parameters negotiated for ROHC compression. This TLV is repeated for each Service Connection for which ROHC has been negotiated. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 35 ROHC Configuration Info TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>Reserved-1</td>
</tr>
<tr>
<td>Forward/Reverse-MAX-CID</td>
<td>Forward/Reverse-MRRU</td>
</tr>
<tr>
<td>LC</td>
<td>Reserved-2</td>
</tr>
<tr>
<td>Forward/Reverse Profile-Count</td>
<td></td>
</tr>
</tbody>
</table>

Forward/Reverse Profiles ....

Type: 0xFF0A
Length: ≥ 24 octets
CM (CID Mode): 1-bit field of type Boolean 0 – small CID, 1 – large CID
Reserved-1: Reserved for future use. Set to all 0s.
SR-ID: This is the identifier of the service connection associated with this ROHC parameter set.
Forward/Reverse MAX-CID: MAX-CID to be used for this ROHC state. For each direction, the ROHC parameters shall be specified separately.
Forward/Reverse MRRU: MRRU to be used for this ROHC state. For each direction, the ROHC parameters shall be specified separately.
LC (Large CID): 1-bit field of type Boolean. If set to 1, indicates whether Large CIDs are supported of not. Otherwise, set to 0.
Reserved-2: Reserved for future use. Set to all 0s.
Forward/Reverse Profile-Count: Number of profiles supported. This parameter is exchanged with the UE at the time of ROHC parameter negotiation. This is a binary number.
Forward/Reverse Profiles: n octet-pairs in ascending order, each octet-pair specifying a ROHC profile supported. See RFC 3095 [58], RFC 3843 [68], RFC 4019 [71], and RFC 5225 [79].
11.3.3.11 ROHC IR Info

This TLV contains the most recent ROHC IR packet for a given Context ID. This TLV is repeated for each flow with a unique Context ID. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 36 ROHC IR Info TLV

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td>Type: 0x0</td>
<td>Type</td>
<td>Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRID</td>
<td>SRID</td>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ROHC IR Packet</td>
<td>ROHC IR Packet</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF0B
Length: ≥ 8 octets
SRID: This is the identifier of the service connection associated with this ROHC parameter set.
Reserved: Reserved for future use. Set to all 0s.
ROHC IR Packet: ROHC IR packets for a flow identified by its Context ID, as per RFC 3095 [58] and RFC 5225 [79].

11.3.3.12 QoS Info

This TLV contains the parameters related to QoS for the UE. This TLV is repeated for each FlowID for which QoS parameters have been negotiated. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 37 QoS Info TLV

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td>Type: 0xFF0C</td>
<td>Type</td>
<td>Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlowID</td>
<td>FlowID</td>
<td>Granted FlowProfileID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated FlowProfileID</td>
<td>Updated FlowProfileID</td>
<td>Num Requested FlowProfileIDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested FlowProfileIDs</td>
<td>Requested FlowProfileIDs</td>
<td>Num Authorized FlowProfileIDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorized FlowProfileIDs</td>
<td>Authorized FlowProfileIDs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF0C
Length: ≥ 12 octets
Flow ID: This is the Flow ID for which the following QoS parameters are reported.

Granted FlowProfileID:

   This is the initial granted FlowProfileID for the Flow ID. See: X.S0011 [6].

Updated FlowProfileID:

   This is the most recently sent updated FlowProfileID for the Flow ID. See: X.S0011 [6].

Num Requested FlowProfileIDs:

   Number of Requested Flow Profile IDs included in this context parameter.

Requested FlowProfileIDs:

   This is the list of requested FlowProfileIDs for the Flow ID. See: X.S0011 [6]. Each FlowProfileID in the list is two octets long.

Num Authorized FlowProfileIDs:

   Number of Authorized Flow Profile IDs included in this context parameter.

Authorized FlowProfileIDs:

   This is the list of authorized FlowProfileIDs for the Flow ID. See: X.S0011 [6]. Each FlowProfileID in the list is two octets long.

11.3.3.13 TFTv4 Info

This TLV contains the parameters related to IPv4 TFT for the UE. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

Table 38 TFTv4 Info TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xFF0D</td>
<td>&gt; 4 octets</td>
</tr>
</tbody>
</table>

TFT IPv4 IE Type #0: This is the IPv4 TFT object as defined in X.S0011 [6].
11.3.3.14 TFTv6 Info

This TLV contains the parameters related to IPv6 TFT for the UE. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

Table 39  TFTv6 Info TLV

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td>Type</td>
<td>Length</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TFT IPv6 IE Type # = 2...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF0E  
Length: > 4 octets  
TFT IPv6 IE Type #0: This is the IPv6 TFT object as defined in X.S0011 [6].

11.3.3.15 AAA Profile Info

This TLV contains the AAA profile (Diameter AVPs) received from the AAA during authentication and authorization at the HSGW for a given UE. For the complete list of the Diameter AVPs, refer to TS 29.273 [34]. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

Table 40  AAA Profile Info TLV

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td>Type</td>
<td>Length</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diameter AVPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF0F  
Length: > 4 octets  
Diameter AVPs: This field contains one or more AAA AVP(s) related to authorization of the user’s packet data service in the eHRPD system.
11.3.3.16  Gxa Info

This TLV contains the Gxa rule objects received from the PCRF that includes all the AVPs (QoS, SDF, charging rules etc.) during PCC transactions for a given UE. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Table 41</th>
<th>Gxa Info TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0  8  16  24  31</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Gxa AVPs</td>
</tr>
</tbody>
</table>

Type: 0xFF10
Length: > 4 octets
Gxa AVPs: Gxa AVPs related to the PCC rule set at the HSGW (BBERF) of the user’s IP-CAN session in the eHRPD system. The PDN information is embedded in the Gxa rule set. The format of the Gxa AVPs shall be as per TS 29.212 [29].

11.3.3.17  Vendor Specific Info

This TLV contains the parameters required by specific vendor’s implementation. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

<table>
<thead>
<tr>
<th>Table 42</th>
<th>Vendor Specific Info TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0  8  16  24  31</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Vendor-ID</td>
</tr>
<tr>
<td></td>
<td>Vendor Specific Values</td>
</tr>
</tbody>
</table>

Type: 0xFF11
Length: > 4 octets
Vendor-ID: This is the vendor identifier for the vendor that has a specific use of this TLV.
Vendor Specific Values: This field is populated based on specific a vendor’s implementation. The field is opaque to any implementation that cannot parse this field. In such case, the TLV should be silently discarded.
### 11.3.3.18 MSK Info

This TLV contains the MSK Info AVPs. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of both full context transfer and in the partial context transfer.

**Table 43 MSK Info TLV**

<table>
<thead>
<tr>
<th>Type (0x0FF12)</th>
<th>Length</th>
<th>MSK Lifetime Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>MSK Info</td>
</tr>
</tbody>
</table>

Type: 0xFF12  
Length: ≥ 24 octets  
MSK Lifetime Info: This 4 octet field contains the lifetime of the MSK delivered to the T-HSGW. This value is of type unsigned 32 and it represents the period of time (in seconds) for which the MSK Info is valid.  
MSK Info: This field contains the unused portion of the MSK.

### 11.3.3.19 QoS-Check Info

This TLV contains the parameters related to authorized QoS for the UE during the QoS-Check procedure. This context parameter shall be transferred if an inter-HSGW handoff occurs after a ResvConf message with opcode QoS-Check Conf has been sent, but before the TFTs can be sent by the UE in a Resv message once the radio interface procedures for establishing that IP Flow are complete. See steps 5 and 8 of Figure 22 in section 4.5.4.1.1. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

**Table 44 QoS-Check Info TLV**

<table>
<thead>
<tr>
<th>Type (0x0FF13)</th>
<th>Length</th>
<th>Flow ID</th>
<th>QoS-Check FlowProfileIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF13  
Length: ≥ 12 octets
Flow ID: This is the Flow ID for which the following FlowProfileIDs are reported during a QoS-Check operation.

QoS-Check FlowProfileIDs: This is the list of authorized FlowProfileIDs for the Flow ID during a QoS-Check operation. See: X.S0011 [6]. Each FlowProfileID in the list is two octets long.

11.3.3.20 QoS-Check TFTv4 Info

This TLV contains the authorized IPv4 TFT for the UE during the QoS-Check procedure. This context parameter shall be transferred if an inter-HSGW handoff occurs between steps 5 and 8 of Figure 22 in section 4.5.4.1.1. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>≥ 4 octets</td>
</tr>
</tbody>
</table>

TFT IPv4 IE Type #0: This is the authorized IPv4 TFT object during a QoS-Check operation. Ref: X.S0011 [6].

11.3.3.21 QoS-Check TFTv6 Info

This TLV contains the authorized IPv6 TFT for the UE during the QoS-Check procedure. This context parameter shall be transferred if an inter-HSGW handoff occurs after a ResvConf message with opcode QoS-Check Conf has been sent, but before the TFTs can be sent by the UE in a Resv message once the radio interface procedures for establishing that IP Flow are complete. See steps 5 and 8 of Figure 22 in section 4.5.4.1.1. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>≥ 4 octets</td>
</tr>
</tbody>
</table>

TFT IPv6 IE Type #2: This is the authorized IPv6 TFT object during a QoS-Check operation.
### 11.3.3.22 VSNP Forward Link Compression Info

This TLV contains the compression information negotiated for each PDN connection in the direction HSGW to UE. This context parameter shall be transferred from the S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDN-ID-1</td>
<td>Count-1</td>
</tr>
<tr>
<td>Compression-1-n</td>
<td>PDN-ID-2</td>
</tr>
<tr>
<td>...</td>
<td>Compression-2-n</td>
</tr>
<tr>
<td>Compression-3-1</td>
<td>...</td>
</tr>
<tr>
<td>PDN-ID-m</td>
<td>Count-m</td>
</tr>
<tr>
<td>Compression-m-n</td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF16

Length: ≥ 4 octets

PDN-ID-k: 8 bits - The PDN Identifier assigned to an APN.

Count-k: 8 bits - The count of following octets that comprise the context information for a single compression protocol, i.e., the count of octets inclusive of Compression-k-1 to Compression-k-n. The binary value contained in this field shall be ≥ 2.

Compression-k-j: size is indicated in the Count-k field.

Following the Count-k octet, the next two octets encode the protocol type with any remaining octets used for parameters specific to that protocol type. Allowed protocol types are:

- 0x0003 – ROHC small-CID. Coding of the specific parameters shall follow RFC 3241 [59].

Note: If multiple compression protocols are defined for a given APN, the PDN-ID may be repeated within this TLV and followed by the context information for another compression protocol.
### 11.3.3.23 VSNP Reverse Link Compression Info

This TLV contains the compression information negotiated for each PDN connection in the direction UE to HSGW. This context parameter shall be transferred from the S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDN-ID-1</td>
<td>Count-1</td>
</tr>
<tr>
<td>Compression-1-n</td>
<td>PDN-ID-2</td>
</tr>
<tr>
<td>…</td>
<td>Compression-2-n</td>
</tr>
<tr>
<td>Compression-3-1</td>
<td>…</td>
</tr>
<tr>
<td>PDN-ID-m</td>
<td>Count-m</td>
</tr>
<tr>
<td>Compression-m-n</td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF17  
Length: ≥ 4 octets  
PDN-ID-k: 8 bits - The PDN Identifier assigned to an APN.  
Count-k: 8 bits - The count of following octets that comprise the context information for a single compression protocol, i.e., the count of octets inclusive of Compression-k-1 to Compression-k-n. The binary value contained in this field shall be ≥ 2.  
Compression-k-j: size is indicated in the Count-k field.  
Following the Count-k octet, the next two octets encode the protocol type with any remaining octets used for parameters specific to that protocol type. Allowed protocol types are:  
0x0003 – ROHC small-CID. Coding of the specific parameters shall follow RFC 3241 [59].  
Note: If multiple compression protocols are defined for a given APN, the PDN-ID may be repeated within this TLV and followed by the context information for another compression protocol.
### 11.3.3.24 PDN Info Extended

This TLV contains PDN connection specific common info and shall be used only if MUPSAP is supported at the S-HSGW. This TLV shall be repeated for each PDN connection at the S-HSGW. This context parameter shall be transferred from S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Table 49</th>
<th>PDN Info Extended TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>PDN ID</td>
<td>User Context Identifier</td>
</tr>
<tr>
<td>APN</td>
<td></td>
</tr>
</tbody>
</table>

- **Type:** 0xFF18
- **Length:** variable
- **PDN ID:** This field carries 1 octet PDN Identifier.
- **User Context Identifier:** This field carries 1 octet User Context Identifier.
- **PDN Connection ID:** This field carries the 1 octet PDN Connection ID that was received from the P-GW.
- **APN Length:** This field indicates the length of the APN field in octets.
- **APN:** This field carries the Access Point Name that is associated with the PDN Identifier. See TS 24.302 [26].

### 11.3.3.25 Forward Link VSNP-Extend-Code Info

This TLV contains the VSNP Extend Code information negotiated for each APN connection in the direction HSGW to UE. This context parameter shall be transferred from the S-HSGW to the T-HSGW only in the case of full context transfer.

<table>
<thead>
<tr>
<th>Table 50</th>
<th>Forward Link VSNP Extend Code Info TLV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>PDN-ID-1</td>
<td>VSNP-Extend-Code</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>PDN-ID-n</td>
<td>VSNP-Extend-Code</td>
</tr>
</tbody>
</table>
Type: 0xFF19
Length: ≥ 4 octets
PDN-ID-k: 8 bits - The PDN Identifier assigned to an APN.
VSNP-Extend-Code: 8 bits – The Forward Link VSNP Extend Code negotiated for that APN.

### 11.3.3.26 Reverse Link VSNP-Extend-Code Info

This TLV contains the VSNP Extend Code information negotiated for each APN connection in the direction UE to HSGW. This context parameter shall be transferred from the S-HSGW to the T-HSGW only in the case of full context transfer.

#### Table 51 Forward Link VSNP Extend Code Info TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>PDN-ID-1</th>
<th>VSNP-Extend-Code</th>
<th>PDN-ID-2</th>
<th>VSNP-Extend-Code</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type: 0xFF1A
Length: ≥ 4 octets
PDN-ID-k: 8 bits - The PDN Identifier assigned to an APN.
VSNP-Extend-Code: 8 bits – The Reverse Link VSNP Extend Code negotiated for that APN.

