

3GPP2 X.S0057-0

Version 1.0

Date: April, 2009



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

REVISION HISTORY

Revision	Description of Changes	Date
Rev 0 v1.0	Initial publication	April 2009

E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

CONTENTS

1	Introduction.....	1
2	1.1 Scope.....	1
3	1.2 Document Convention	1
4		
5		
6	2 References.....	2
7	2.1 Normative References.....	2
8		
9	3 Definitions, Symbols and Abbreviations.....	6
10	3.1 Definitions	6
11	3.1.1 Symbols and Abbreviations.....	8
12		
13	4 E-UTRAN - eHRPD Connectivity and Interworking Architecture.....	10
14	4.1 E-UTRAN – eHRPD Interworking Non-Roaming Architecture	10
15	4.2 E-UTRAN – eHRPD Interworking Roaming Architecture (Home-Routed Traffic)	11
16	4.3 E-UTRAN – eHRPD Interworking Roaming Architecture (Local Breakout)	12
17	4.4 Reference Points	13
18	4.4.1 H1/H2 Reference Points	13
19	4.4.2 Gxa Reference Point.....	13
20	4.4.3 Pi* Reference Point	13
21	4.4.4 S101 Reference Point	13
22	4.4.5 S103 Reference Point	13
23	4.4.6 S2a Reference Point.....	13
24	4.4.7 STa Reference Point.....	14
25	4.5 Protocol Stacks	15
26	4.5.1 User Plane.....	16
27	4.5.2 Control Plane	20
28		
29	5 eHRPD Functionality.....	22
30	5.1 General HSGW Capabilities	22
31	5.2 Authentication and Subscription Information Retrieval	23
32	5.2.1 EAP Protocol Negotiation	23
33	5.2.2 UE Requirements.....	23
34	5.2.3 HSGW Requirements	24
35	5.2.4 3GPP AAA Server Requirements.....	25
36	5.2.5 Call Flows.....	25
37	5.3 Use of EAP-AKA' – Fast Re-Authentication	29
38	5.4 IP Address Allocation.....	29
39	5.4.1 General	29
40	5.4.2 IPv4 Address Allocation during Default and Additional PDN Connection Establishment	34
41	5.4.3 IPv6 Prefix Allocation via IPv6 Stateless Address Auto-configuration	34
42	5.4.4 IPv4 Address Allocation in eHRPD Access using DHCPv4.....	35
43		
44		
45		
46		
47		
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		

	5.4.5	Call Flows.....	36	1
5.5		Quality of Service	44	2
	5.5.1	The EPS Bearer with PMIP-based S2a and eHRPD Access.....	45	3
	5.5.2	Mapping Parameters for Multi-PDN connectivity.....	47	4
	5.5.3	Network Initiated Dedicated Bearer Procedures for eHRPD Access.....	47	5
	5.5.4	UE Initiated Dedicated Bearer Procedures for eHRPD	51	6
5.6		Policy and Charging.....	56	7
	5.6.1	Application of 3GPP PCC to the HSGW.....	56	8
	5.6.2	3GPP Gxa Interface (Diameter).....	57	9
	5.6.3	Charging	57	10
	5.6.4	Policy interworking during handovers.....	57	11
	5.6.5	Priority and Conflict Resolution.....	57	12
	5.6.6	Mapping of QoS parameters between 3GPP and 3GPP2.....	57	13
	5.6.7	Application of 3GPP PCC to the eHRPD Access Network.....	58	14
5.7		S103 Interface: S-GW – HSGW	58	15
	5.7.1	S103 Protocol Stack.....	59	16
	5.7.2	S103 Procedures	59	17
5.8		PPP/VSNCNCP Renegotiation.....	59	18
				19
6		S2a Interface from the HSGW to the P-GW	60	20
	6.1	Protocol Definition.....	60	21
	6.2	HSGW Requirements.....	60	22
	6.2.1	PMIPv6 Triggers	60	23
	6.2.2	PMIPv6 Registration Process	61	24
	6.2.3	PMIPv6 Revocation Support	61	25
	6.3	P-GW Requirements	61	26
	6.4	Call Flows.....	62	27
	6.4.1	S2a Connection Establishment with the Default PDN.....	62	28
	6.4.2	S2a Connection Release.....	65	29
	6.4.3	S2a Connection Establishment During Pre-Registration	65	30
	6.4.4	S2a Additional PDN Connection Establishment	65	31
	6.4.5	S2a Connection Movement at Handover	65	32
	6.4.6	S2a Connection Release at De-Registration	65	33
				34
7		STa Interface from the HSGW to the AAA	66	35
				36
8		Gxa Interface from the HSGW to the PCRF	67	37
	8.1	Protocol Definition.....	67	38
	8.2	Stage 2 Flows.....	67	39
	8.2.1	Initial Attachment over S2a	68	40
	8.3	Stage 3.....	69	41
				42
9		A11 Interface from the HSGW to the eAN/ePCF	70	43
				44
10		Interface between the HSGW and the UE.....	71	45
	10.1	Main service connection between UE and HSGW	72	46
	10.1.1	Establishment of a Main Service Connection.....	72	47
				48
				49
				50
				51
				52
				53
				54
				55
				56
				57
				58
				59
				60

1	10.1.2	HSGW-UE Link Layer Encapsulation	72
2	10.1.3	PPP-Based Main Service Connection.....	72
3	10.1.4	3GPP2 Vendor Specific Network Control Protocol (VSNCP) Packet for PDN	
4		connectivity	73
5	10.1.5	3GPP2 Vendor Specific Network Protocol (VSNP) Packet Format.....	80
6	10.1.6	RSVP Protocol.....	81
7	10.1.7	Always On service in eHRPD	93
8			
9	10.2	Auxiliary service connections between UE and HSGW	94
10	10.2.1	PDN Identifier Description.....	95
11	10.3	Use of the VSNCP Protocol.....	96
12	10.3.1	UE Requested PDN Connectivity.....	96
13	10.4	Non-optimized inter-RAT handoff requirements.....	97
14			
15			
16			
17	11	Session Release Call Flows.....	98
18	11.1	UE Initiated Detach and UE-Requested PDN Disconnection Procedure.....	98
19	11.2	Network Initiated Detach and PDN Disconnection Procedure	100
20			
21	12	Inter-HSGW Handoff.....	102
22	12.1	Optimized Handoff	103
23	12.1.1	Call Flows	103
24	12.2	Dormant Handoff.....	108
25	12.2.1	Call Flows	108
26	12.3	Intra-eHRPD Handover with HSGW Relocation without Context Transfer	111
27	12.4	Inter-HSGW Stage 3	113
28	12.4.1	HSGW Requirements	113
29	12.4.2	Context Parameter TLVs.....	114
30			
31	13	Handoff FROM E-UTRAN to eHRPD	126
32	13.1	Active Mode Handoff.....	126
33	13.1.1	eHRPD Pre-registration via E-UTRAN.....	126
34	13.1.2	Handover Phase	128
35	13.2	Idle Mode Handoff.....	130
36	13.2.1	Idle Mode Mobility from E-UTRAN to eHRPD (Same eAN/ePCF)	130
37	13.2.2	Idle Mode Mobility from E-UTRAN to eHRPD (Different eAN/ePCF).....	132
38			
39			
40	14	Non-Optimized Active Handoff and Idle Mode Mobility.....	134
41	14.1	Non-Optimized Active Handoff or Idle Mode Mobility from E-UTRAN to eHRPD	
42		using PMIPv6 based S5 and S2a.....	134
43	14.2	Non-Optimized Mobility from eHRPD to E-UTRAN using PMIPv6 based S5 and S2a	136
44			
45			
46			
47			
48			
49			
50	15	Annex A (Informative) – Mapping QoS between 3GPP and 3GPP2	138
51			
52	16	Annex B (Informative) – Mapping Gxa Parameters between 3GPP and 3GPP2	143
53			
54	17	Annex C (Informative) – Mapping STa Parameters between 3GPP and 3GPP2	146
55			
56			
57			
58			
59			
60			

LIST OF FIGURES

		1
		2
		3
		4
		5
		6
		7
		8
		9
		10
		11
		12
		13
		14
		15
		16
		17
		18
		19
		20
		21
		22
		23
		24
		25
		26
		27
		28
		29
		30
		31
		32
		33
		34
		35
		36
		37
		38
		39
		40
		41
		42
		43
		44
		45
		46
		47
		48
		49
		50
		51
		52
		53
		54
		55
		56
		57
		58
		59
		60