### 11.3.3.27 User supplied Mobile Identity for emergency PDN connection

This TLV is of the following format. It carries the Mobile Identity of the user sent from the UE to HSGW using Mobile Identity Configuration Option of the VSNCP Configure Request message during Emergency PDN connection. This context parameter shall be transferred from S-HSGW to the T-HSGW in the case of full context transfer if an emergency PDN connection is active.

#### Table 52 User supplied Mobile Identity for emergency PDN connection

| Type | Length | Mobile Identity |
|------|--------|----------------|----------------|
| 0x0  |        |                |

Type: 0xFF1B
Length: ≤ 11 octets
Mobile Identity: This is the Mobile Identity supplied by the UE using Mobile Identity Configuration Option of the VSNCP Configure Request message during Emergency PDN connection. The format of this field is set to the value portion of the “Mobile Identity” IE as defined in Section 10.5.1.4 of [3GPP TS 24.008] [25]. The type of identity shall be set to ‘001’ (IMSI) or to ‘010’ (IMEI) as sent by the UE in the VSNCP Configuration Request message.

11.3.4 H2 Stage 3

11.3.4.1 H2 Downlink Data

Each downlink data packet shall be encapsulated in an IPv4 or IPv6 packet with a GRE header. The key present bit of the GRE header is set to 1, and the H2 downlink GRE key is included in the key field. The source IP address of the packet is set to the S-HSGW H2 IP address and the destination IP address is the T-HSGW H2 IP address. The H2 downlink GRE key identifies the packet as a downlink packet that belongs to the UE. The protocol type field of the GRE header shall be set to “Unstructured Byte Stream” (88 81H – ref. A.S0017-D [5]).

The payload packet is always preceded with an 8 bit field that includes the PDN-ID with the 0 bit as the most significant followed by the IPv6/IPv4 payload packet. The outline of the packet is shown in:

Table 53  H2 Downlink Data Packet

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘0000’</td>
<td>PDN-ID</td>
<td>Downlink IP Packet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PDN-ID: This is the PDN-ID for the PDN connection for this downlink data packet

Downlink IP Packet: This is the user’s IP packet received on a PDN connection from the P-GW and being forwarded from the S-HSGW to the T-HSGW and then to the UE.

11.3.4.2 H2 Uplink Data

Each uplink data packet shall be encapsulated in an IPv4 or IPv6 packet with a GRE header. The key present bit of the GRE header is set to 1, and the H2 uplink GRE key is included in the key field. The source IP address of the packet is set to the S-HSGW H2 IP address, and the destination IP address is the T-HSGW H2 IP address. The H2 uplink GRE key identifies the packet as an uplink packet that belongs to the UE. The protocol type field of the GRE header shall be set to “Unstructured Byte Stream” (88 81H – ref. A.S0017-D [5]).

The payload packet is always preceded with an 8 bit field that includes the SR_ID associated with the A10 connection over which this uplink data packet was received with the 0 bit as the most significant followed by the payload packet. The outline of the packet is shown in Table 17.
Table 54 H2 Uplink Data Packet

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR_ID</td>
<td>A10 GRE Payload</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| ... | ...

SR_ID: This is the SR_ID associated with the A10 connection over which this uplink data packet was received.

A10 GRE Payload: This is the GRE payload received on a specific A10 connection at the S-HSGW and being forwarded from the S-HSGW to the T-HSGW.

11.3.5 HSGW Relocation Procedure Stage 3

The HSGW shall follow the procedure described in this section during an inter-HSGW relocation with context transfer.

11.3.5.1 Update Location Procedure

11.3.5.1.1 General

The Update Location Procedure is used between the HSGW and the 3GPP2 AAA Proxy to update location information in the 3GPP2 AAA Proxy. The procedure is invoked by the HSGW and is used to inform the 3GPP2 AAA Proxy about the identity of the HSGW currently serving the user.

This procedure is mapped to the commands Update Location Request/Answer (ULR/ULA) in the Diameter application.

Table 55 specifies the involved information elements for the request.

Table 56 specifies the involved information elements for the answer.
### Table 55  Update Location Request

<table>
<thead>
<tr>
<th>Information Element Name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
<td>User-Name (See IETF RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [19], clause 2.2.</td>
</tr>
<tr>
<td>RAT Type</td>
<td>RAT-Type</td>
<td>M</td>
<td>This Information Element contains the radio access type the UE is using. See section 7.3.13 of 3GPP TS 29.272 [33] for details.</td>
</tr>
<tr>
<td>Supported Features</td>
<td>Supported-Features (ref. 3GPP TS 29.229 [32])</td>
<td>O</td>
<td>This is a Grouped AVP. The Vendor-Id sub AVP shall be set to SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535). The Feature-List-ID sub AVP shall be set to 1 (&quot;Query Group&quot;); and the Feature-List sub AVP shall have bit 1 set indicating the ‘HSGWReloc’ (HSGW Relocation) feature.</td>
</tr>
</tbody>
</table>

### Table 56  Update Location Answer

<table>
<thead>
<tr>
<th>Information Element Name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Result-Code / Experimental-Result</td>
<td>M</td>
<td>This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP is defined in section 7.4 of 3GPP TS 29.272 [33]</td>
</tr>
<tr>
<td>Supported Features</td>
<td>Supported-Features (ref. 3GPP TS 29.229 [32])</td>
<td>C</td>
<td>This is a Grouped AVP. The Vendor-Id AVP shall be set to SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535). The Feature-List-ID sub AVP shall be set to 1 (“Query Group”); and the Feature-List sub AVP shall have the bits set for the complete set of features supported by the 3GPP2 AAA Proxy/Server.</td>
</tr>
</tbody>
</table>

### 11.3.5.1.2  Behaviour of the HSGW

The HSGW shall make use of this procedure to update the HSGW identity stored in the 3GPP2 AAA Proxy. The HSGW uses this procedure during Intra-eHRPD Handoff with the HSGW Relocation procedure using Context Transfer as defined in this specification.

If both the HSGW and the 3GPP2 AAA Proxy/Server support the Pi*3GPP2 Diameter Application and the HSGW needs to update the HSGW identity stored in the 3GPP2 AAA Proxy, the HSGW initiates the HSGW Relocation procedure by sending a Update Location Request (ULR) command to the 3GPP2 AAA Proxy. If the HSGW does not know if the ‘HSGWReloc’ feature is supported by the 3GPP2 AAA Proxy, the ULR command shall include the Supported-Features AVP with the ‘M’ bit set, the Feature-List-ID sub AVP set to 1 (“Query Group”), and the Feature-List sub AVP shall have bit 1 set indicating a request for the HSGW Relocation procedure.

If a Update Location Answer (ULA) command is received with the Experimental-Result-Code AVP set to DIAMETER_ERROR_FEATURE_UNSUPPORTED, the HSGW shall abort the HSGW Relocation procedure.

When receiving an Update Location Answer from the 3GPP2 AAA Proxy, the HSGW shall check the result code. If it indicates other than success the HSGW shall take corrective action based on the received result code.
11.3.5.1.3 Behaviour of the 3GPP2 AAA Proxy/Server.

On receiving the Update Location Request (ULR) command, if the Supported-Feature AVP is received, the 3GPP2 AAA Proxy/Server shall do one of the following:

- If it supports all the features indicated in the Supported-Features AVP, the 3GPP2 AAA Proxy/Server shall include the Supported-Features AVP in the ULA command, identifying the complete set of features that it supports for the Pi*3GPP2 Diameter Application.

- If it does not support all the features indicated in the Supported-Features AVP, the 3GPP2 AAA Proxy/Server shall return the ULA command with the Experimental-Result-Code AVP set to DIAMETER_ERROR_FEATURE_UNSUPPORTED and shall include the Supported-Features AVP identifying the complete set of features that it supports for the Pi*3GPP2 Diameter Application.

- If it does not support the Supported-Features AVP, it shall return the ULA command with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED and a Failed-AVP containing the Supported-Features AVP as received in the ULR command.

If the 3GPP2 AAA Proxy/Server includes the Supported-Features AVP in the Update Location Answer (ULA) command, the Supported-Features AVP shall have the ‘M’ bit cleared. In this Grouped AVP, the Feature-List-ID sub AVP shall be set to 1 “Query Group”; and the Feature-List sub AVP shall have bits set for the complete set of features supported by the 3GPP2 AAA Proxy/Server.

When receiving a Update Location Request the 3GPP2 AAA Proxy/Server shall check whether the IMSI is known. If it is not known, a Result Code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.

When the 3GPP2 AAA Proxy/Server receives the Update Location Request, it shall send a Cancel Location Request (CLR; see 7.3.2.1) to the source HSGW and replace the stored HSGW-Identity with the received value (the HSGW-Identity is received within the Origin-Host AVP).

If the 3GPP2 AAA Proxy/Server successfully processes the received Update Location Request, the 3GPP2 AAA Proxy/Server shall respond with a Update Location Answer with result code success. The 3GPP2 AAA Proxy/Server may send the Update Location Answer before receiving the Cancel Location Answer from the source HSGW.

11.3.5.2 Cancel Location Procedure

11.3.5.2.1 General

The Cancel Location procedure shall be invoked by the 3GPP2 AAA Proxy/Server. It is used between the 3GPP2 AAA proxy/Server and the HSGW to delete a subscriber’s session information due to intra-eHRPD HSGW relocation.

This procedure is mapped to the commands Cancel Location Request/Answer (CLR/CLA) in the Pi*3GPP2 Diameter application specified in section 6.3.
Table 57 specifies the involved information elements for the Cancel Location Request.

Table 58 specifies the involved information elements for the Cancel Location Answer.

Table 59 specifies the 3GPP2 Diameter AVP defined for the Pi*3GPP2 Diameter application, the AVP Code value, type, possible flag values and whether or not the AVP may be encrypted.

<table>
<thead>
<tr>
<th>Information Element Name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
<td>User-Name (See IETF RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [19], clause 2.2.</td>
</tr>
<tr>
<td>3GPP2-Cancellation-Type(See Section 6.3)</td>
<td>Cancellation-Type</td>
<td>M</td>
<td>Defined values that can be used are: HSGW-Location-Update-Procedure (value=0)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Element Name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Result-Code / Experimental-Result</td>
<td>M</td>
<td>This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP is defined in section 7.4 of 3GPP TS 29.272 [33].</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Value Type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP2-Cancellation-Type</td>
<td>5535/56</td>
<td>Enumerated</td>
<td>M, V</td>
<td></td>
<td></td>
<td></td>
<td>NO</td>
</tr>
</tbody>
</table>

11.3.5.2.2 Behavior of the HSGW

When receiving a Cancel Location Request the source HSGW shall check whether the user name is known. If it is not known, a result code of DIAMETER_SUCCESS is returned.

If it is known and the value of the 3GPP2-Cancellation-Type AVP is HSGW-Location-Update-Procedure, the source HSGW shall complete any inter-HSGW context transfer procedures and then delete all the user session contexts.
11.3.5.2.3 Behavior of the 3GPP2 AAA Proxy/Server

The 3GPP2 AAA Proxy/Server shall make use of this procedure when it detects that the UE has moved to a new HSGW.

If the UE moved to a new HSGW, the 3GPP2 AAA Proxy/Server shall include the 3GPP2 Cancelation Type AVP with a value of "HSGW-Location-Update-Procedure" when sending Cancel Location Request to the source HSGW.

11.3.5.3 Pi*3GPP2 Diameter Application Commands

The ABNF of the ULR and ULA are defined in sections 6.3.1.1 and 6.3.1.2. The ABNF of the CLR and CLA are defined in sections 6.3.1.3 and 6.3.1.4.
**12 Handoff from E-UTRAN to eHRPD**

This section provides E-UTRAN to eHRPD handoff flows for both non-roaming and roaming scenarios.

NOTE: This specification supports handoff to and from E-UTRAN, where the S-GW in the EPS is connected to the P-GW via either GTP or PMIPv6.

There are two types of handoff from E-UTRAN to eHRPD, optimized handoff and non-optimized handoff.

Section 12.1 provides E-UTRAN to eHRPD optimized handoff flows. Section 12.2 provides E-UTRAN to eHRPD non-optimized handoff flows.

- Optimized handoff uses the S101 interface between the E-UTRAN and eHRPD access networks to allow the UE to establish and maintain the eHRPD radio session and HSGW context. This minimizes delay before the UE can send and receive packets after moving to eHRPD. For active mode optimized handoff, the HSGW establishes S103 interface (if supported) with S-GW for forwarding the packets from E-UTRAN to eHRPD.

- Non-optimized handoff generally requires the UE to establish an eHRPD radio session and HSGW context after moving to eHRPD. However, it is possible that the HSGW has partial context for the UE, which somewhat reduces the delay before the UE can send and receive packets.

If the UE performs an initial attach on E-UTRAN, then the UE shall delete any eHRPD PPP context (i.e., LCP, EAP-AKA', VSNCP and RSVP) it may have stored.

For optimized handoff, when the UE accesses eHRPD via the E-UTRAN radio and the S101 tunnel, it shall send a VSNCP Configure-Request message with attach-type set to handover to the HSGW for each of its existing PDN connections in the EPS system that it intends to maintain in eHRPD.

For non-optimized handoff, when the UE moves to the eHRPD access network, the UE shall send a VSNCP Configure-Request message with attach type set to handover to the HSGW for each PDN connection it wants to maintain in eHRPD.

When the UE sends a VSNCP Configure-Request message as described above, one of two outcomes will occur:

1. In the case the HSGW has full or partial context for the UE as described in section 9.1.9, the HSGW shall respond with VSNCP Configure-Ack as described in section 9.1.4. The UE then configures dedicated bearers, for any flows that the HSGW has not previously established. See sections 12.2.1 and 12.2.2.

2. In the case the HSGW has no context for the UE, the HSGW shall respond with LCP Configure-Request (if not already sent). In this case, the UE and network shall perform LCP negotiation, CCP negotiation as needed, authentication, and then establish PDN connections and dedicated bearers as described in item (1) of this list.
12.1 Optimized Handoff E-UTRAN to eHRPD

The flows for the pre-registration and E-UTRAN to eHRPD handoff phases of optimized handoff are shown in the following subsections.

12.1.1 eHRPD Pre-registration via E-UTRAN

The following flow describes the use of the S101 interface to tunnel eHRPD signaling between the UE and the eAN/ePCF.

![Diagram of eHRPD Pre-registration via E-UTRAN]

**Figure 53** eHRPD Pre-registration via E-UTRAN

1. The UE is initially attached to the E-UTRAN. The UE acquires IPv4 address(es) and/or IPv6 prefix(es). Data flows between the UE and the P-GW(s) through the eNodeB and the S-GW.
2. Based on a Radio Layer trigger, the UE decides to initiate a pre-registration procedure with potential target eHRPD access. It is assumed that an S101 signalling relationship exists between the MME and eAN/ePCF.

3. The UE initiates the establishment of a new session in the eHRPD system through the S101 tunnel.

4. If RAN-level authentication is required, the UE establishes an AN-PPP connection with the eAN/ePCF and performs RAN-level authentication using the A12 interface. For details refer to A.S0022 [4].

5. The eHRPD eAN/ePCF establishes the main A10 connection with the HSGW by exchanging A11-Registration Request/Registration Reply messages. The A11-Registration Request message contains an indication that the access is occurring through the S101 tunnel. For details refer to A.S0022 [4]. This information is used by the HSGW in step 7 to defer interaction with the P-GW. The UE and HSGW initiate the PPP connection establishment procedure.

6. a-b. The UE performs user authentication and authorization in the eHRPD access system using EAP-AKA'. The EAP-AKA’ messages are transferred between the UE and HSGW over PPP. The EAP authenticator resides in the HSGW. The detailed EAP-AKA’ authentication flows are specified in Section 4.2. The 3GPP AAA server authenticates and authorizes the UE for access in the eHRPD system. The 3GPP AAA server queries the HSS and returns the subscription profile, and APN and P-GW address pair for each PDN connection to the eHRPD system in this step. The 3GPP AAA server also returns the NAI to be used to identify the UE in Proxy Binding Update message.

6c. The HSGW stores the information received from the 3GPP AAA/HSS server.

7. The UE exchanges VSNCP messages with the HSGW for each PDN connection (See section 5.4.1 for details) that it currently has attachments to within E-UTRAN and that it wants to maintain on eHRPD. The UE sets the Attach Type to “handoff” in the VSNCP Configure-Request message. Also, the UE includes the IP address(es) it obtained via LTE in the VSNCP Configure-Request message. If the PDN Type is IPv6 or IPv4v6, the UE includes the IPv6 HSGW Link Local Address IID option and sets the value to all zeros in the VSNCP Configure-Request message. The HSGW includes the IPv6 HSGW Link Local Address IID option and sets the value to the interface ID of the HSGW link local address in the VSNCP Configure-Ack message. Interactions occur among the HSGW and PCRF per 3GPP specifications (TS23.402 [23] section 9.3.1). The HSGW exchanges Gateway Control Session Establishment/Ack messages with the hPCRF to obtain QoS policy rules required to perform bearer binding update for all the active IP flows. As shown in the figure for the roaming scenario, the policy interactions between the hPCRF in the HPLMN and the HSGW are relayed via the vPCRF in the VPLMN.

NOTE: The HSGW defers interaction with the P-GW until the UE arrives in eHRPD, at which time it sends a PBU to the P-GW to complete the PDN connection.

8. The network initiates resource reservation procedures to establish all dedicated bearers.

At this point the UE is registered in the eHRPD access system and it has been authenticated by the AAA/HSS.

9. It may become necessary to modify the eHRPD radio session configuration between the UE and the eAN/ePCF. For example, this may be necessary as a result of moving under the coverage area of a new eAN/ePCF. This is accomplished by eHRPD signalling exchanges between the UE and the eAN/ePCF via S101 tunneling.

10. If any bearer is added, modified, or deleted while the UE is operating on E-UTRAN, similar changes shall be made in the context between the UE and the HSGW. This is accomplished by signaling those changes between the UE and HSGW via S101 tunneling. Likewise, if any PDN connection is added, or deleted while the UE is operating on E-UTRAN, similar changes are made in the HSGW via the use of VSNCP.

10a. If the HSGW receives a VSNCP Configure-Request for a PDN connection for which it does not have a P-GW identity, it obtains that information via an AAR/AAA exchange with the HSS/AAA. If the HSGW already has the corresponding P-GW IP address, or receives it from the HSS/AAA
associated with the VSNCP Configure-Request message, the HSGW exchanges PBU/PBA messages with the P-GW. The exchanges of AAR/AAA and PBU/PBA messages are not shown in the figure.

11. If not already initiated, PCRF interactions due to session maintenance can be initiated by the PCRF or the HSGW. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [20]. The HSGW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [20].
### 12.1.2 Active Mode Optimized Handoff Phase E-UTRAN to eHRPD

It is assumed that either a full pre-registration context, or a partial context has been setup in the HSGW, and PMIP binding is not established.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a.</td>
<td>Decision to handover to eHRPD</td>
</tr>
<tr>
<td>1b.</td>
<td>Handover Request</td>
</tr>
<tr>
<td>1c.</td>
<td>S101 (HRPD Conn. Req., P-GW Address(es), GRE Key(s), APN(s))</td>
</tr>
<tr>
<td>2a.</td>
<td>A11-RRQ (P-GW Address(es), GRE Key(s), APN(s))</td>
</tr>
<tr>
<td>2b.</td>
<td>A11-RRP (HSGW Address, GRE Key(s), APN(s))</td>
</tr>
<tr>
<td>3.</td>
<td>S101 (HRPD TCA, HSGW Address, GRE Key)</td>
</tr>
<tr>
<td>4a.</td>
<td>Create forwarding tunnel (HSGW Address, GRE Key)</td>
</tr>
<tr>
<td>4b.</td>
<td>HRPD TCA</td>
</tr>
<tr>
<td>5.</td>
<td>Indirect data forwarding over S103-U (optional)</td>
</tr>
<tr>
<td>6a.</td>
<td>UE acquires HRPD Radio</td>
</tr>
<tr>
<td>6b.</td>
<td>HRPC TCC</td>
</tr>
<tr>
<td>7a.</td>
<td>A11-RRQ (Active Start)</td>
</tr>
<tr>
<td>7b.</td>
<td>A11-RRP</td>
</tr>
<tr>
<td>8a.</td>
<td>Proxy Binding Update</td>
</tr>
<tr>
<td>8b.</td>
<td>Proxy Binding Update (IPv4 address or IPv6 prefix)</td>
</tr>
<tr>
<td>8c.</td>
<td>Modify IP-CAN Session/Ack</td>
</tr>
<tr>
<td>9.</td>
<td>IP Packets Flowing</td>
</tr>
<tr>
<td>10.</td>
<td>3GPP EPS Resource Release</td>
</tr>
<tr>
<td>11a.</td>
<td>(Optional) HSGW obtains updated list of P-GW identities and PDN connections via AAR/AAA message exchange.</td>
</tr>
</tbody>
</table>

**Figure 54** Active Mode Optimized Handoff E-UTRAN to eHRPD
1a. E-UTRAN receives CDMA measurement reports from the UE and makes a HO decision.

1b. UE sends an HRPD Connection Request message to the E-UTRAN to request an HRPD traffic channel. This request is forwarded to the MME. See TS 23.402 [23] for details.

1c. The MME sends the P-GW address(es) and the associated APNs and the uplink GRE key(s) along with the HRPD Connection Request message to the eHRPD access node over the S101 tunnel.

NOTE: The GRE keys (one for each APN) sent in step 1c are further sent in step 2a to the HSGW, and the HSGW uses them for uplink traffic towards the P-GW after the HO. The same keys are in use between the S-GW and P-GW before the HO. Using the same keys assures that the P-GW can associate the uplink data to the right UE, if the HSGW decides to send uplink data even before the PBA message is received in step 8b (note that the P-GW as defined in TS 23.402 [23] is equipped to receive data with the same GRE key even before updating the binding).

2a. The eHRPD eAN/ePCF allocates the requested radio resources and sends an A11-Registration Request message to the HSGW. In this message the eAN/ePCF includes the P-GW address(es), the associated uplink GRE key(s) received in step 1c and the indicator that the UE is communicating via a tunnel (ref. Tunnel Mode indicator in A.S0022 [4]).

2b. The HSGW responds with an A11-Registration Reply containing a forwarding address (i.e., HSGW IP address, GRE key(s), and associated APN(s)).

3. In response to the HRPD Connection Request message received in step 1c, the eHRPD eAN/ePCF sends the HRPD Traffic Channel Assignment (TCA) message in an S101 message to the MME. The S101 message also carries the HSGW IP address, GRE key(s) for data forwarding, and associated APN(s).

4a. The MME configures resources for indirect data forwarding and signals the HSGW IP address and GRE key(s) to the S-GW. The S-GW confirms data forwarding resources.

4b. The MME forwards the HRPD TCA message embedded in the S101 message to the E-UTRAN which forwards it to the UE over the airlink.

5. E-UTRAN may return downlink IP packets back to the S-GW to be sent to the HSGW over the S103 interface. The HSGW will perform any necessary processing on the IP packets and forward them over the appropriate A10 connection to the eAN/ePCF.

6a. L2 attach is completed (i.e., the UE acquires the eHRPD radio).

6b. The UE sends a Traffic Channel Completion (TCC) message to the eHRPD eAN/ePCF.

7a. The eHRPD eAN/ePCF sends an A11-Registration Request carrying an Active Start airlink record and the indicator that the UE is now operating on the eHRPD radio to the HSGW.

7b. The HSGW responds to the eHRPD eAN/ePCF with an A11-Registration Reply.

In the case of pre-registration with one or more PDN connections already established at the HSGW, steps 8 to 10 will take place. Otherwise, only step 8d will take place, and the HSGW waits for the UE to setup PDN connections by sending VSNCP-Configure-Request messages for each PDN connection at step 11.

8a. Triggered by step 7a, the HSGW/MAG sends a PBU(s) to establish a PMIPv6 tunnel(s) with the P-GW(s) the UE is associated with. The HSGW uses the NAI received in the Mobile-Node-Identifier AVP upon successful authentication to identify the UE.

8b. The P-GW processes the PBU and updates the binding cache entry for the UE. The same IP address(es) or prefix(es) are assigned to the UE. The P-GW/LMA sends a PBA message to the HSGW/MAG, including the IP address(es)/prefix(es) allocated for the UE. The PMIPv6 tunnel is now setup.

8c. The P-GW requires configuration for enforcing policy, the P-GW sends a Modify IP-CAN session message to the hPCRF. The P-GW has requested an IP-CAN session, the hPCRF responds to the
P-GW with a Modify IP-CAN session Ack message. This message includes the Policy and Charging rules provisioned into the P-GW.

Note: Steps 8a to 8c are repeated for each PDN connection that is to be established.

8d. The eHRPD eAN/ePCF signals handoff completion to the MME to confirm HO completion, and receives an acknowledgement.

9. L3 attach is completed and the UE can now send/receive packets to/from the eHRPD access network.

10. The E-UTRAN system, including eNodeB, MME, S-GW, and P-GW release resources, including sending a PMIPv6 BRI message from the P-GW to the S-GW as specified in TS 29.275 [35]. See also TS 23.402 [23].

11. If the UE had not completed PDN connection and bearer addition/deletion while on E-UTRAN, the UE completes those activities over the eHRPD radio. In the case of pre-registration with partial context, EPS resources including eNodeB, MME, S-GW are released when the UE sets up the PDN connections over eHRPD. If any PDN connection is added, modified, or deleted while the UE is operating on E-UTRAN, similar changes are made in the HSGW via the use of VSNCP.

11a. If the HSGW receives a VSNCP Configure-Request for a PDN connection for which it does not have a P-GW identity, it obtains that information via an AAR/AAA exchange with the HSS/AAA. If the HSGW already has the corresponding P-GW IP address, or receives it from the HSS/AAA associated with the VSNCP Configure-Request message, the HSGW exchanges PBU/PBA messages with the P-GW. The exchanges of AAR/AAA and PBU/PBA messages are not shown in the figure.
12.1.3 Idle Mode Optimized Handoff from E-UTRAN to eHRPD

This procedure is used in the case the UE has a dormant PPP session in the target HSGW through the pre-registration procedure. It is assumed that the UE has pre-registered with eHRPD, that the PPP inactivity timer is still running, and that the HSGW has full context for the UE (except for PMIP bindings).

Figure 55 Idle Mode Optimized Handoff from E-UTRAN to eHRPD

1. The UE is attached to the E-UTRAN network and stays in ECM_IDLE state. The UE has a dormant eHRPD session in the target eHRPD eAN through the pre-registration procedure.
2. The UE is in idle mode. Based on some trigger, the idle UE decides to perform cell re-selection to the eHRPD eAN. Note, the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network (including as soon as the UE has completed pre-registration).
3. The UE follows eHRPD procedures to inform the eAN the UE has performed an inter-technology idle mode mobility event and is now tuned to eHRPD.
4. The eAN sends an A11-Registration Request for all A10s. This A11-Registration Request contains the “tunnelled mode indicator” set to ‘0’ to indicate to the HSGW that the UE is operating on the eHRPD radio. If the Tunnel Mode Indicator is not present, then the HSGW shall always assume that the UE is operating on the eHRPD radio, and thus all PMIP bindings for the UE should be established.

5–6. Upon receipt of the A11-Registration Request message for eHRPD session with nonzero lifetime timer and the Tunnel Mode Indicator is set to ‘0’ or is not present, the HSGW determines that it does not have a PMIPv6 binding(s) for this UE and exchanges PBU/PBA messages with the appropriate P-GW(s). The UE address information in PMIPv6 PBA returns the IP Address assigned to the UE. At this point the user plane is switched in the P-GW towards the eHRPD access network via the HSGW. The P-GW updates the HSS/AAA using an exchange of AAR/AAA messages (not shown in the figure).

6a-6b. The P-GW sends an Indication of IP-CAN Session Modification message to the PCRF and PCRF acknowledges. Since steps 6 and 6a are both triggered by the PBU in step 5, steps 6 and 6a may occur in parallel.

NOTE: For multiple PDN connections, steps 5-6 and 6a-6b are performed for each PDN connection.

7. The HSGW sends A11-Registration Reply to acknowledge the eHRPD access. The A11-Registration Request message is validated and, if new A10 connections are being established, the HSGW accepts the A10 connections by returning an A11-Registration Reply message with an accept indication. This step may occur any time after step 4.

8. At any time after step 6, the P-GW shall initiate resource allocation deactivation procedure in E-UTRAN as defined in TS 23.402 subclause 5.6.2.2 [23].

9. The UE is now attached to eHRPD.

10. If the UE had not completed PDN connection and bearer addition/deletion while on E-UTRAN, the UE completes those activities over the eHRPD radio. If any PDN connection is added, modified, or deleted while the UE is operating on E-UTRAN, similar changes are made in the HSGW via the use of VSNCP.