<i>Figure 1</i>	E-UTRAN - eHRPD Interworking Non-Roaming Architecture	10
<i>Figure 2</i>	E-UTRAN – eHRPD Interworking – Roaming Architecture (Home-Routed Traffic)	11
<i>Figure 3</i>	E-UTRAN – eHRPD Interworking – Roaming Architecture (Local Breakout)	12
<i>Figure 4</i>	Protocol stack for traffic multiplexed on an SO72 Auxiliary Connection	16
<i>Figure 5</i>	Protocol stack for non-multiplexed traffic on an Auxiliary Connection	17
<i>Figure 6</i>	Main Service Connection User-Plane Protocol Stack	18
<i>Figure 7</i>	SO64 Auxiliary Service Connection User-Plane Protocol Stack	19
<i>Figure 8</i>	Main Service Connection Protocol Stack for EAP	20
<i>Figure 9</i>	Main Service Connection Control Plane Protocol Stack for VSNCIP	20
<i>Figure 10</i>	RSVP Over the Main Service Connection Using VSNCIP	21
<i>Figure 11</i>	Protocol stack for UE mobility management control using PMIPv6 over S2a	21
<i>Figure 12</i>	EAP-AKA' Authentication for eHRPD	26
<i>Figure 13</i>	IPv4 address allocation during PDN connection establishment	36
<i>Figure 14</i>	IPv4 Address Allocation using DHCPv4 with Rapid Commit Option	38
<i>Figure 15</i>	IPv4 Address Allocation using DHCPv4 without Rapid Commit Option	40
<i>Figure 16</i>	IPv6 Address Allocation	42
<i>Figure 17</i>	Sample Bearer Mapping in eHRPD	45
<i>Figure 18</i>	Network Initiated Dedicated Bearer Setup	48
<i>Figure 19</i>	Dedicated Bearer Deactivation	50
<i>Figure 20</i>	UE Requested bearer resource allocation	52
<i>Figure 21</i>	UE Requested Radio Bearer State Modification	55
<i>Figure 22</i>	HSGW Policy Enforcement	56
<i>Figure 23</i>	S103 Protocol Stack	59
<i>Figure 24</i>	S2a Connection Establishment with the Default PDN	63
<i>Figure 25</i>	Initial attachment over S2a	68
<i>Figure 26</i>	Auxiliary service connections	95
<i>Figure 27</i>	UE Requested Additional PDN Connectivity	96
<i>Figure 28</i>	UE initiated detach procedure and PDN-disconnection	98
<i>Figure 29</i>	Network initiated detach procedure and PDN-disconnection	100
<i>Figure 30</i>	Inter-HSGW Interworking Architecture in eHRPD	102
<i>Figure 31</i>	Inter-HSGW Active Handoff	104
<i>Figure 32</i>	Inter-HSGW Idle Handoff	108
<i>Figure 33</i>	Intra-eHRPD Handover with HSGW Relocation without Context Transfer	111
<i>Figure 34</i>	eHRPD Pre-registration via E-UTRAN	126
<i>Figure 35</i>	E-UTRAN to eHRPD Handover	128
<i>Figure 36</i>	E-UTRAN to eHRPD mobility in idle mode (same eAN/ePCF)	130
<i>Figure 37</i>	E-UTRAN to eHRPD mobility in idle mode (different eAN/ePCF)	132
<i>Figure 38</i>	E-UTRAN to eHRPD non-optimized handoff between PMIPv6 S5 and S2a	134
<i>Figure 39</i>	eHRPD to E-UTRAN non-optimized handover between PMIPv6 S2a and S5 (Resource Release)	136
<i>Figure 40</i>	Flow ID and QCI Applicability	139

LIST OF TABLES

Table 1	3GPP2 VSNCP packet format.....	73
Table 2	VSNCP Configuration Options.....	74
Table 3	Error Code values.....	75
Table 4	Address Allocation Cause values.....	75
Table 5	Configuration Option Data Format.....	76
Table 6	3GPP2 VSNP packet format.....	80
Table 7	TFT Error Codes.....	85
Table 8	3GPP2 OBJECT.....	86
Table 9	3GPP2 OBJECT- IE List.....	87
Table 10	3GPP2 OBJECT- IE Type #.....	87
Table 11	TFT IPv4 IE Type# = 0.....	87
Table 12	TFT IPv6 IE Type# = 2.....	88
Table 13	TFT OpCodes.....	89
Table 14	QoS List Layout.....	90
Table 15	Result Code Values.....	92
Table 16	User NAI TLV.....	114
Table 17	User MSID TLV.....	114
Table 18	LCP Info TLV.....	115
Table 19	CCP Info TLV.....	116
Table 20	VSNCP State and Common Info TLV.....	116
Table 21	PDN Info TLV.....	117
Table 22	PCO Info TLV.....	117
Table 23	PDN Address Info TLV.....	118
Table 24	PMIPv6 Info TLV.....	120
Table 25	ROHC Configuration Info TLV.....	121
Table 26	ROHC IR Info TLV.....	122
Table 27	QoS Info TLV.....	122
Table 28	TFTv4 Info TLV.....	123
Table 29	TFTv6 Info TLV.....	123
Table 30	AAA Profile Info TLV.....	124
Table 31	Gxa Info TLV.....	124
Table 32	Vendor Specific Info TLV.....	125
Table 33	MSK Info TLV.....	125
Table 34	Example of QoS Mapping.....	140
Table 35	Mapping Gxa Parameters between 3GPP and 3GPP2.....	143
Table 36	Mapping STa Parameters between 3GPP and 3GPP2.....	146

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document is the first version of this specification.

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
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1 Introduction

This document provides a specification of the functions and interfaces of the evolved High Rate Packet Data (eHRPD) Serving Gateway (HSGW) used with 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 using the eHRPD air interface to access the core network architecture defined in 3GPP TS 23.401 [14] and TS 23.402 [15]. 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.
- An interface from the HSGW to 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 (in the negative form) that 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.

2 References

2.1 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.

- [1] **3GPP2**: A.S0008-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, August 2007. (HRPD IOS)
- [2] **3GPP2**: A.S0009-C v1.0: Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function, August 2007. (HRPD IOS)
- [3] **3GPP2**: A.S0022-0 v1.0: E-UTRAN - HRPD Connectivity and Interworking: Access Network Aspects (E-UTRAN – HRPD IOS), March 2009.
- [4] **3GPP2**: A.S0017-D v1.0: Interoperability Specification (IOS) for cdma2000 Access Network Interfaces - Part 7 (A10 and A11 Interfaces), June, 2007.
- [5] **3GPP2**: X.S0011-D v1.0: cdma2000 Wireless IP Network Standard, March 2006.
- [6] **3GPP2**: C.S0024-A v3.0: cdma2000 High Rate Packet Data Air Interface Specification, April 2007.
- [7] **3GPP2**: C.R1001-G v1.0: Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards.
[Editor's Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor's Note is removed, the inclusion of the above document is for informational purposes only.]
- [8] **3GPP2**: C.S0063-A v2.0: cdma2000 High Rate Packet Data Supplemental Services, April 2007.
- [9] **3GPP2**: C.S0067-0 v1.0: Generic Key Exchange Protocol for cdma2000 High Rate Packet Data Air Interface, November 2005.
- [10] **3GPP2**: C.S0087: E-UTRAN – HRPD and cdma2000 1x Connectivity and Interworking: Air Interface Aspects.
[Editor's Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor's Note is removed, the inclusion of the above document is for informational purposes only.]