10a. If the HSGW receives a VSNCP Configure-Request for a PDN connection for which it does not have a P-GW identity, it obtains that information via an AAR/AAA exchange with the HSS/AAA. If the HSGW already has the corresponding P-GW IP address, or receives it from the HSS/AAA associated with the VSNCP Configure-Request message, the HSGW exchanges PBU/PBA messages with the P-GW. The exchanges of AAR/AAA and PBU/PBA messages are not shown in the figure.
12.2 Non-Optimized Handoff

The flows for non-optimized handoff are shown in the following sections.

12.2.1 Non-Optimized Handoff from E-UTRAN to eHRPD – Partial Context

The flow in Figure 56 assumes that the UE had previously registered on eHPRD, and that the UE Context Maintenance timer is still running at the HSGW (i.e., the A10 session, LCP and authentication session info are still maintained at the HSGW).

When the UE returns to eHPRD to resume the existing eHPRD session, the PDN connections are created per the context that the UE had on E-UTRAN. Likewise, bearers are established to match those that were available on E-UTRAN.

Note also that the bearer re-establishment procedures in step 13 may occur in parallel, within the rules of the HRPD radio interface, C.S0024 [7].

Figure 56 Non-Optimized Handoff from E-UTRAN to eHPRD – Partial HSGW Context
In this flow, it is assumed that the UE is returning to the same HSGW and eHRPD RAN that hold the context for the UE. This assumption makes it possible to avoid showing the removal of the A10 connections to the S-eAN/ePCF by the S-HSGW, as well as context transfer between HSGWs. Those procedures are defined in A.S0008-C [1] and A.S0009-C [2], and in section 11 of this document.

1. The UE and the eAN/ePCF reconnect the existing eHRPD session.
2. The ePCF recognizes that the A10 session associated with the UE is available, and sends an “Active Start” indication in an A11-Registration Request message to the HSGW.
3. The HSGW responds with an A11-Registration Reply message.
4. The HSGW retrieves the UE context from the HSS/AAA, including the IP address(es) of P-GW(s) currently in use by all PDN connections for the UE.

Steps 5-12 are repeated for each additional PDN connection that the UE must re-establish.
5. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, PDN Type, APN, PDN Address, Protocol Configuration Options, and Attach Type = “Handoff Attach”. The User Context Identifier is also included if MUPSAP is supported. When known, PDN Type indicates the UE IP version capability (IPv4, IPv4/IPv6, IPv6), which is the capability of the IP stack associated with the UE. The Protocol Configuration Options indicates whether the UE supports network initiated bearers.
6. The HSGW performs the Gateway Control Session Establishment procedure with the PCRF (see TS 23.203 [21]). As part of this step, the PCRF sends the QoS rules and events to the HSGW.
7. The HSGW sends a PMIP Binding Update to the P-GW in order to update the registration see TS 29.275 [35]. If MUPSAP is supported, the HSGW includes the PDN Connection ID information element in the PBU message.
8. The P-GW performs a PCRF interaction to retrieve the QoS policy parameters.
9. The P-GW responds with a PBA message to the HSGW see TS 29.275 [35].
10. The HSGW sends a VSNCP Configure-Ack (PDN-ID, User Context Identifier if the PDN Connection ID information element received in the PBA message, APN, PDN Address, PCO, and Attach Type) message to the UE over the main service connection. The Protocol Configuration Options parameter may indicate the Selected Bearer Control Mode.

NOTE: If dynamic policy is not supported, the Selected Bearer Control Mode is “MS-only”.
11. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID and may include the IPv4 Default Router Address if an IPv4 address is to be assigned either immediately or deferred.
12. The UE responds with a VSNCP Configure-Ack message.

Step 13 is repeated as necessary until all bearers for all PDN connections are re-established.
13. Bearers for a PDN connection are re-established on eHRPD based on the Selected Bearer Control Mode:
   13a.) If the Selected Bearer Control Mode is “MS-only”, the HSGW assumes that the UE will re-establish all bearers. The UE performs UE requested bearer resource allocation – section 4.5.4.1.1 for all bearers. If there is no change to the QoS info, steps 6 and 7 are not performed as the QoS info and service connections are retained. As part of re-establishing bearers, one or more bearers may need to be deleted with the RAN. The UE performs standard HRPD procedures to remove the corresponding Reservations.
   13b.) If the Selected Bearer Control Mode is “MS/NW”, the HSGW re-establishes all bearers. The HSGW performs NW initiated dedicated bearer setup – section 4.5.3.1 for all bearers. If there is no change to the QoS info steps 4 and 5 are not performed as the QoS info and service connections are retained. As part of re-establishing bearers, one or more bearers may need to be deleted.
Note: It is FFS how the stale bearers get deleted in the case the Selected Bearer Control Mode is “MS/NW”.

Note: It is FFS how the HSGW informs the UE in “MS/NW” mode about which IP Flows the UE shall initiate.
12.2.2 Non-Optimized Handoff – Null HSGW Context

This procedure is used in the case there is null context in the target HSGW for the UE. For simplicity, it is assumed that the eHRPD session context already is available to the eAN/ePCF to which the UE performs the handoff. The UE had previously been on eHRPD, and does not use the S101 tunneling mechanism to pre-register on eHRPD.

1. Attached to E-UTRAN (UE does not use S101 to pre-register)

2. UE Decision to perform Cell re-selection

3. eHRPD Traffic Channel Assignment

4. A11-RRQ

5. A11-RRP

6. VSNCP Configure-Request

7. The HSGW determines that it has no context saved for this UE. The UE, RAN, HSGW, and Core Network perform steps 6 through 17 of the flow in section 5.4.1 with Attach Type = Handover Attach.

8. DHCP Discover (Optional)

9a. (optional) Router Solicitation

9b. (conditional) Router Advertisement

10. The UE, RAN, HSGW, and PCRF establish dedicated bearers (IP flows) based on the Bearer Control Mode:

10a. If the selected BCM = NW-Initiated, then the UE, RAN, HSGW, and Core Network perform the procedures in section 4.5.3.1 to establish dedicated bearers (IP flows) using Network Initiated QoS.

10b. If the selected BCM = UE-Initiated, then the UE, RAN, HSGW, and Core Network perform the procedures in section 4.5.4.1.1 to establish dedicated bearers (IP flows) using UE Initiated QoS.

**Figure 57 Non-Optimized Handoff – Null HSGW Context**

1. It is assumed that the UE has an existing eHRPD session with the eAN/ePCF, and that the HSGW has no saved context for the UE. The UE does not use S101 to pre-register with eHRPD. When the UE re-attaches to eHRPD, it needs to establish complete context with the HSGW.

2. The UE is in LTE. Based on some trigger, the UE decides to perform cell re-selection to the eHRPD AN. Note: the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network. The eNB may be involved in redirecting the UE to eHRPD.

3. The UE follows eHRPD procedures to establish connection with the eAN.

4. Since the eHRPD session is in this subnet, and since no A10 connections exist, the eHRPD eAN/ePCF sends an A11-Registration Request to establish all A10s. This A11-Registration Request contains the Tunnel Mode Indicator set to ‘0’ to indicate to the HSGW that the UE is
operating on the eHRPD radio. If the Tunnel Mode Indicator is not present, then the HSGW always assumes that the UE is operating on the eHRPD radio.

5. Triggered by step 4 the HSGW sends A11-Registration Reply to acknowledge the eHRPD access. The A11-Registration Request message is validated.

6. Since the UE had previously been on eHRPD and had not used S101 to pre-register, the UE sends a VSNCP Configure-Request to the HSGW. The User Context Identifier configuration option is also included if MUPSAP is supported. The UE makes the assumption that the HSGW has maintained partial context from the previous time that the UE had established context on eHRPD.

7. The HSGW notes that it has no saved context for the UE. The HSGW initiates LCP and the other procedures contained in steps 6 to 17 of the flow in section 5.4.1 to establish PPP, authentication, CCP, and PDN contexts for the UE. This step may occur prior to the VSNCP Configure-Request being sent in step 6.

8. (optional) The UE can now issue a DHCPv4 DISCOVER (optionally with rapid commit option) message on the BE service connection provided the UE requested deferred IP address allocation.

9. 9a. The UE may send a Router solicitation message.
    9b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

10. The UE, RAN, HSGW and PCRF proceed to re-establish dedicated bearers based on the Bearer Control Mode.
    10a. If the selected BCM indicates NW-initiated QoS, then the procedures of section 4.5.3.1 are executed for each dedicated bearer (IP flow) that was setup on LTE.
    10b. If the selected BCM indicates UE-initiated QoS, then the procedures of section 4.5.4.1.1 are executed for each dedicated bearer (IP flow) that was setup on LTE that the UE wishes to establish.
### 12.2.3 Non-Optimized Handoff: No Existing eHRPD Session

This procedure is used in the case there is no eHRPD session in the target evolved HRPD system for the UE.

1. Attached to E-UTRAN (UE does not use S101 to pre-register)

2. UE Decision to perform Cell re-selection

3. Steps 1-7b from the call flow in section 5.4.1

4. VSNCP Configure-Request (PDN-ID, Attach Type = "handover", …)

5. Gateway Control Session Setup

6. PMIP Binding Update (Attach type = "handover")

7. PCRF Interaction

8. PMIP Binding Ack

9. VSNCP Configure-Ack (PDN-ID, …)

10. VSNCP Configure-Request (PDN-ID)

11. VSNCP Configure-Ack (PDN-ID)

Steps 4 - 11 are executed for each PDN connection that must be moved to/establish on eHRPD.

12. DHCP Discover (Optional)

**Figure 58** Non-Optimized Handoff: No Existing eHRPD Session

1. It is assumed that the UE does not have an existing eHRPD session with the eAN/ePCF (thus, the HSGW has no saved context for the UE). The UE does not use S101 to pre-register with eHRPD. When the UE re-attaches to eHRPD, it needs to go through full eHRPD session establishment and establish complete context with the HSGW.

2. The UE is in LTE. Based on some trigger, the UE decides to perform cell re-selection to the eHRPD AN. Note: the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network. The eNB may be involved in redirecting the UE to eHRPD.
3. The UE follows the steps 1 to 7b from the call flow in section 5.4.1 to establish an eHRPD session and a PPP and authentication session with the HSGW.

Steps 4 - 11 are repeated for each additional PDN connection that the UE must move from the LTE system.

4. The UE sends a VSNCP Configure-Request message over the main service connection. The information in the message includes a PDN-ID, User Context Identifier if MUPSAP is supported, PDN Type, APN, PDN Address, Protocol Configuration Options, and Attach Type = “Handover Attach”. When known, PDN Type indicates the UE IP version capability (IPv4, IPv4/IPv6, IPv6), which is the capability of the IP stack associated with the UE. The Protocol Configuration Options indicates whether the UE supports network initiated bearers.

5. The HSGW performs the Gateway Control Session Establishment procedure with the PCRF (see TS 23.203 [21]). As part of this step, the PCRF sends the QoS rules and events to the HSGW.

6. The HSGW sends a Proxy Binding Update to the P-GW in order to update the registration see TS 29.275 [35]. If MUPSAP is supported, the HSGW includes PDN Connection ID information element in the Proxy Binding Update message.

7. The P-GW performs a PCRF interaction to retrieve the QoS policy parameters.

8. The P-GW responds with a PBA message to the HSGW see TS 29.275 [35].

9. The HSGW sends a VSNCP Configure-Ack (PDN-ID, User Context Identifier if the PDN Connection ID information element is received in the PBA message, APN, PDN Address, PCO, and Attach Type) message to the UE over the main service connection. The Protocol Configuration Options parameter may indicate the Selected Bearer Control Mode.

   NOTE: If dynamic policy is not supported, the Selected Bearer Control Mode is “MS-only”.

10. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in RFC 3772 [67]. The message includes the PDN-ID and may include the IPv4 Default Router Address if an IPv4 address is to be assigned either immediately or deferred.

11. The UE responds with a VSNCP Configure-Ack message.

12. (optional) The UE can now issue a DHCPv4 DISCOVER (optionally with rapid commit option) message on the BE service connection provided the UE requested deferred IP address allocation in Step 8.

13. 13a. The UE may send a Router solicitation message.

   13b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6 prefix to the HSGW.

Step 14 is repeated as necessary until all bearers for all PDN connections are established.

14. Bearers for a PDN connection are re-established on eHRPD based on the Selected Bearer Control Mode:

   14a. If the Selected Bearer Control Mode is “MS-only”, the HSGW assumes that the UE will establish all bearers. The UE performs UE requested bearer resource allocation – section 4.5.4.1.1 for all bearers.

   14b. If the Selected Bearer Control Mode is “MS/NW”, the HSGW establishes all bearers. The HSGW performs NW initiated dedicated bearer setup – section 4.5.3.1 for all bearers.
13 Handoff from eHRPD to E-UTRAN

This section includes procedures for handoff from eHRPD to E-UTRAN.

13.1 Non-Optimized Idle Handoff from eHRPD to E-UTRAN

Idle handoff from eHRPD to EUTRAN is shown in Figure 59.

![Diagram of handoff procedure]

Figure 59 eHRPD to E-UTRAN Non-Optimized Idle Handoff
1. The UE performs an idle handoff to E-UTRAN.

2. The P-GW sends a Binding Revocation Indication message to the trusted non-3GPP IP access as defined in RFC 5846 [84], with the Revocation Trigger value set to “Inter-MAG Handover - Different Access Type”.

3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [20].

4. The PCRF responds to the HSGW with Acknowledge Gateway Control Session Termination message.

5. The HSGW returns a Binding Revocation Acknowledgement message to the P-GW. This message can be sent any time after step 2.

6. Anytime after step 2, the HSGW releases the PDN connection contexts and TFTs. The HSGW retains the LCP, CCP, authentication session and A10 session information for the UE, including the QoS information received from the RAN associated with the A10 connections for the UE (including the Flow ID to A10 mapping).

7. The HSGW uses the UE Context Maintainance timer per section 9.1.9 to wait to release the remainder of the session information for the UE.

8. Upon expiry of the UE Context Maintenance timer, the HSGW sends aSession Termination Request to the 3GPP2 AAA Proxy/Server for releasing the Pi* and STa Diameter Sessions.

9. The 3GPP2 AAA Proxy/Server responds with a Session Termination Answer.
   Note: The 3GPP2 AAA Proxy/Server forwards the Session Termination Request to the 3GPP HSS/AAA and responds to the HSGW with a Session Termination Answer on receiving the response from the 3GPP HSS/AAA.