- 1 [11] **3GPP**: TS 22.278: Service requirements for the Evolved Packet System (EPS),
2 (Release 8).
3
4 [12] **3GPP**: TS 23.003: Numbering, addressing and identification.
5
6 [13] **3GPP**: TS 23.203: Policy and charging control architecture.
7
8 [14] **3GPP**: TS 23.401: GPRS Enhancements for E-UTRAN Access.
9
10 [15] **3GPP**: TS 23.402: Architecture Enhancements for non-3GPP Accesses.
11
12 [16] **3GPP**: TS 24.008: Mobile radio interface Layer 3 specification; Core network
13 protocols; Stage 3 (Release 8).
14
15 [17] **3GPP**: TS 24.301: Non-access Stratum (NAS) Protocol for Evolved Packet System
16 (EPS), Stage 3 (Release 8).
17
18 [18] **3GPP**: TS 24.302: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP
19 access networks; Stage 3; (Release 8).
20
21 [19] **3GPP**: TS 29.061: Interworking between the Public Land Mobile Network (PLMN)
22 supporting packet-based services and Packet Data Networks (PDN).
23
24 [20] **3GPP**: TS 29.212: Policy and charging control over Gx reference point.
25
26 [21] **3GPP**: TS 29.213: Policy and Charging Control signalling flows and QoS parameter
27 mapping; (release 8).
28
29 [22] **3GPP**: TS 29.273: 3GPP EPS AAA Interfaces.
30
31 [23] **3GPP**: TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling
32 protocols; Stage 3 (Release 8).
33
34 [24] **3GPP**: TS 29.276: Optimized Handover Procedures and Protocols Between E-
35 UTRAN Access and cdma2000 HRPD Access – Stage 3.
36
37 [25] **3GPP**: TS 32.240: Charging Management; Charging Architecture and Principles
38 (Release 8).
39
40 [26] **3GPP**: TS 32.251: Charging Management; Packet Switched (PS) domain charging
41 (Release 8).
42
43 [27] **3GPP**: TS 33.402: Security aspects of non-3GPP accesses.
44
45 [28] **IETF**: RFC1661: Simpson, The Point-to-Point Protocol (PPP), July 1994.
46
47 [29] **IETF**: RFC1962: Rand, The PPP Compression Control Protocol (CCP), June 1996.
48
49 [30] **IETF**: RFC2131: Dorns, “Dynamic Host Configuration Protocol”, March 1997.
50
51 [31] **IETF**: RFC2205: Braden, et al., “Resource ReSerVation Protocol (RSVP)”,
52 September 1997.
53
54 [32] **IETF**: RFC2460: Deering, et.al., “Internet Protocol, Version 6 (IPv6) Specification”,
55 December 1998.
56
57
58
59
60

- [33] **IETF**: RFC2461: Narten, et.al., “Neighbor Discovery for IP Version 6 (IPv6)”, December 1998. 1
- [34] **IETF**: RFC2462: Thomson, et.al., “IPv6 Stateless Address Autoconfiguration”, December 1998. 2
- [35] **IETF**: RFC2463: Conta, et.al., “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, December 1998. 3
- [36] **IETF**: RFC2784: Farinacci, et al., Generic Routing Encapsulation (GRE), March 2000. 4
- [37] **IETF**: RFC2890: Dommety, Key and Sequence Number Extensions to GRE, September 2000. 5
- [38] **IETF**: RFC3041: Narten, et al., Privacy Extensions for Stateless Address Autoconfiguration in IPv6, December 2001. 6
- [39] **IETF**: RFC3095: Bormann, et al., RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed, July 2001. 7
- [40] **IETF**: RFC3315: Droms, et.al., “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, July 2003. 8
- [41] **IETF**: RFC3513: Hinden, et al., “Internet Protocol Version 6 (IPv6) Addressing Architecture”, April 2003. 9
- [42] **IETF**: RFC3587: Hinden, et al., “IPv6 Global Unicast Address Format”, August 2003. 10
- [43] **IETF**: RFC3588: Calhoun, et al., “Diameter Base Protocol”, September 2003. 11
- [44] **IETF**: RFC3633: Troan, et al., IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, December 2003. 12
- [45] **IETF**: RFC3736: Droms, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”, April 2004. 13
- [46] **IETF**: RFC3748: Aboba, et al., Extensible Authentication Protocol (EAP), June 2004. 14
- [47] **IETF**: RFC3772: Carlson, et al., PPP Vendor Protocol, May 2004. 15
- [48] **IETF**: RFC4005: Calhoun, et al., “Diameter Network Access Server Application”, August 2005. 16
- [49] **IETF**: RFC4039: Park, et al., “Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)”, March 2005. 17
- [50] **IETF**: RFC4072: Eronen, et al., “Diameter Extensible Authentication Protocol (EAP) Application”, August 2005. 18
- [51] **IETF**: RFC4862: Thomson, et al., IPv6 Stateless Address Autoconfiguration, September 2007. 19

- 1 [52] **IETF**: RFC5213: Gundavelli, et al., Proxy Mobile IPv6, August 2008.
- 2
- 3 [53] **IETF**: draft-ietf-mipshop-pfmipv6, Fast Handovers for Proxy Mobile IPv6.
4 [Editor's Note: The above document is a work in progress and should not be
5 referenced unless and until it is approved and published. Until such time as this
6 Editor's Note is removed, the inclusion of the above document is for informational
7 purposes only.]
- 8
- 9 [54] **IETF**: draft-ietf-mext-binding-revocation, Binding Revocation for IPv6 Mobility.
10 [Editor's Note: The above document is a work in progress and should not be
11 referenced unless and until it is approved and published. Until such time as this
12 Editor's Note is removed, the inclusion of the above document is for informational
13 purposes only.]
- 14
- 15 [55] **IETF**: draft-ietf-netlmm-pmip6-ipv4-support, IPv4 Support for Proxy Mobile IPv6.
16 [Editor's Note: The above document is a work in progress and should not be
17 referenced unless and until it is approved and published. Until such time as this
18 Editor's Note is removed, the inclusion of the above document is for informational
19 purposes only.]
- 20
- 21
- 22 [56] **IETF**: draft-arkko-eap-aka-kdf, Improved Extensible Authentication Protocol
23 Method for 3rd Generation Authentication and Key Agreement (EAP-AKA').
24 [Editor's Note: The above document is a work in progress and should not be
25 referenced unless and until it is approved and published. Until such time as this
26 Editor's Note is removed, the inclusion of the above document is for informational
27 purposes only.]
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

3 Definitions, Symbols and Abbreviations

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

3.1 Definitions

APN

An APN is an Access Point Name as defined in TS 23.003 [12].

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 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 [15]. 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 [15].

EPC

The evolved packet core: The EPC domain name is defined in TS 23.003 [12]. The EPC architecture is defined in TS 23.401 [14], and TS 23.402 [15].

EPS

The evolved packet system is defined in TS 23.003 [12], TS 23.401 [14], and TS 23.402 [15]. 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-D 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 “handover” 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).

Legacy AT

A legacy AT is defined as an AT that is compliant to X.S0011-D [5], and 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-D [5]. Within this specification, the use of “PDSN” implies a legacy PDSN.

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.

UE

In this specification, a UE is the User Equipment.

3.1.1 Symbols and Abbreviations

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization, Accounting
AKA	Authentication and Key Agreement
AMBR	Aggregated Maximum Bit Rate
APN	Access Point Name
AT	Access Terminal
AVP	Attribute Value Pair
BBERF	Bearer Binding and Event Reporting Function
BCM	Bearer Control Mode
BE	Best Effort
BLOB	BLOCK Of Bits
CCP	Compression Configuration Protocol
CMIP	Client Mobile IP
DHCP	Dynamic Host Configuration Protocol
DL	Down Link
eAN	evolved Access Network
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePCF	evolved Packet Control Function
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network

1	FQDN	Fully Qualified Domain Name
2	GBR	Guaranteed Bit Rate
3	GRE	Generic Routing Encapsulation
4	HRPD	High Rate Packet Data
5	HSGW	HRPD Serving Gateway
6	HSS	Home Subscriber Server
7	IMSI	International Mobile Subscriber Identity
8	IP	Internet Protocol
9	IP-CAN	IP Connectivity Access Network
10	LCP	Link Control Protocol
11	LMA	Local Mobility Agent
12	MAG	Mobile Access Gateway
13	MBR	Maximum Bit Rate
14	MME	Mobility Management Entity
15	MSID	Mobile Station ID
16	MSK	Master Session Key
17	NAI	Network Access Identifier
18	OUI	Organizationally Unique Identifier
19	P-GW	Packet Data Network Gateway (specified by 3GPP)
20	PBA	Proxy Binding Acknowledgement
21	PBU	Proxy Binding Update
22	PCEF	Policy and Charging Enforcement Function
23	PCO	Protocol Configuration Options
24	PCRF	Policy and Charging Rules Function
25	PDN	Packet Data Network
26	PDN-ID	PDN Identifier
27	PDSN	Packet Data Serving Node
28	PMIP	Proxy Mobile IP
29	PPP	Point-to-Point Protocol
30	QCI	QoS Class Index
31	QoS	Quality of Service
32	RA	Router Advertisement
33	RAN	Radio Access Network
34	RAT	Radio Access Technology/Radio Access Type
35	ROHC	RObust Header Compression
36	RS	Router Solicitation
37	RSVP	Resource Reservation Protocol
38	S-GW	Serving Gateway (specified by 3GPP)
39	SDF	Service Data Flow (specified by 3GPP)
40	SLAAC	Stateless Address Autoconfiguration
41	TNL	Transport Network Layer
42	TFT	Traffic Flow Template
43	TLV	Type Length Value
44	UE	User Equipment
45	UL	Uplink
46	VSA	Vendor Specific Attribute
47	VSNC	Vendor Specific Network Control Protocol
48	VSNP	Vendor Specific Network Protocol
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		

4 E-UTRAN - eHRPD Connectivity and Interworking Architecture

4.1 E-UTRAN – eHRPD Interworking Non-Roaming Architecture

Figure 1 below 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 [15], 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 [24]). Note that the eAN/ePCF functions are defined in A.S0022-0 [3],
- S103: the bearer interface between the Evolved Packet Core (EPC) Serving Gateway (S-GW) and the HSGW (ref. TS 29.276 [24]),

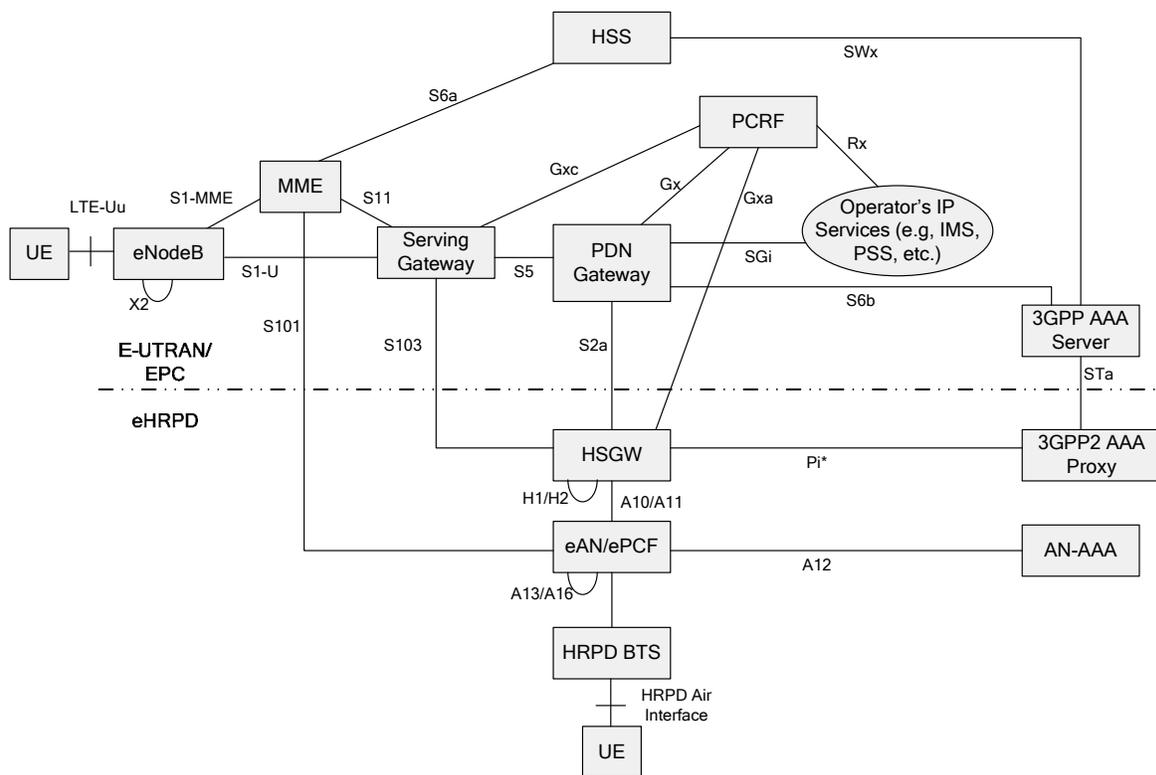


Figure 1 E-UTRAN - eHRPD Interworking Non-Roaming Architecture

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.2 E-UTRAN – eHRPD Interworking Roaming Architecture (Home-Routed Traffic)

Figure 2 below 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.

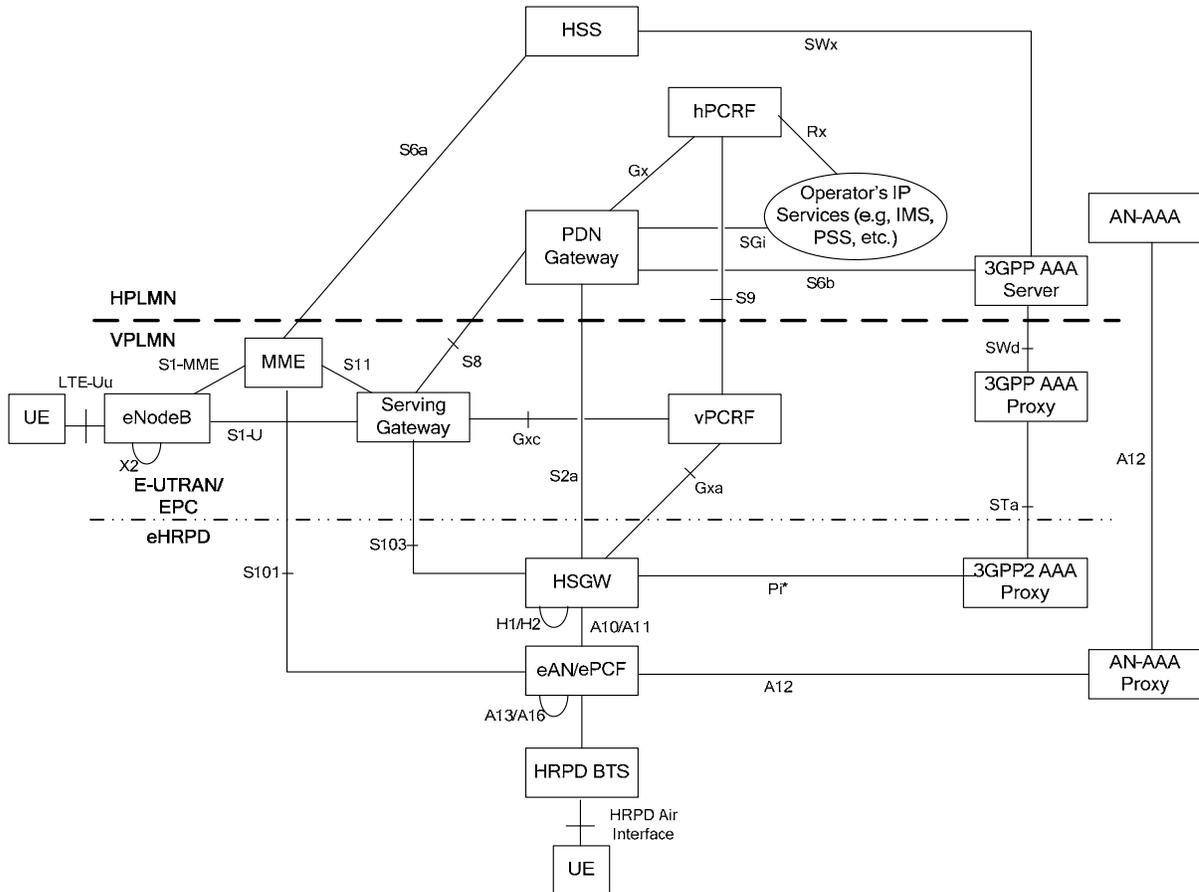


Figure 2 E-UTRAN – eHRPD Interworking – Roaming Architecture (Home-Routed Traffic)

4.3 E-UTRAN – eHRPD Interworking Roaming Architecture (Local Breakout)

Figure 3 below 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.