10. Upon expiry of the UE Context Maintenance timer, the HSGW sends an A11-Registration Update message to initiate with the ePCF the release of the A10 session for the UE.

11. The ePCF responds with an A11-Registration Acknowledge message.

12. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release the A10 session.

13. The HSGW responds with A11-Registration Reply with lifetime zero.
13.2 Non-Optimized Redirected Handoff from eHRPD to E-UTRAN

Redirected handoff from eHRPD to E-UTRAN is shown in Figure 60.

**Figure 60 eHRPD to E-UTRAN Non-Optimized Active Handoff**

1. The UE is redirected by the eAN/ePCF to E-UTRAN as per C.S0087 [15].
2. The eAN/ePCF sends an A11-Registration Request message to the HSGW with an Active Stop indication to the HSGW for all IP flows in the activated state associated with the UE.
3. The HSGW acknowledges the A11-Registration Request message.
4. The UE performs the E-UTRAN access procedures shown in TS 23.402 [23] clause 8.2.1.1 or 8.2.1.2.
5. Steps 2 to 13 from the call flow in section 13.1 are performed to release the related eHRPD network resources.
14 BCMCS Support over eHRPD

When the UE is operating in the eHRPD network, BCMCS support over eHRPD is same as BCMCS support over HRPD, refer to [16], [7], [3], and [11]. The UE that supports BCMCS has its RK (Registration Key) provisioned in the CSIM and the 3GPP2 AAA Proxy. TK (Temporary Key) is generated from RK and is sent from the 3GPP2 AAA Proxy to the BCMCS Controller to protect the BAK (BCMCS Access Key) that is distributed to the UE. The BAK is used to generate SK (Session Key) which is used for content encryption and decryption. See [16] for BCMCS key management.

If BCMCS is supported in an eHRPD network, the UE shall follow MS/AT requirements, the eAN shall follow AN requirements, and the BSN shall follow BSN requirements, as specified in [16], [7], [3], and [11]. The requirements for the rest of the network BCMCS entities (e.g., BCMCS Controller) remain the same.
15 Subscriber QoS Profile Configuration Procedure

15.1 General

The procedures in this section shall be supported if the HSGW and the 3GPP2 AAA Proxy/Server support Pi*3GPP2 Diameter Application. It is assumed that the deployment of the Pi*3GPP2 Diameter Application will be consistent throughout the operator network.

The Subscriber QoS Profile Configuration procedure is mapped to the command pair Query Profile Request/Answer (QPR/QPA) defined for the Pi*3GPP2 Diameter Application. Appropriate settings of the Supported-Features AVP within the QPR command are used to query the Subscriber QoS Profile Configuration information.
15.2 Subscriber QoS Profile Information Retrieval – During Authentication

The following figure shows the Subscriber QoS Profile information retrieval procedure during UE authentication. The UE performs authentication with the 3GPP AAA using EAP-AKA’ via the 3GPP2 AAA Proxy/Server and the authenticator in the HSGW as illustrated in section 4.2.5.1. After successful authentication, the HSGW shall initiate the Subscriber QoS Profile Information retrieval procedure with the 3GPP2 AAA Proxy/Server. On validation of such a request for Subscriber QoS Profile information from the HSGW, the 3GPP2 AAA Proxy/Server shall return Subscriber QoS Profile information to the HSGW, if available, over the Pi* reference point.

**Figure 61** Retrieval of Subscriber QoS Profile Information from 3GPP2 AAA – During Authentication

0. User is authenticated with the 3GPP AAA as per EAP-AKA’ authentication procedures. That is, steps 1-23, section 4.2.5.1 have successfully completed.

1. The HSGW invokes the Subscriber QoS Profile Configuration procedure by sending the Query Profile Request (QPR) command to the 3GPP2 AAA Proxy/Server. If the HSGW does not know if the 3GPP2 AAA Proxy/Server supports the SubQoSConfig feature, it includes the Supported-Features AVP within the QPR command, with the Feature-List-ID sub AVP set to 1 (“Query Group”) and feature bit ‘0’ in the Feature-List sub AVP set to ‘1’. The HSGW uses this procedure to retrieve Subscriber QoS Profile information from the 3GPP2 AAA Proxy/Server.

2. On successful processing of the Query Profile Request (QPR) command, the 3GPP2 AAA Proxy/Server responds with a Query Profile Answer (QPA) command with Result Code success (DIAMETER_SUCCESS) that includes the Subscriber QoS Profile information to the HSGW. If Supported-Features AVP is included in the QPR command, the Supported-Features AVP is included in the QPA command also, indicating the complete set of features supported by the 3GPP2 AAA Proxy/Server. The 3GPP2 AAA Proxy/Server uses IMSI-based Network Access Identifier (NAI) as the key to the subscriber profile information.
3. If the HSGW receives the Subscriber QoS Profile information from the 3GPP2 AAA Proxy/Server, it forwards Subscriber QoS Profile information elements to the eAN/ePCF via A11 Session Update procedures. Refer to A.S0008 [1] and A.S0009 [2].
**15.3 Subscriber QoS Profile Information Retrieval – Intra-eHRPD Handoff with HSGW Relocation with Context Transfer**

During intra-eHRPD handoff with HSGW relocation with context transfer, the Subscriber QoS Profile Information context is not transferred from the S-HSGW to the T-HSGW. The T-HSGW shall perform the Subscriber QoS Profile Information retrieval procedures with the 3GPP2 AAA Proxy/Server after receiving the H1-Ack message from the S-HSGW.

**Figure 62 Retrieval of Subscriber QoS Profile Information from 3GPP2 AAA – Intra-eHRPD Handoff with HSGW Relocation with Context Transfer**

Note: The following procedure assumes that the deployment of Subscriber QoS Profile Configuration feature is consistent throughout the operator network.

0. UE has an active session with the P-GW via the S-eAN/ePCF and the S-HSGW. The UE or the S-eAN decides that the UE moves to the T-eAN. eHRPD radio session context is transferred to the T-eAN including the H1 address of the S-HSGW. The T-eAN/ePCF sets up the A10 connection with the selected T-HSGW. The T-HSGW performs the Handover Initiate procedures with the S-HSGW over the H1 Interface, and the S-HSGW responds with a Handover Ack message that contains the user session context parameters as described in section 11.1.1 steps 0-7, and section 11.1.2 steps 0-7. Context parameters related to the Subscriber QoS Profile are not transferred from the S-HSGW to the T-HSGW.

1. The T-HSGW invokes the Subscriber QoS Profile Configuration procedure by sending the Query Profile Request (QPR) command to the 3GPP2 AAA Proxy/Server. If the HSGW does not know if the 3GPP2 Proxy/Server supports the SubQosConfig feature, it includes Supported-Features AVP in the QPR command, with the Feature-List-ID sub AVP set to 1 (“Query Group”) and feature bit ‘0’ in the Feature-List sub AVP set to ‘1’.

2. On successful processing of the Query Profile Request (QPR) command, the 3GPP2 AAA Proxy/Server responds to the T-HSGW with a Query Profile Answer (QPA) command with Result Code success (DIAMETER_SUCCESS) that includes the 3GPP2 Subscriber QoS Profile...
information. If the Supported-Features AVP is included in the QPR command, the Supported-Features AVP is included in the QPA command also, indicating the complete set of features supported by the 3GPP2 AAA Proxy/Server. The 3GPP2 AAA Proxy/Server uses the IMSI-based Network Access Identifier (NAI) as the key to the subscriber profile information.

3. If the T-HSGW receives the 3GPP2 Subscriber QoS Profile information from the 3GPP2 AAA Proxy/Server, it forwards the Subscriber QoS Profile information elements to the T-eAN/ePCF via A11-Session Update procedures.

4. The remainder of the handoff procedure continues from step 8 in sections 11.1.1 and 11.1.2.

**15.4 Subscriber QoS Profile Information Attributes**

The Subscriber QoS Profile Configuration procedure is initiated by the HSGW, and the 3GPP2 AAA Proxy/Server responds with the Subscriber QoS Profile information, if available. As specified in X.S0011 [6], the following attributes of the Subscriber QoS Profile are sent to the eAN/ePCF:

- Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic
- Authorized Flow Profile IDs for Each Direction
- Maximum per Flow Priority
- Service Option Profile
- Inter-User Priority for Best Effort Traffic

The handling and usage of the Subscriber QoS Profile attributes at the HSGW shall be as specified in Annex D (Section 19). The HSGW shall store the Subscriber QoS Profile attributes.

Table 60 specifies the information elements supported in the Query Profile Request command.

Table 61 specifies the information elements supported in the Query Profile Answer command.
### Table 60  Information Elements in the Query Profile Request command

<table>
<thead>
<tr>
<th>Information Element Name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Identity (IMSI)</td>
<td>User-Name (ref. IETF RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [20] clause 2.2.</td>
</tr>
<tr>
<td>Authentication Session State</td>
<td>Auth-Session-State (ref. IETF RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall include a value of NO_STATE_MAINTAINED.</td>
</tr>
<tr>
<td>Supported Features</td>
<td>Supported-Features (ref. 3GPP TS 29.229 [32])</td>
<td>O</td>
<td>This is a Grouped AVP. Vendor-Id sub AVP shall be set to SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535). The Feature-List-ID sub AVP shall be set to 1 (&quot;Query Group&quot;); and the Feature-List sub AVP shall have bit ‘0’ set indicating the ‘SubQoSConfig’ (Subscriber QoS Profile Configuration) feature.</td>
</tr>
<tr>
<td>Information Element Name</td>
<td>Mapping to Diameter AVP</td>
<td>Cat.</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Result Code</td>
<td>Result-Code / Experimental-Result (ref. RFC3588 [63]).</td>
<td>M</td>
<td>This information element shall contain the result of the operation. The Result-Code AVP shall be used to indicate success or errors as defined in the Diameter Base Protocol (ref RFC3588 [63]). The Experimental-Result AVP shall be used for the Pt*3GPP2 Diameter Application and associated Subscriber QoS Profile Configuration feature errors. This is a Grouped AVP, and shall contain 3GPP2 Vendor ID (5535) in the Vendor-ID AVP, and the error code in the Experimental-Result-Code AVP.</td>
</tr>
<tr>
<td>User Identity (IMSI)</td>
<td>User-Name (ref. RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [19] clause 2.2.</td>
</tr>
<tr>
<td>Authentication Session State</td>
<td>Auth-Session-State (ref. RFC 3588 [63])</td>
<td>M</td>
<td>This information element shall include a value of NO_STATE_MAINTAINED.</td>
</tr>
<tr>
<td>3GPP2 AAA Server Name</td>
<td>Redirect-Host (ref. RFC 3588 [63])</td>
<td>C</td>
<td>This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION, and shall contain the Diameter identity of the 3GPP2 AAA Proxy/Server in the home domain that is currently serving the user. The QPA command shall contain zero or more occurrences of this information element.</td>
</tr>
<tr>
<td>Supported Features</td>
<td>Supported-Features (ref. 3GPP TS 29.229 [32])</td>
<td>C</td>
<td>This is a Grouped AVP. Vendor-Id AVP shall be set to SMI Network Management Private Enterprise Codes assigned to 3GPP2 (5535). The Feature-List-ID sub AVP shall be set to 1 (“Query Group”); and the Feature-List sub AVP shall have the bits set for the complete set of features supported by the 3GPP2 AAA Proxy/Server.</td>
</tr>
<tr>
<td>Service Option Profile</td>
<td>Service-Option-Profile (ref. section 15.4.5)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included. This is a Grouped AVP and shall indicate the maximum number of allowed link flows and allowed Service Options.</td>
</tr>
<tr>
<td>Maximum Authorized Aggregate Bandwidth for Best Effort Traffic</td>
<td>Maximum-Allowed-Aggregate-Bandwidth-for-Best-Effort-Traffic (ref. section 15.4.6)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included and shall indicate the maximum bandwidth that may be allocated to a user for best effort traffic.</td>
</tr>
<tr>
<td>Information Element Name</td>
<td>Mapping to Diameter AVP</td>
<td>Cat.</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Authorized Flow Profile IDs for the User for Each Direction (ref. X.S0011 [6])</td>
<td>Authorized-Flow-Profile-IDs-for-the-User (ref. section 15.4.7)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included. This is a Grouped AVP and indicates the Flow Profile IDs that the user is allowed to request in a QoS Sub Blob.</td>
</tr>
<tr>
<td>Authorized Flow Profile IDs for the User for Each Direction (ref. X.S0011 [6])</td>
<td>Authorized-Flow-Profile-IDs-for-the-User (ref. section 15.4.7)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included. This is a Grouped AVP and indicates the Flow Profile IDs that the user is allowed to request in a QoS Sub Blob.</td>
</tr>
<tr>
<td>Inter User Priority for Best Effort Traffic (ref. X.S0011 [6])</td>
<td>Inter-User-Priority (ref. section 15.4.8)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included and indicates the inter-user priority that may be assigned to user’s packet flow for best effort traffic.</td>
</tr>
<tr>
<td>Maximum Per Flow Priority (ref. X.S0011 [6])</td>
<td>Max-Per-Flow-Priority-for-the-User (ref. section 15.4.9)</td>
<td>O</td>
<td>If the Result-Code is DIAMETER_SUCCESS, this information element may be included and shall indicate the maximum priority that may be assigned to a user’s packet flow.</td>
</tr>
</tbody>
</table>

### 15.4.1 Behavior of the HSGW

If both the HSGW and the 3GPP2 AAA Proxy/Server support the Pi*3GPP2 Diameter Application and the HSGW needs the Subscriber QoS Profile information, the HSGW shall initiate the Subscriber QoS Profile Configuration procedure by sending a Query Profile Request (QPR) command to the 3GPP2 AAA Proxy/Server. If the HSGW does not know if the SubQosConfig features is supported by the 3GPP2 AAA Proxy/Server, the QPR command shall include the Supported-Features AVP with the ‘M’ bit set, the Feature-List-ID sub AVP set to 1(“Query Group”), and the Feature-List sub AVP shall have bit ‘0’ set indicating a request for the Subscriber QoS Profile Configuration procedure. The HSGW uses this procedure to retrieve Subscriber QoS Profile information from the 3GPP2 AAA Proxy/Server.

The Subscriber QoS Profile Configuration procedure is a stateless procedure. The HSGW shall include the Auth-Session-State AVP in the Query Profile Request (QPR) command, with the value set to NO_STATE_MAINTAINED.