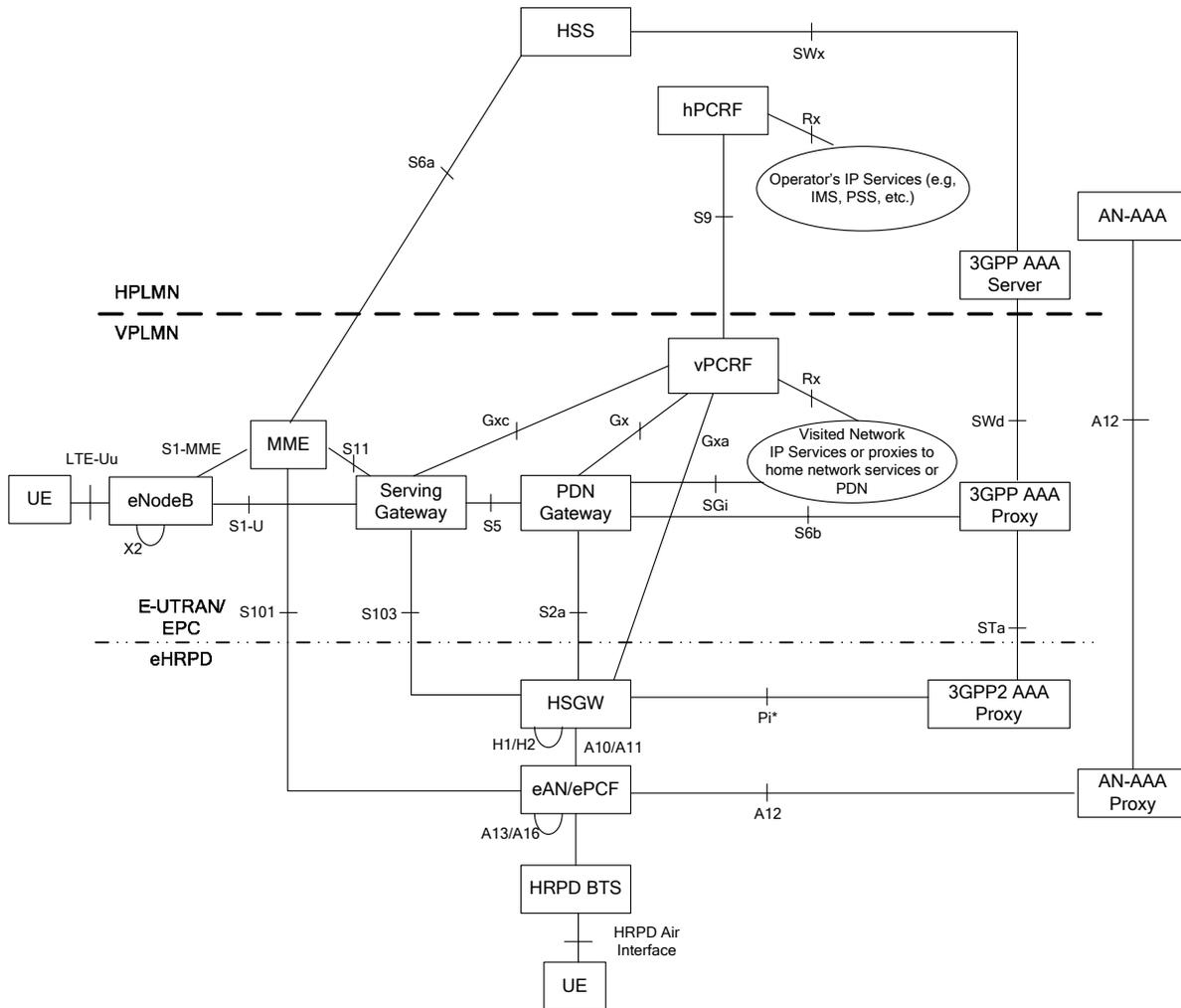


Figure 3 E-UTRAN – eHRPD Interworking – Roaming Architecture (Local Breakout)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.4 Reference Points

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

4.4.1 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 between a source HSGW (S-HSGW) and a target HSGW (T-HSGW) for optimized inter-HSGW handoff.

4.4.2 Gxa Reference Point

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

Detailed requirements and operation of this interface is defined in TS 23.203 [13], TS 29.212 [20] and TS 29.213 [21].

4.4.3 Pi* Reference Point

The Pi* reference point connects the HSGW to the 3GPP2 AAA Proxy. The Pi* reference point is identical to the STa reference point.

4.4.4 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.S0022-0 [3]. 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 [15] and TS 29.276 [24].

4.4.5 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 DL 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 [15] and TS 29.276 [24].

4.4.6 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 [18], TS 29.275 [23], and Section 5.8.

4.4.7 STa Reference Point

The STa reference point connects the AAA in the 3GPP EPC to the AAA 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 [12] and TS 29.273 [22].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.5 Protocol Stacks

The protocol supported on the S2a interface is PMIPv6 per TS 29.275 [23].

The following apply to the S2a interface between the HSGW and the P-GW:

- The PMIPv6 MAG and LMA functionality reside in the HSGW and P-GW, respectively.
- The mobility management control plane stack is PMIPv6 over IPv6/IPv4.
- The user plane carries IPv4/v6 packets over either an IPv4 or an IPv6 transport network.

The figures in the following subsections illustrate the user plane and the control plane protocol stacks 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 per-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.

4.5.1 User Plane

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

4.5.1.1 User Plane Traffic via SO72

The protocol stack in Figure 4 indicates that traffic from 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.

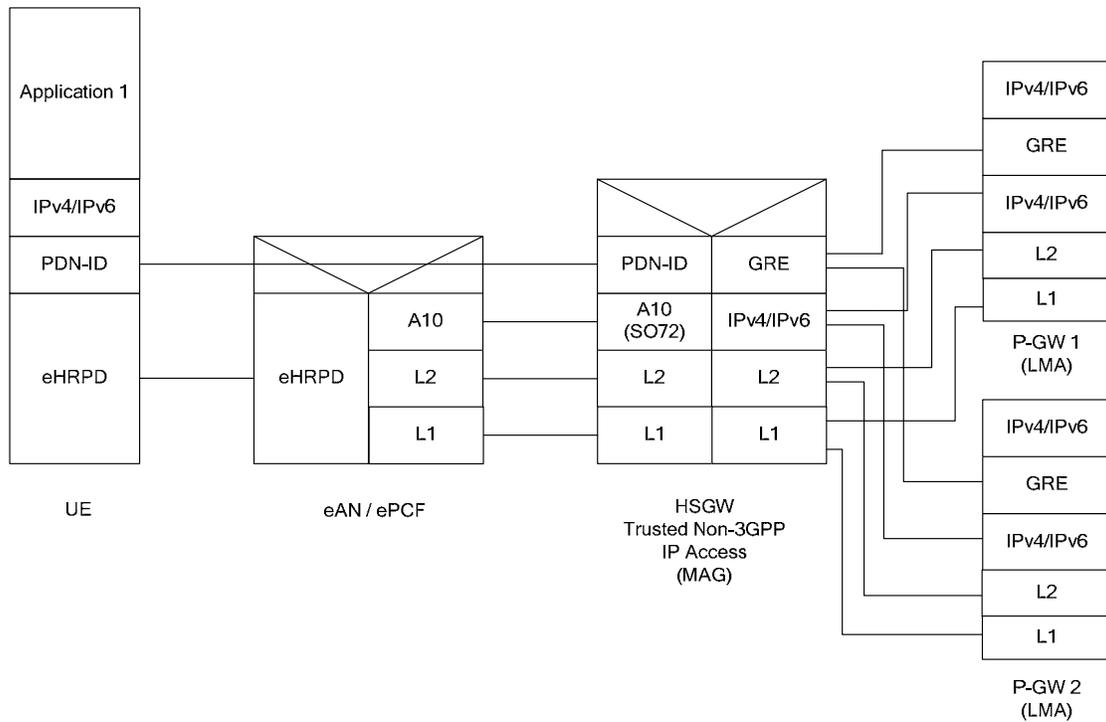


Figure 4 Protocol stack for traffic multiplexed on an SO72 Auxiliary Connection

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.5.1.2 User Plane Traffic via SO67

Figure 5 illustrates the use of an auxiliary service connection that is dedicated to one or more IP flows with similar QoS characteristics from a single PDN. This type of auxiliary service connection uses SO67 and does not involve use of the PDN-ID for multiplexing. Such a service connection may be used for, for example, VoIP traffic or streaming video. Header compression may be configured for an SO67 auxiliary service connection.

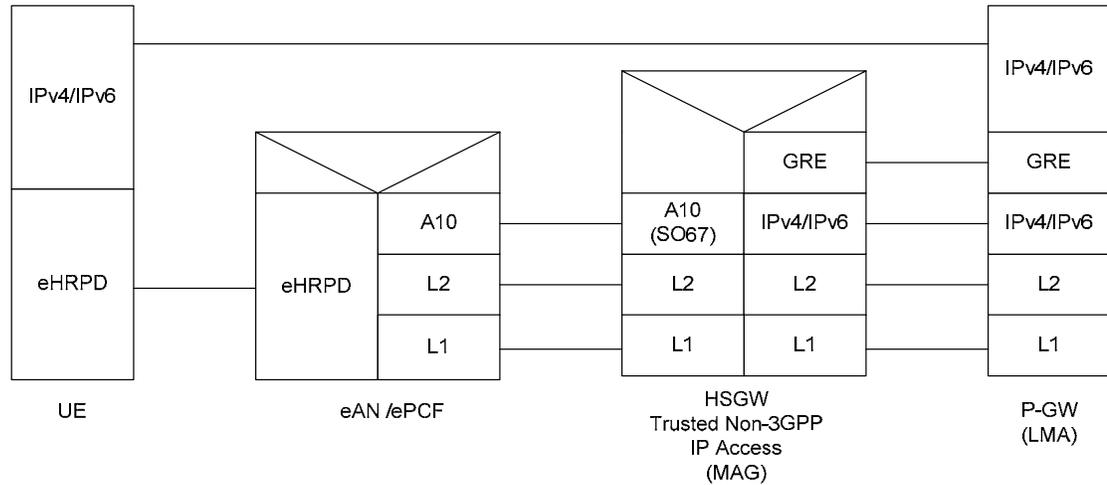


Figure 5 Protocol stack for non-multiplexed traffic on an Auxiliary Connection

4.5.1.3 User Plane Traffic via VSNP on the Main Service Connection

The protocol stack in Figure 6 indicates that traffic from 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 4.5.2.

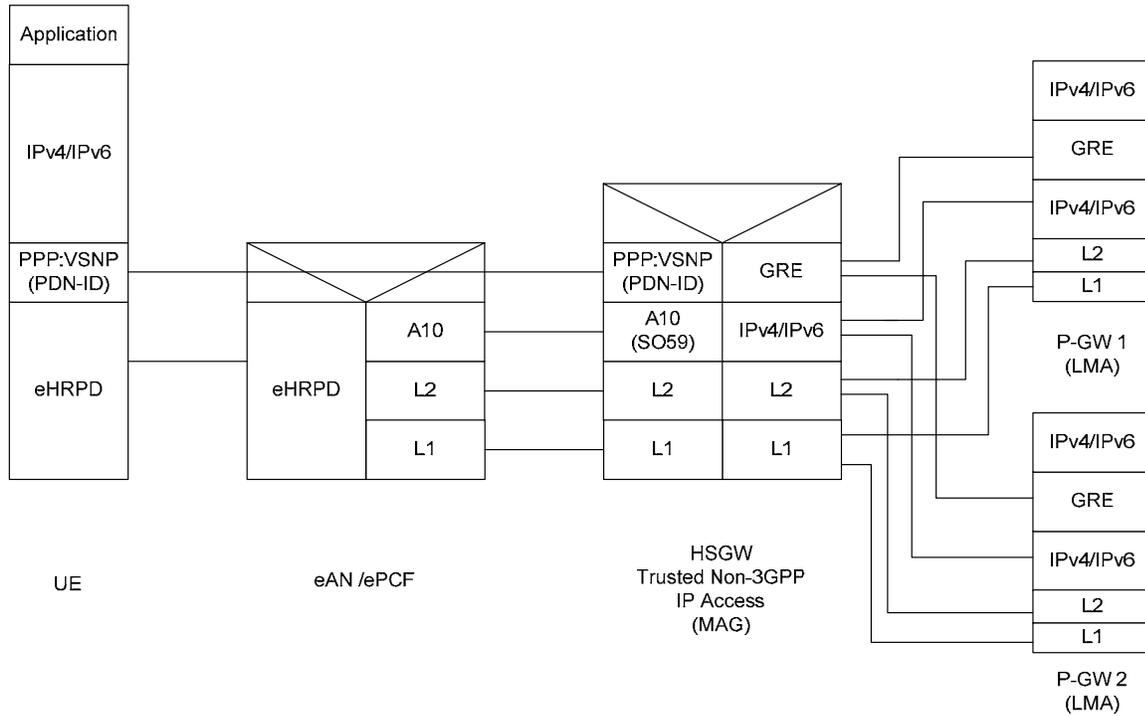


Figure 6 Main Service Connection User-Plane Protocol Stack

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.5.1.4 User Plane Traffic via SO64

The protocol stack in Figure 7 indicates that traffic from 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.