On receiving a Query Profile Answer (QPA) command from the 3GPP2 AAA Proxy/Server, the HSGW shall check the Result Code. If the result code indicates other than success (DIAMETER_SUCCESS) the HSGW takes corrective action based on the received result code.

On receiving a Query Profile Answer (QPA) command from the 3GPP2 AAA Proxy/Server with success (DIAMETER_SUCCESS) Result Code, the HSGW shall check for the presence of the Subscriber QoS Parameters listed in Section 15.1, and shall handle them as per procedures specified in Annex D (Section 19).
If a Query Profile Answer (QPA) command is received with the Experimental-Result-Code AVP set to DIAMETER_ERRORFEATURE_UNSUPPORTED, the HSGW shall abort the Subscriber QoS Profile Configuration procedure.

### 15.4.2 Behavior of the 3GPP2 AAA Proxy/Server

On receiving the Query Profile Request (QPR) command, if the Supported Feature AVP is included, the 3GPP2 AAA Proxy/Server shall do one of the following:

- If it supports all the features indicated in the Supported-Features AVP, the 3GPP2 AAA Proxy/Server shall include the Supported-Features AVP in the QPA command, identifying the complete set of features that it supports for the Pi*3GPP2 Diameter Application.

- If it does not support all the features indicated in the Supported-Features AVP, the 3GPP2 AAA Proxy/Server shall return the QPA command with the Experimental-Result-Code AVP set to DIAMETER_ERROR_FEATURE_UNSUPPORTED and shall include the Supported-Features AVP identifying the complete set of features that it supports for the Pi*3GPP2 Diameter Application.

- If it does not support the Supported-Features AVP, it shall return the QPA command with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED and a Failed-AVP containing the Supported-Features AVP as received in the QPR command.

If the 3GPP2 AAA Proxy/Server includes the Supported-Features AVP in the Query Profile Answer (QPA) command, the Supported-Features AVP shall have the 'M' bit cleared. In this Grouped AVP, the Feature-List-ID sub AVP shall be set to 1 (“Query Group”); and the Feature-List sub AVP shall have bits set for the complete set of features supported by the 3GPP2 AAA Proxy/Server.

If the 3GPP2 AAA Proxy/Server supports the Subscriber QoS Profile Configuration (SubQoSConfig) feature:

- It shall check whether the User Name (IMSI) in the User-Name AVP is known. If it is not known, a Result Code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.

- If the user is known but does not have any Subscriber QoS Profile configured for it, the 3GPP2 AAA Proxy/Server shall respond with Experimental-Result-Code DIAMETER_ERROR_NO_SUBSCRIBER_QoS_PROFILE.

- For any other error, the Result Code DIAMETER_UNABLE_TO_COMPLY shall be returned.

The Subscriber QoS Profile Configuration procedure is a stateless procedure. The 3GPP2 AAA Proxy/Server shall include the Auth-Session-State AVP in the Query Profile Answer (QPA) command, with the value set to NO_STATE_MAINTAINED.

If the 3GPP2 AAA Proxy/Server successfully processes the received Query Profile Request (QPR) command, the 3GPP2 AAA Proxy/Server shall respond with a Query Profile Answer (QPA) command with Result Code success (DIAMETER_SUCCESS), and shall include the subscribed QoS information elements as listed in Table 61.
15.4.3 Result-Code and Experimental-Result AVP values

15.4.3.1 Result-Code

The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [63] shall be applicable.

15.4.3.2 Experimental-Result

When one of the result codes defined here is included in an answer command, it shall be inside an Experimental-Result AVP with Vendor-ID set to the 3GPP2 Vendor-ID (5535).

15.4.3.3 Experimental-Result-Code

The Experimental-Result-Code AVP contains the 3GPP2 assigned value representing the result of processing a request command.

15.4.3.3.1 DIAMETER_ERROR_FEATURE_UNSUPPORTED (3001)

This Experimental Result Code shall be sent by the 3GPP2 AAA Proxy/Server to the HSGW if it does not support all the features indicated in the Supported-Features AVP.

15.4.3.3.2 DIAMETER_ERROR_NO_SUBSCRIBER_QoS_PROFILE (4001)

This Experimental Result Code shall be sent by the 3GPP2 AAA Proxy/Server to the HSGW if the user is known but it does not have a Subscriber QoS Profile configured for the user.
15.4.4 AVPs

Table 62 lists the Diameter AVPs defined for the Subscriber QoS Profile Configuration feature for use in the Query Profile Request (QPR) and Query Profile Answer (QPA) commands.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Section defined</th>
<th>Value Type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service-Option-Profile</td>
<td>9074</td>
<td>15.4.5</td>
<td>Grouped</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum-Authorized-Aggregate-</td>
<td>9130</td>
<td>15.4.6</td>
<td>Unsigned32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth-for-Best-Effort-Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorized-Flow-Profile-IDs-for-the-User</td>
<td>9131</td>
<td>15.4.7</td>
<td>Grouped</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-User-Priority</td>
<td>9139</td>
<td>15.4.8</td>
<td>Integer32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum-Per-Flow-Priority-for-the-User</td>
<td>9133</td>
<td>15.4.9</td>
<td>Integer32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProfileID-Forward</td>
<td>35</td>
<td>15.4.10</td>
<td>Integer32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProfileID-Reverse</td>
<td>36</td>
<td>15.4.11</td>
<td>Integer32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProfileID-Bi-Directional</td>
<td>37</td>
<td>15.4.12</td>
<td>Integer32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max-Link-Flows</td>
<td>57</td>
<td>15.4.13</td>
<td>Unsigned32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service-Option-Number</td>
<td>58</td>
<td>15.4.14</td>
<td>Unsigned32</td>
<td>V M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: The AVP header bit denoted as ‘M’, indicates whether support of the AVP is required. The AVP header bit denoted as ‘V’, indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [63].

Table 63 lists the Diameter AVPs re-used by the Subscriber QoS Profile Configuration feature for use in the Query Profile Request (QPR) and Query Profile Answer (QPA) commands from existing Diameter Applications, including a reference to their respective specifications. Other AVPs from existing Diameter Applications except for the AVPs from Diameter Base Protocol do not need to be supported.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Reference</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>RFC3588 [63]</td>
<td>This information element shall contain the identity of the user.</td>
</tr>
<tr>
<td>Supported-Features</td>
<td>TS 29.229 [32]</td>
<td>This information element shall contain the list of features supported by the node originating the command (Origin Host).</td>
</tr>
<tr>
<td>Feature-List-ID</td>
<td>TS 29.229 [32]</td>
<td>This information element shall contain the identity of the feature list.</td>
</tr>
<tr>
<td>Feature-List</td>
<td>TS 29.229 [32]</td>
<td>This information element shall contain a bit mask indicating the supported features of an application.</td>
</tr>
</tbody>
</table>
15.4.5 Service-Option-Profile

The Service-Option-Profile AVP (AVP code 5535/9074) is of type Grouped. It specifies the authorized packet data Service Options and the allowed maximum number of simultaneous Link Flows.

AVP format:

```
Service-Option-Profile ::= < AVP Header: 9074 5535 >
{Max-Link-Flows}
* [Service Option Number]
* [AVP]
```

15.4.6 Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort-Traffic

The Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort-Traffic AVP (AVP code 5535/9130) is of type Unsigned32. It shall indicate the maximum bandwidth with range 1 to \(2^{32}\) (binary value of the maximum allowed aggregate bandwidth, in bits per second) that may be allocated to a user for best-effort traffic.

15.4.7 Authorized-Flow-Profile-IDs-for-the-User

The Authorized-Flow-Profile-IDs-for-the-User AVP (AVP code 5535/9131) is a Grouped AVP. It provides the list of Flow Profile IDs that the user is allowed to specify/request in a QoS_Sub_Blob.

Authorized-Flow-Profile-IDs-for-the-User ::= < AVP Header: 9131 5535 >

```
* [ProfileID-Forward]
* [ProfileID-Reverse]
* [ProfileID-Bi-direction]
* [AVP]
```

15.4.8 Inter-User-Priority

The Inter-User-Priority AVP (AVP code 5535/9139) is of type Integer32. It indicates the inter-user priority assigned to the user for best effort traffic. The low order 3 bits shall indicate the inter-user priority used for scheduling packets (ref. X.S0011 [6] ). Priority 7 is the highest and 0 is the lowest.

- 000-011: Priority 0 to 3 for regular users.
- 100-111: Priority 4 to 7 for Reserved Class.
15.4.9 Maximum-Per-Flow-Priority-for-the-User

The Maximum-Per-Flow-Priority-for-the-User AVP (AVP code 5535/9133) is of type Integer32. It indicates the maximum priority that may be assigned to user’s packet flow. The low order 4 bits shall indicate the maximum priority that the user can specify for a packet data flow. Priority 15 is the highest and 0 is the lowest. Specifically:

- 0000-0111: Priority 0 to 7 for regular users.
- 1000-1111: Priority 8 to 15 for Reserved Class.

15.4.10 ProfileID-Forward

The ProfileID-Forward AVP (AVP code 5535/35) is of type Integer32. It is used to indicate Flow Profile ID that the user is allowed to request on the forward link. The Flow Profile ID shall be included in the least significant 16 bits. The most significant 16 bits shall be set to 0.

15.4.11 ProfileID-Reverse

The ProfileID-Reverse AVP (AVP code 5535/36) is of type Integer32. It is used to indicate Flow Profile ID that the user is allowed to request on the reverse link. The Flow Profile ID shall be included in the least significant 16 bits. The most significant 16 bits shall be set to 0.

15.4.12 ProfileID-Bi-Directional

The ProfileID-Bi-Direction AVP (AVP code 5535/37) is of type Integer32. It is used to indicate Flow Profile ID that the user is allowed to request bi-directionally. The Flow Profile ID shall be included in the least significant 16 bits. The most significant 16 bits shall be set to 0.

15.4.13 Max-Link-Flows

The Max-Link-Flows AVP (AVP code 5535/57) is of type Unsigned32. It shall indicate the maximum number of link flows that the user is allowed to establish.

15.4.14 Service-Option-Number

The Service-Option-Number AVP (AVP code 5535/58) is of type Unsigned32. It shall indicate the Service Option allowed for the user.
16 Annex A (Informative) – Mapping QoS between 3GPP and 3GPP2

In section 4.6.6, the differences between the specification of QoS parameters in 3GPP EPS and 3GPP2 eHRPD is discussed. For 3GPP EPS networks which use eHRPD access, the 3GPP QoS parameters specify the desirable packet forwarding treatment within the LTE EPC. However the specification of QoS parameters for eHRPD uses the 3GPP2 FlowProfileID. Since the HSGW serves as the interworking point between the 3GPP EPS network and the 3GPP2 eHRPD access network, the HSGW maintains a mapping of the 3GPP2 QoS parameters and the 3GPP QoS parameters. This mapping is between the 3GPP2’s FlowProfileIDs and the 3GPP’s triple <QCI, GBR, MBR>.

3GPP defines nine standard QCIs (see TS 23.203 [20]). A QCI is a scalar value which classifies a set of bearer parameters suitable to a particular class of applications. The bearer parameters associated with a QCI are:

- Packet Delay Budget (PDB)
- Packet Loss Rate (PLR)
- Priority
- Resource Type (GBR or Non-GBR)

In addition to these standard QCIs, operators are allowed to define additional QCIs for specific services in which the standard QCIs are insufficient. An example is a public safety service where the operator may want a unique priority associated with the service.

On the other hand, eHRPD uses FlowProfileIDs (see 3GPP2 C.R1001 [11]). A FlowProfileID is a scalar value representing a flow description. A flow description specifies all relevant air interface parameters necessary to support a particular packet data service. There are hundreds of flow descriptions identified in C.R1001 with a FlowProfileID associated with each description.

The QCIs are used exclusively in the EPC and E-UTRAN portion of the network while FlowProfileIDs are used exclusively in the eHRPD portion of the network (see Figure 63). So the method used for specifying service parameters for a particular service in eHRPD (namely FlowProfileIDs) shall be mapped to the service parameters associated with the same service in EPC (namely QCIs).
When mapping from 3GPP to 3GPP2, a twofold mapping strategy is recommended:

1. Associate 3GPP QCI values with 3GPP2 FlowProfileIDs based on service similarities.
2. For a given QCI to FlowProfileID association, map the GBR value used in 3GPP to the data rate associated with the FlowProfileID.

When mapping from 3GPP2 to 3GPP, a twofold mapping strategy is recommended:

1. From the characteristics of the 3GPP2 FlowProfileID, find the associated 3GPP QCI.
2. From the bit rate of the 3GPP2 FlowProfileID, determine the 3GPP GBR.

Any mapping strategy should follow these general principles:

1. Mapping across technologies is only to convey the type of service. Therefore, the mapping will associate QCI values with FlowProfileID values.
2. A bi-directional mapping between E-UTRAN and eHRPD should be supported. Providing this supports both UE initiated and network initiated bearers.
3. The mapping maintained in the HSGW may be customized by the operator and is guided by the services deployed by the operator.
4. When mapping between FlowProfileID data rates and GBR, the following considerations apply:
a. When mapping from a FlowProfileID data rate to GBR, a bit rate shall be calculated such that the EPS bearer supports the service.

b. When mapping from a GBR values to a FlowProfileID data rate, all FlowProfileIDs with a sufficient bit rate to support the GBR value are chosen. When none of the authorized FlowProfileID(s) support the GBR value, the QoS request from the PCRF is rejected by the HSGW.

c. It is assumed that both the FlowProfileID data rates and the GBR data rate values include IP/UDP/RTP headers. The IP/UDP/RTP components being referred to are not part of the tunneling header.

d. It is further assumed that for variable data rate GBR services (e.g., voice), the peak data rate value is used to represent the GBR data rate values.

5. Given that a set of FlowProfileIDs is provided to the HSGW, the HSGW maps the FlowProfileIDs to a single QCI when considering the service characteristics. To facilitate this mapping, the UE should select FlowProfileIDs that have similar QoS characteristics resulting in the same QCI.

6. When multiple bit rates are indicated by the FlowProfileIDs, the operator determines (based on operator determined charging rules, etc.) the mapping of the QCI information returned by the PCRF to a set (one or more) of FlowProfileIDs that are sent to the UE.

An example of this mapping is shown in Table 64.
### Table 64  Example of QoS Mapping

<table>
<thead>
<tr>
<th>QCI</th>
<th>Resource Type (bit rate included if GBR)</th>
<th>Priority</th>
<th>Packet Delay Budget</th>
<th>Packet Error Loss Rate</th>
<th>Example Services</th>
<th>eHRPD Flow-ProfileID</th>
<th>eHRPD Flow Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GBR (32.8 kbps)</td>
<td>2</td>
<td>100 ms</td>
<td>10^{-2}</td>
<td>0x0100</td>
<td>Conversational Rate Set 1 Speech</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>GBR (32.8 kbps)</td>
<td>2</td>
<td>100 ms</td>
<td>10^{-2}</td>
<td>PTT Voice</td>
<td>0x0118</td>
<td>PTT Rate set 1 Speech (maximum of 6 frames bundled)</td>
</tr>
<tr>
<td>1</td>
<td>GBR (37.6 kbps)</td>
<td>2</td>
<td>100 ms</td>
<td>10^{-2}</td>
<td>Conversational Voice</td>
<td>0x0101</td>
<td>Conversational Rate Set 2 Speech</td>
</tr>
<tr>
<td>2</td>
<td>GBR (24 kbps)</td>
<td>4</td>
<td>150 ms</td>
<td>10^{-3}</td>
<td>Conversational Video (Live Streaming)</td>
<td>0x0300</td>
<td>Conversational Video Streaming</td>
</tr>
<tr>
<td>2</td>
<td>GBR (32 kbps)</td>
<td>4</td>
<td>150 ms</td>
<td>10^{-3}</td>
<td>Conversational Video (Live Streaming)</td>
<td>0x0301</td>
<td>Conversational Video Streaming</td>
</tr>
<tr>
<td>2</td>
<td>GBR (40 kbps)</td>
<td>4</td>
<td>150 ms</td>
<td>10^{-3}</td>
<td>Conversational Video (Live Streaming)</td>
<td>0x0302</td>
<td>Conversational Video Streaming</td>
</tr>
<tr>
<td>2</td>
<td>GBR (48 kbps)</td>
<td>4</td>
<td>150 ms</td>
<td>10^{-3}</td>
<td>Conversational Video (Live Streaming)</td>
<td>0x0303</td>
<td>Conversational Video Streaming</td>
</tr>
<tr>
<td>2</td>
<td>GBR (64 kbps)</td>
<td>4</td>
<td>150 ms</td>
<td>10^{-3}</td>
<td>Conversational Video (Live Streaming)</td>
<td>0x0305</td>
<td>Conversational Video Streaming</td>
</tr>
<tr>
<td>3</td>
<td>GBR</td>
<td>3</td>
<td>50 ms</td>
<td>10^{-3}</td>
<td>Real Time Gaming</td>
<td>0x0005</td>
<td>Real Time Gaming</td>
</tr>
<tr>
<td>4</td>
<td>GBR (24 kbps)</td>
<td>5</td>
<td>300 ms</td>
<td>10^{-6}</td>
<td>Non-Conversational Video (Buffered Streaming)</td>
<td>0x030c</td>
<td>Video Streaming</td>
</tr>
<tr>
<td>4</td>
<td>GBR (64 kbps)</td>
<td>5</td>
<td>300 ms</td>
<td>10^{-6}</td>
<td>Non-Conversational Video (Buffered Streaming)</td>
<td>0x030e</td>
<td>Video Streaming</td>
</tr>
<tr>
<td>4</td>
<td>GBR (128 kbps)</td>
<td>5</td>
<td>300 ms</td>
<td>10^{-6}</td>
<td>Non-Conversational Video (Buffered Streaming)</td>
<td>0x0311</td>
<td>Video Streaming</td>
</tr>
<tr>
<td>5</td>
<td>Non-GBR</td>
<td>1</td>
<td>100 ms</td>
<td>10^{-6}</td>
<td>PTT Control Signaling</td>
<td>0x0503</td>
<td>Real Time Control Signaling</td>
</tr>
<tr>
<td>5</td>
<td>Non-GBR</td>
<td>1</td>
<td>100 ms</td>
<td>10^{-6}</td>
<td>IMS Signaling</td>
<td>0x0500</td>
<td>Conversational Control Signaling</td>
</tr>
<tr>
<td>QCI</td>
<td>Resource Type (bit rate included if GBR)</td>
<td>Priority</td>
<td>Packet Delay Budget</td>
<td>Packet Error Loss Rate</td>
<td>Example Services</td>
<td>eHRPD Flow ProfileID</td>
<td>eHRPD Flow Description</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------</td>
<td>----------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>6</td>
<td>Non-GBR</td>
<td>6</td>
<td>300 ms</td>
<td>10^6</td>
<td>Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)</td>
<td>0x0000</td>
<td>Best effort</td>
</tr>
<tr>
<td>7</td>
<td>Non-GBR</td>
<td>7</td>
<td>100 ms</td>
<td>10^3</td>
<td>Voice, Video (Live Streaming) Interactive Gaming</td>
<td>0x0600</td>
<td>Interactive Gaming</td>
</tr>
<tr>
<td>8</td>
<td>Non-GBR</td>
<td>8</td>
<td>300 ms</td>
<td>10^6</td>
<td>TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)</td>
<td>0x0000</td>
<td>Best effort</td>
</tr>
<tr>
<td>9</td>
<td>Non-GBR</td>
<td>9</td>
<td>300 ms</td>
<td>10^6</td>
<td>TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)</td>
<td>0x0000</td>
<td>Best effort</td>
</tr>
</tbody>
</table>

Footnote 1:
Assumptions for GBR rate set 1 and rate set 2 calculations:
- Rate Set 1 and rate set 2 conversational voice, no voice-frame bundling, and no header compression.
- This yields 1 voice frame carried in 1 IP packet every 20ms in each (uplink and downlink) direction.
- Assume GBR accounts for the peak data rate; therefore data rate of only the full rate frame is used.
  - Rate Set 1 Full Rate frame: 171 bits => 22 octets
  - Rate Set 2 Full Rate frame: 266 bits => 34 octets
  - RTP Header = 12 octets
  - UDP Header = 8 octets
  - IPv4 Header = 20 octets
  - IPv6 Header = 40 octets
  - Rate Set 1 GBRv4 = (22+12+8+20)*8*50 = 24.8 kbps (use rate set 1 GBRv6 value).
  - Rate Set 1 GBRv6 = (22+12+8+40)*8*50 = 32.8 kbps => use 32.8.
  - Rate Set 2 GBRv4 = (34+12+8+20)*8*50 = 29.6 kbps (use rate set 2 GBRv6 value).
  - Rate Set 2 GBRv6 = (34+12+8+40)*8*50 = 37.6 kbps => use 37.6 kbps in each direction.

Footnote 2:
The maximum bit rate for PTT using FlowProfileID 0x0118 is the same as that for FlowProfileID 0x0100. It is possible that bundling may occur, and in that case, the bit rate would be reduced.

Footnote 3:
There is no GBR FlowProfileID in C.R1001 that provides 50 ms maximum latency. FlowProfileID 0x0005 provides 100 ms maximum latency and supports 32 kbps as a close approximation for QCI 3,
# 17 Annex B (Informative) – Mapping Gxa Parameters between 3GPP and 3GPP2

The information received across the Gxa interface is illustrated in Table 65 along with an indication if it is required and how it is used in eHRPD.

## Table 65  Mapping Gxa Parameters between 3GPP and 3GPP2

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Reference (3GPP TS 29.212 Clause)</th>
<th>Description</th>
<th>Access type</th>
<th>eHRPD Mapping</th>
<th>Need on Gxa for eHRPD access</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP-MS-TimeZone</td>
<td>3GPP TS 29.061 [27]</td>
<td>Indicate the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.</td>
<td>All</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>3GPP-SGSN-Address</td>
<td>3GPP TS 29.061 [27]</td>
<td>The IPv4 address of the SGSN</td>
<td>3GPP-EPS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>3GPP-SGSN-IPv6-Address</td>
<td>3GPP TS 29.061 [27]</td>
<td>The IPv6 address of the SGSN</td>
<td>3GPP-EPS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>AN-GW-Address</td>
<td>5.3.49</td>
<td>Carries the address of the AN-GW (HSGW)</td>
<td>All</td>
<td>Carries the address of the serving HSGW.</td>
<td>Yes</td>
</tr>
<tr>
<td>3GPP-SGSN-MCC-MNC</td>
<td>3GPP TS 29.061 [27]</td>
<td>Carries the MCC/MNC information of the AN-GW</td>
<td>All</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>3GPP-User-Location-Info</td>
<td>3GPP TS 29.061 [27]</td>
<td>Indicates details of where the UE is currently located (e.g., SAI or CGI)</td>
<td>3GPP</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>3GPP2-BSID</td>
<td>3GPP2 X.S0011 [6]</td>
<td>Indicates the BSID of where the UE is currently located (e.g. Cell-Id, SID, NID).</td>
<td>3GPP2</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access-Network-Charging-Identifier-Value</td>
<td>3GPP TS 29.214 [31]</td>
<td>Contains a charging identifier.</td>
<td>All</td>
<td>No mapping required.</td>
<td>No Note 3</td>
</tr>
<tr>
<td>Allocation-and-Retention-Priority</td>
<td>5.3.32</td>
<td>Indicates a priority for accepting or rejecting a bearer establishment or modification request and dropping a bearer in case of resource limitations.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>APN-Aggregate-Max-Bitrate-DL</td>
<td>5.3.39</td>
<td>Indicates the aggregate maximum bitrate for the downlink direction for all non-GBR bearers of the APN.</td>
<td>3GPP-EPS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>APN-Aggregate-Max-Bitrate-UL</td>
<td>5.3.40</td>
<td>Indicates the aggregate maximum bitrate for the uplink direction for all non-GBR bearers of the APN.</td>
<td>3GPP-EPS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Bearer-Control-Mode</td>
<td>5.3.23</td>
<td>Indicates the PCRF selected bearer control mode.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Called-Station-ID</td>
<td>IETF RFC 4005 [69]</td>
<td>The address the user is connected to (i.e., the PDN identifier).</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>PDN-Connection-ID</td>
<td>5.3.58</td>
<td>The identification of PDN connection to the same APN.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>CC-Request-Number</td>
<td>IETF RFC 4006 [70]</td>
<td>The number of the request for mapping requests and answers</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Reference (3GPP TS 29.212 Clause) [29]</td>
<td>Description</td>
<td>Access type</td>
<td>eHRPD Mapping</td>
<td>Need on Gxa for eHRPD access</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>CC-Request-Type</td>
<td>IETF RFC 4006 [70]</td>
<td>The type of the request (initial, update, termination)</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>User-CSG-Information</td>
<td>3GPP TS 32.299 [39]</td>
<td>Indicates the user &quot;Closed Subscriber Group&quot; Information associated to CSG cell access</td>
<td>3GPP-EPS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Event-Trigger</td>
<td>5.3.7</td>
<td>Reports the event that occurred on the BBERF.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Flow-Description</td>
<td>3GPP TS 29.214 [31]</td>
<td>Defines the service flow filter parameters for a QoS rule</td>
<td>All</td>
<td>The HSGW maps the 'flow-description' to the packet filter field in the TFT.</td>
<td>Yes</td>
</tr>
<tr>
<td>Flow-Information</td>
<td>5.3.53</td>
<td>Defines the service flow filter parameters for a QoS rule and may include flow description, packet filter identifier, ToS/Traffic Class, SPI and Flow Label information. May also include an instruction as to whether signalling the information to the UE is to occur.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Flow-Label</td>
<td>5.3.52</td>
<td>Defines the IPv6 flow label</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>IETF RFC 4005 [69]</td>
<td>The IPv4 address allocated for the user.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Framed-IPv6-Prefix</td>
<td>IETF RFC 4005 [69]</td>
<td>The IPv6 address prefix allocated for the user.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Guaranteed-Bit Rate-DL (note 1)</td>
<td>5.3.25</td>
<td>Defines the guaranteed bit rate for downlink.</td>
<td>All</td>
<td>HSGW uses this in the selection of appropriate FlowProfileID</td>
<td>Yes</td>
</tr>
<tr>
<td>Guaranteed-Bit Rate-UL (note 1)</td>
<td>5.3.26</td>
<td>Defines the guaranteed bit rate for uplink.</td>
<td>All</td>
<td>HSGW uses this in the selection of appropriate FlowProfileID</td>
<td>Yes</td>
</tr>
<tr>
<td>IP-CAN-Type</td>
<td>5.3.27</td>
<td>Indicates the type of Connectivity Access Network that the user is connected to.</td>
<td>All</td>
<td>HSGW sets this value to non-3GPP-EPS (6)</td>
<td>Yes</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-UL (note 2)</td>
<td>3GPP TS 29.214 [31]</td>
<td>Defines the maximum authorized bandwidth for uplink.</td>
<td>All</td>
<td>HSGW uses this in the selection of appropriate FlowProfileID</td>
<td>Yes</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-DL (note 2)</td>
<td>3GPP TS 29.214 [31]</td>
<td>Defines the maximum authorized bandwidth for downlink.</td>
<td>All</td>
<td>HSGW uses this in the selection of appropriate FlowProfileID</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet-Filter-Content</td>
<td>5.3.54</td>
<td>Indicates the content of the packet filter.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet-Filter-Identifier</td>
<td>5.3.55</td>
<td>The identity of the packet filter.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet-Filter-Information</td>
<td>5.3.56</td>
<td>Information related to the packet filters that the BBERF provides to the PCRF.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Reference (3GPP TS 29.212 Clause) [29]</td>
<td>Description</td>
<td>Access type</td>
<td>eHRPD Mapping</td>
<td>Need on Gxa for eHRPD access</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Packet-Filter-Operation</td>
<td>5.3.57</td>
<td>Indicates the operation that the terminal is requesting over the packet filters provided by the Packet-Filter-Information AVPs.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet-Filter-Usage</td>
<td>5.3.66</td>
<td>Indicates whether the UE shall be provisioned with the related traffic mapping information.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Network-Request-Support</td>
<td>5.3.24</td>
<td>Indicates whether the access network supports the network requested bearer control mode or not.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Precedence</td>
<td>5.3.11</td>
<td>Indicates the precedence of QoS rules or packet filters.</td>
<td>All</td>
<td>HSGW maps this to the TFT evaluation precedence value.</td>
<td>Yes</td>
</tr>
<tr>
<td>PCC-Rule-Status</td>
<td>5.3.19</td>
<td>Describes the status of one or a group of QoS rules.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS-Class-Identifier (QCI)</td>
<td>5.3.17</td>
<td>Identifies a set of IP-CAN specific QoS parameters</td>
<td>All</td>
<td>See Annex A.</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS-Information</td>
<td>5.3.16</td>
<td>Defines the QoS information for a resource, QoS rule or QCI</td>
<td>All</td>
<td>HSGW shall use the values in this AVP to determine the appropriate FlowProfileID. See Annex A.</td>
<td>Yes</td>
</tr>
<tr>
<td>Default-EPS-Bearer-Qos</td>
<td>5.3.48</td>
<td>Defines the QoS information of the default bearer</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>RAI</td>
<td>3GPP TS 29.061 [27]</td>
<td>Contains the Routing Area Identity of the SGSN where the UE is registered</td>
<td>3GPP-GPRS</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>RAT-Type</td>
<td>5.3.31</td>
<td>Identifies the radio access technology that is serving the UE.</td>
<td>All</td>
<td>The HSGW sets this AVP to '2003' to indicate eHRPD access RAT.</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource-Allocation-Notification</td>
<td>5.3.50</td>
<td>Indicates whether successful resource allocation notification for rules is needed or not.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rule-Activation-Time</td>
<td>5.3.41</td>
<td>Indicates the NTP time at which the QoS rules have to be enforced.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rule-Deactivation-Time</td>
<td>5.3.42</td>
<td>Indicates the NTP time at which the BBERF has to stop enforcing the QoS rules.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rule-Failure-Code</td>
<td>5.3.38</td>
<td>Identifies the reason a QoS rule is being reported.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Security-Parameter-Index</td>
<td>5.3.51</td>
<td>Defines the IPSec SPI</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Session-Release-Cause</td>
<td>5.3.44</td>
<td>Indicate the reason of termination initiated by the PCRF. Only the reason code UNSPECIFIED_REASON is applicable for the PCRF-initiated Gxx session termination.</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Reference (3GPP TS 29.212 Clause)</td>
<td>Description</td>
<td>Access type</td>
<td>eHRPD Mapping</td>
<td>Need on Gxa for eHRPD access</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Subscription-Id</td>
<td>IETF RFC 4006 [70]</td>
<td>The identification of the subscription (i.e., IMSI)</td>
<td>All</td>
<td>HSGW uses the IMSI obtained from A11 messaging to map to this AVP</td>
<td>Yes</td>
</tr>
<tr>
<td>Supported-Features</td>
<td>3GPP TS 29.229 [32]</td>
<td>If present, this AVP informs the destination host about the features that the origin host requires to successfully complete this command exchange</td>
<td>All</td>
<td>No mapping required.</td>
<td>Yes</td>
</tr>
<tr>
<td>ToS-Traffic-Class</td>
<td>5.3.15</td>
<td>See 3GPP TS 29.212 [29].</td>
<td>All</td>
<td>HSGW may include this in the TFT sent to or received from the UE.</td>
<td>Yes</td>
</tr>
<tr>
<td>Trace-Data</td>
<td>3GPP TS 29.272 [33]</td>
<td>Contains trace control and configuration parameters, specified in 3GPP TS 32.422 [40].</td>
<td>All</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Trace-Reference</td>
<td>3GPP TS 29.272 [33]</td>
<td>Contains the trace reference parameter, specified in 3GPP TS 32.422 [40].</td>
<td>All</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Tunnel-Header-Filter</td>
<td>5.3.34</td>
<td>Defines the tunnel (outer) header filter information of a tunneled IP flow.</td>
<td>Non-3GPP</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Tunnel-Header-Length</td>
<td>5.3.35</td>
<td>Indicates the length of the tunnel (outer) header.</td>
<td>Non-3GPP</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>Tunnel-Information</td>
<td>5.3.36</td>
<td>Defines the tunnel (outer) header information for an IP flow.</td>
<td>Non-3GPP</td>
<td>No mapping required.</td>
<td>No</td>
</tr>
<tr>
<td>User-Equipment-Info</td>
<td>IETF RFC 4006 [70]</td>
<td>The identification and capabilities of the terminal (IMEISV, etc.)</td>
<td>All</td>
<td>HSGW sets this to indicate that the UE provides an IMSI MN-ID.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE 1:** When sending from the PCRF to the BBERF, the Guaranteed-Bit-Rate-UL/DL AVP indicate the allowed guaranteed bit rate for the uplink/downlink direction; when sending from the BBERF to the PCRF, the Guaranteed-Bit-Rate-UL/DL AVP indicate the requested guaranteed bit rate for the uplink/downlink direction.