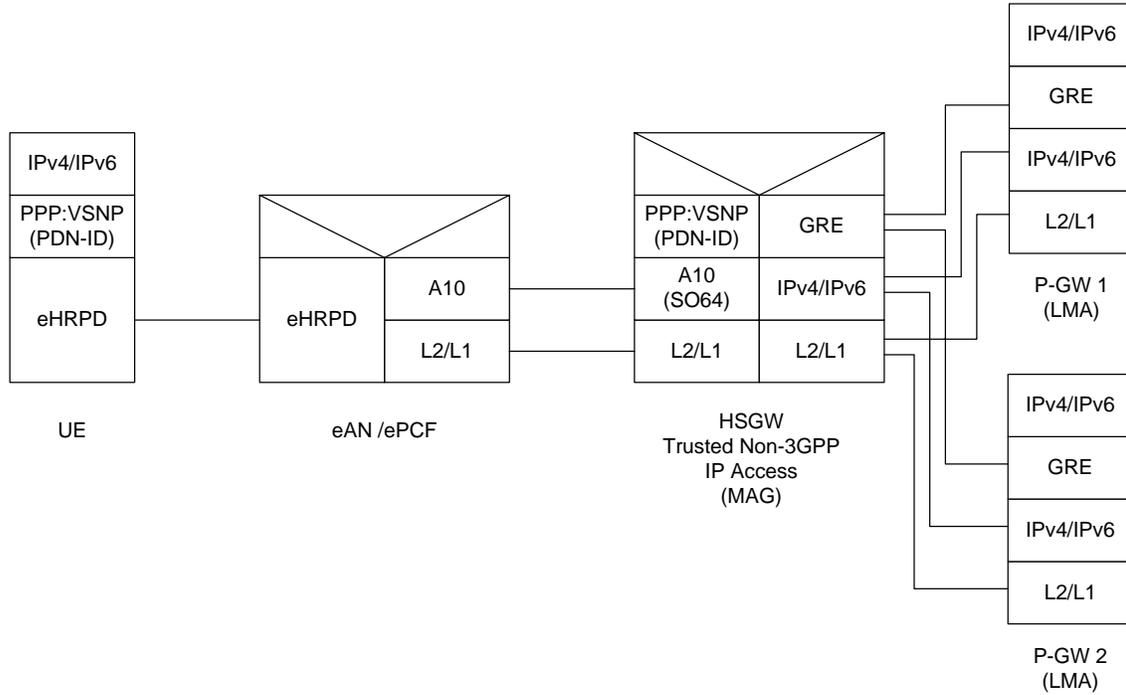


Figure 7 SO64 Auxiliary Service Connection User-Plane Protocol Stack

4.5.2 Control Plane

4.5.2.1 Control Plane HSGW to UE – EAP

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

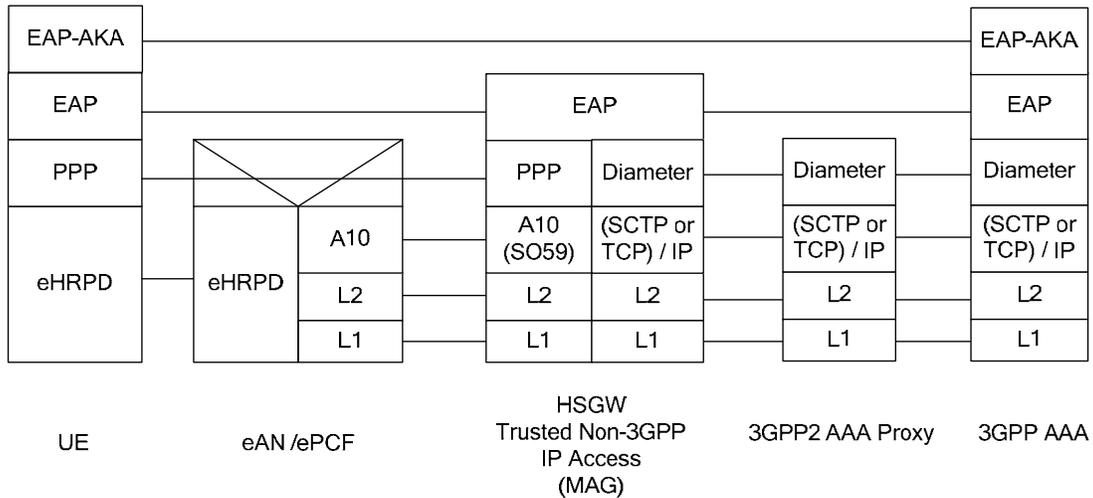


Figure 8 Main Service Connection Protocol Stack for EAP

4.5.2.2 Control Plane HSGW to UE – VSNCP

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

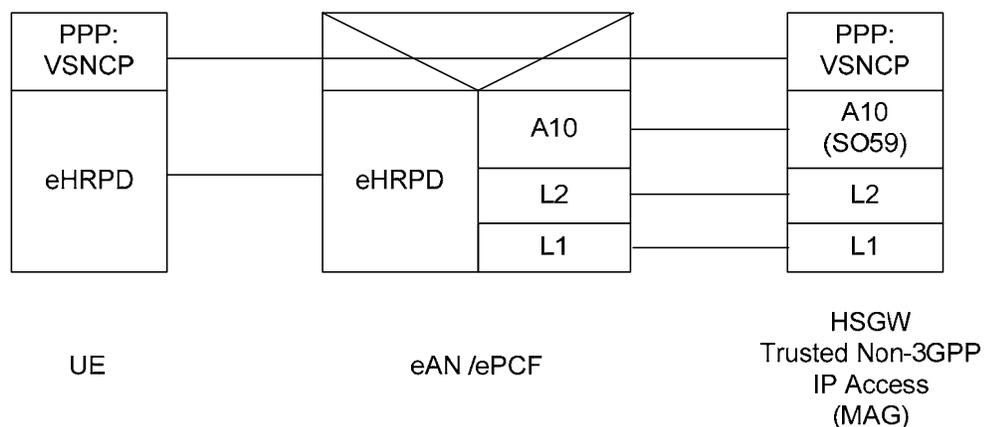


Figure 9 Main Service Connection Control Plane Protocol Stack for VSNCP

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.5.2.3 Control Plane HSGW to UE – RSVP

RSVP signaling is carried as IP traffic within the user plane. See Figure 10 below. The PDN-ID is used to specify the PDN to which the RSVP message applies.

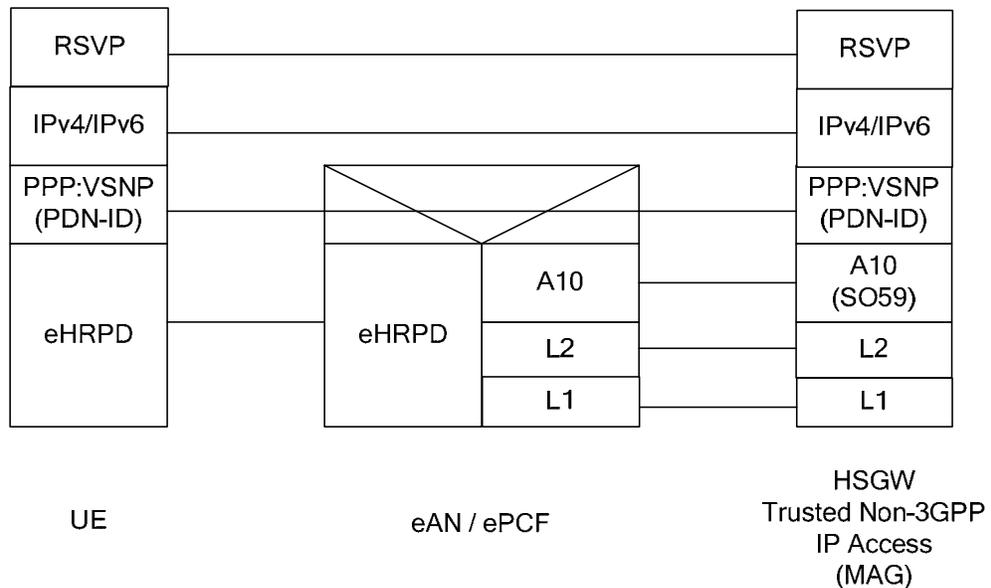


Figure 10 RSVP Over the Main Service Connection Using VSNP

4.5.2.4 Control Plane HSGW to P-GW – PMIPv6

The PMIPv6 signaling specified in RFC 5213 [52] is used to manage mobility between the P-GW and multiple HSGWs. See Figure 11 below.

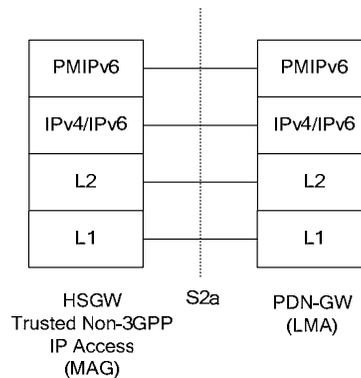


Figure 11 Protocol stack for UE mobility management control using PMIPv6 over S2a

5 eHRPD Functionality

5.1 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 A.S0022-0 [3]. 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 [15]. This includes support for mobility, policy control and charging (PCC), access authentication, and roaming. The HSGW shall support inter-HSGW handoff with context transfer. The HSGW may use inter-HSGW handoff without context transfer.

The HSGW supports seamless inter-technology mobility between E-UTRAN and eHRPD. The following requirements exist:

- a. An optimized handoff bearer interruption shall be less than the 300 msec interruption time for the RAT change procedures specified in TS 22.278 [11].
- b. Inter-technology handoff between 3GPP E-UTRAN and eHRPD shall be supported.
- c. Inter-HSGW handoff shall be supported using S2a (PMIPv6).

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 UL traffic that does not comply with established uplink policy.
- i. MAG functions for S2a mobility (i.e., Network-based mobility based on PMIPv6).
- j. Support for IPv4 and IPv6 address assignment.
- k. Authenticator function.
- l. Policy enforcement functions defined for the Gxa interface.
- m. Support for ROHC.
- n. Support for PPP-based operation (i.e., 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.

- 1 q. Examination of the PCO received from the UE to extract the Address Allocation
2 Preference and BCM values. The Address Allocation Preference is used by the HSGW
3 to determine whether the PDN address will be sent in VSNCP or not. The value of
4 BCM is used by the HSGW to determine whether the UE supports network initiated
5 bearer or not.
6

7 **5.2 Authentication and Subscription Information Retrieval**

9 This section defines eHRPD authentication and authorization procedures.

10 When eHRPD access is used to connect to the 3GPP EPC, 3GPP based access authentication
11 is required across a SWx/STa/Pi* reference point as depicted in section 4. The following
12 principles shall apply in this case:
13

- 14 - Transport of authentication signaling shall be independent of the eHRPD technology.
- 15 - Access authentication signaling shall be based on IETF protocols, for e.g., Extensible
16 Authentication Protocol (EAP) as specified in RFC 3748 [46].
- 17 - Access authentication signaling procedures shall be based on TS 33.402 [27].