**NOTE 2:** When sending from the PCRF to the BBERF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum allowed bit rate for the uplink/downlink direction; when sending from the BBERF to the PCRF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum requested bit rate for the uplink/downlink direction.

**NOTE 3:** This AVP only applies to case 2a as defined in 3GPP TS 29.213 [30].
18 Annex C (Informative) – CDR Parameters Supported for Offline Charging

The following table provides a brief description of CDR parameters specified in 3GPP TS 32.251 [38] for offline charging, along with an indication if it is required and how it is used in eHRPD. The categorization of the CDRs as Mandatory (M), Conditional (C) or Operator Optional (O_M or O_C) shall be as specified in 3GPP TS 32.251 [38]. The use of these parameters for IP CAN bearer charging (IPBC) and/or for Flow Based Bearer Charging (FBC) is also indicated.

<table>
<thead>
<tr>
<th>Field</th>
<th>Category</th>
<th>Description</th>
<th>Needed for eHRPD access</th>
<th>eHRPD Mapping</th>
<th>Charging Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Type</td>
<td>M</td>
<td>HSGW IP CAN bearer record.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Record Type</td>
<td>M</td>
<td>P-GW IP CAN bearer record.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Served IMSI</td>
<td>C</td>
<td>IMSI of the served party, if available.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>IMSI Unauthenticated Flag</td>
<td>O_C</td>
<td>Indicates the provided served IMSI is not authenticated (emergency bearer service situation).</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Served IMEISV</td>
<td>O_C</td>
<td>IMEISV of the ME, if available. Used for identifying the user in case Served IMSI is not present during emergency bearer service.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>S-GW Address used</td>
<td>M</td>
<td>The control plane IP address of the HSGW used.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Served 3GPP2 MEID</td>
<td>O_C</td>
<td>MEID of the served party’s terminal equipment for 3GPP2 access.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Served MN NAI</td>
<td>O_C</td>
<td>Mobile Node Identifier in NAI format</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>P-GW Address used</td>
<td>M</td>
<td>The control plane IP address of the P-GW used.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Charging ID</td>
<td>M</td>
<td>Charging Identifier for different records</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>PDN Connection Id</td>
<td>O_M</td>
<td>PDN Connection Id for MUPSAP</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Serving node Address</td>
<td>M</td>
<td>List of eAN/ePCF control plane IP addresses used during this record.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Serving node Address</td>
<td>M</td>
<td>List of HSGW control plane IP addresses used during this record.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Serving node Type</td>
<td>M</td>
<td>List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC Note -1</td>
</tr>
<tr>
<td>Serving node Type</td>
<td>M</td>
<td>List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Field</td>
<td>Category</td>
<td>Description</td>
<td>Needed for eHRPD access</td>
<td>eHRPD Mapping</td>
<td>Charging Mode</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S-GW Change</td>
<td>O_C</td>
<td>Present if this is the first record after HSGW change.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>PGW PLMN Identifier</td>
<td>O_C</td>
<td>PLMN identifier (MCC MNC) of the PGW used.</td>
<td>No</td>
<td>Not Supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Access Point Name Network Identifier</td>
<td>O_M</td>
<td>Logical name of the external packet data network.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>PDP/PDN Type</td>
<td>O_M</td>
<td>PDN type (i.e IPv4, IPv6 or IPv4v6).</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Served PDP/PDN Address</td>
<td>O_C</td>
<td>IP address allocated for the PDN connection, i.e. IPv4 or IPv6, if available.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Dynamic Address Flag</td>
<td>O_C</td>
<td>Indicates whether served PDN address is dynamic. This field is missing if address is static.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>List of Service Data</td>
<td>O_M</td>
<td>List of all charging data</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>List of Traffic Data Volumes</td>
<td>O_M</td>
<td>List of changes in charging conditions for this QCI/ARP pair. Charging conditions are used to categorize traffic volumes,</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Record Opening Time</td>
<td>M</td>
<td>Time stamp when IP CAN bearer is activated in this HSGW or record opening time on subsequent partial records.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>MS Time Zone</td>
<td>O_C</td>
<td>This field contains the MS Time Zone the UE is currently located as defined in TS 29.060[27] , if available.</td>
<td>No</td>
<td>Not Supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Duration</td>
<td>M</td>
<td>Duration of this record in the HSGW.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Duration</td>
<td>M</td>
<td>Duration of this record in P-GW</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Cause for Record Closing</td>
<td>M</td>
<td>The reason for the release of record from this HSGW.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Cause for Record Closing</td>
<td>M</td>
<td>The reason for the release of record from this P-GW.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>O_M</td>
<td>A more detailed reason for the release of the connection.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Record Sequence Number</td>
<td>C</td>
<td>Partial record sequence number, present in case of partial records only.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Node ID</td>
<td>O_M</td>
<td>Name of the recording entity.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Record Extensions</td>
<td>O_C</td>
<td>A set of network operator/manufacturer specific extensions to the record.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Local Record Sequence Number</td>
<td>O_M</td>
<td>Consecutive record number created by this node.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>APN Selection Mode</td>
<td>O_M</td>
<td>An index indicating how the APN was selected.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Served MSISDN</td>
<td>O_M</td>
<td>The primary MSISDN of the subscriber.</td>
<td>No</td>
<td>Not Supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Field</td>
<td>Category</td>
<td>Description</td>
<td>Needed for eHRPD access</td>
<td>eHRPD Mapping</td>
<td>Charging Mode</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>User Location Information</td>
<td>OC</td>
<td>User Location Information of the MS for GPRS case</td>
<td>No</td>
<td>Not Supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>User CSG information</td>
<td>OC</td>
<td>User CSG information of the UE</td>
<td>No</td>
<td>Not Supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>3GPP2 User Location information</td>
<td>OC</td>
<td>This field contains the User Location Information of the UE as defined in TS 29.212 [29] for 3GPP2 access, if available.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>Charging Characteristics</td>
<td>M</td>
<td>Charging Characteristics applied to the IP CAN bearer.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Charging Characteristics Selection Mode</td>
<td>OM</td>
<td>How Charging Characteristics were selected.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>IMS Signalling Context</td>
<td>OC</td>
<td>Used for IM-CN Subsystem Signalling Flag is set, see 3GPP TS 23.060 [20] IP CAN bearer is used for IMS signalling.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>External Charging Identifier</td>
<td>OC</td>
<td>A Charging Identifier received from a non-EPC, external network entity. Used of IM-CN Subsystem</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>P-GW Address used.</td>
<td>OC</td>
<td>P-GW IP Address for the Control Plane</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC</td>
</tr>
<tr>
<td>Serving Node PLMN Identifier</td>
<td>OC</td>
<td>Serving node PLMN Identifier (MCC and MNC) used during this record, if available.</td>
<td>No</td>
<td>Not supported</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>PS Furnish Charging Information</td>
<td>OC</td>
<td>Online charging session specific information</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>FBC</td>
</tr>
<tr>
<td>CAMEL Information</td>
<td>OC</td>
<td>Set of CAMEL information related to IP CAN bearer, if available. This field applies only for GPRS.</td>
<td>No</td>
<td>Not Supported</td>
<td>FBC</td>
</tr>
<tr>
<td>RAT Type</td>
<td>OC</td>
<td>Radio Access Technology (RAT) type currently used by the Mobile Station.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Start Time</td>
<td>OC</td>
<td>Time when User IP-CAN session starts, available in the CDR for the first bearer in an IP-CAN session.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
<tr>
<td>Stop Time</td>
<td>OC</td>
<td>Time when User IP-CAN session is terminated, available in the CDR for the last bearer in an IP-CAN session.</td>
<td>Yes</td>
<td>No Mapping Required</td>
<td>IPBC FBC</td>
</tr>
</tbody>
</table>

Note-1: At this time there is no definition for Serving Node Type of ‘eAN’ or ‘ePCF’ in 3GPP specifications. The operator may choose to set this field according to operator policy.
19 Annex D (Normative) – 3GPP2 Subscriber QoS Profile Parameters

The procedures in this Annex shall be applicable if the HSGW uses Subscriber QoS Profile Configuration procedures to retrieve Subscriber QoS Profile information over the Pi* reference point. The HSGW shall process SubscriberQoSProfile parameters received from the 3GPP2 AAA Proxy/Server as specified in Table 67 below. The following SubscriberQoSProfile parameters are applicable to the 3GPP2 eHRPD access network:

- Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic
- Authorized Flow Profile IDs for Each Direction
- Maximum per Flow Priority
- Service Option Profile
- Inter-User Priority for Best-Effort Traffic

Table 67 Usage of 3GPP2 SubscriberQoSProfile Parameters

<table>
<thead>
<tr>
<th>3GPP2 Access Network QoS Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic | • Shall be set to the value in the Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort Traffic parameter received from the 3GPP2 AAA Proxy/Server.  
  • The HSGW shall forward the Maximum-Authorized-Aggregate-Bandwidth-for-Best-Effort-Traffic parameter, if available, as part of the Subscriber QoS Profile via A11-Session Update message to the eAN/ePCF. |
| Authorized Flow Profile IDs for Each Direction | • Shall be set to the value in the Authorized-Flow-Profile–IDs-for-the-User AVP received from the 3GPP2 AAA Proxy/Server.  
  • HSGW shall forward Authorized Flow Profile IDs for Each Direction parameter, if available, to the eAN/ePCF via A11-Session Update message. |
| Maximum per Flow Priority | • Shall be set to the value in the Maximum-Per-Flow–Priority-for-the-User AVP received from the 3GPP2 AAA Proxy/Server.  
  • HSGW shall forward Maximum per Flow Priority parameter, if available, to the eAN/ePCF via A11-Session Update message. |
| Service Option Profile | • Shall be set to the value in the Service-Option-Profile AVP received from the 3GPP2 AAA Proxy/Server.  
  • HSGW shall forward Service Option Profile parameter, if available, to the eAN/ePCF via A11-Session Update message. |
<table>
<thead>
<tr>
<th><strong>3GPP2 Access Network QoS</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Inter-User Priority for Best-Effort Traffic | • Shall be set to the value in the Inter-User-Priority AVP received from the 3GPP2 AAA Proxy/Server.  
• HSGW shall forward Inter-User Priority for Best-Effort Traffic parameter, if available, to the eAN/ePCF via A11-Session Update message. |