18 EAP-AKA' authentication shall follow trusted non-3GPP access procedures specified in TS
19 33.402 [27]. The UE as the EAP Peer and the 3GPP AAA as the EAP Authentication Server
20 mutually authenticate each other using the EAP-AKA' procedures. Upon successful
21 authentication, if the UE is authorized to access the network, the 3GPP AAA sends the Master
22 Session Key (MSK) to the HSGW which acts as the EAP Authenticator.
23

24 **5.2.1 EAP Protocol Negotiation**

25 During the PPP session negotiation between the HSGW and the UE, the HSGW shall propose
26 EAP as the authentication protocol in the LCP Configure-Request message by setting
27 Authentication-Protocol option to C227 (see RFC 3748 [46]).
28

29 Once the UE receives an LCP Configure-Request message from the HSGW that contains the
30 Authentication-Protocol option that is set to C227, the UE shall respond with LCP Configure-
31 Ack, indicating to the HSGW the acceptance of EAP based authentication for PPP session
32 establishment as described in RFC 3748 [46] and RFC 1661 [28].
33

34 If the HSGW receives LCP Configure-Ack from the UE indicating the acceptance of EAP
35 based authentication, the HSGW shall select EAP as the PPP authentication protocol and
36 proceed to play the role of EAP authenticator.
37

38 **5.2.2 UE Requirements**

39 The UE shall support the EAP-AKA' protocol defined in TS 33.402 [27] for Network Access
40 Authentication.
41

42 **5.2.2.1 UE Identity Management**

43 The UE shall have a permanent ID that is an IMSI-based NAI as defined in TS 23.003 [12].
44 The UE shall support temporary identities (pseudonym and fast-reauthentication) as specified
45 in 3GPP TS 24.302 [18] and 3GPP TS 33.402 [27]. Temporary identities are defined in 3GPP
46 TS 23.003 [12] and are one time identities.
47

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 3GPP TS 23.003 [12]. See TS 24.302 [18] for further information on UE identity management.

If upon successful EAP-AKA' access authentication (see draft-arkko-eap-aka-kdf [56]), a protected pseudonym and/or re-authentication identity were received, the UE shall store the temporary identity(s) for future authentications.

5.2.2.2 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 AUTN is incorrect per draft-arkko-eap-aka-kdf [56] and TS 33.402 [27], the UE shall reject the authentication. If the sequence number is out of synch, the UE shall initiate a synchronization procedure, c.f. draft-arkko-eap-aka-kdf [56].

If AUTN is correct, the UE shall compute MAC and 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 MAC and RES to the HSGW in the EAP Response / AKA' Challenge, as specified in draft-arkko-eap-aka-kdf [56].

5.2.2.3 UE Key Generation for Access Security

The UE shall derive required additional new keying material, including the key MSK, according to EAP-AKA' draft-arkko-eap-aka-kdf [56] and TS 33.402 [27] from the new computed CK', IK' and check the received 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 PairwiseMasterKeyID associated with each PMK as specified in C.S0067 [9]. In addition, the UE may also pre-compute the PMKs, PairwiseMasterKeyIDs associated with the other Sub-MSKs. This pre computation of PMKs, 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.

Because EAP-AKA' does not support Master Session Key (MSK) lifetime negotiation, the UE shall rely on the HSGW (EAP Authenticator), to initiate EAP re-authentication prior to MSK expiry.

5.2.3 HSGW Requirements

The HSGW shall support the following RFCs:

- RFC 3748 [46], Extensible Authentication Protocol (EAP).
- draft-arkko-eap-aka-kdf [56].

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.

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 12.4.1. The HSGW shall use the Sub-MSK for the computation of PMKs using the procedures specified in section 5.2.2.3. 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 Response (or) A11-Session Update message [1] if the ePCF has indicated in the A11-RRQ 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.

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

- RFC 3588 [43], Diameter Base Protocol.
- RFC 4005 [48], Diameter Network Access Server Application.
- RFC 4072 [50] Diameter Extensible Authentication Protocol (EAP) Application.

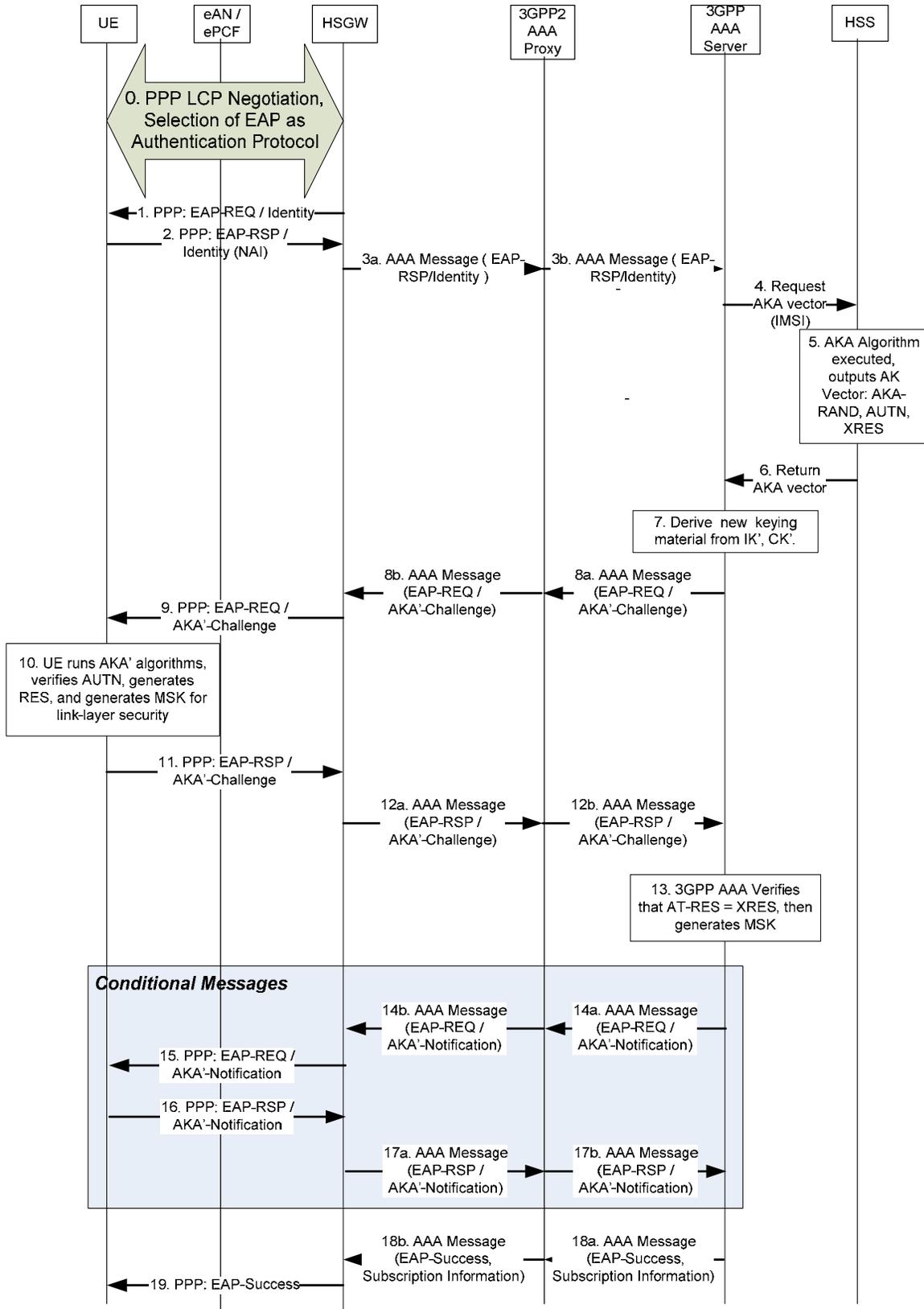
5.2.4 3GPP AAA Server Requirements

3GPP AAA Server requirements are defined in TS 29.273 [22] and in TS 24.302 [18].

5.2.5 Call Flows

5.2.5.1 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 draft-arkko-eap-aka-kdf [56]. The subscription information from the HSS/AAA is also retrieved during this procedure.



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Figure 12 EAP-AKA' Authentication for eHRPD

- 1 0. PPP LCP negotiation occurs. EAP is negotiated as the authentication protocol.
- 2 1. The HSGW sends an EAP-Request / Identity message to the UE over the A10 main signaling
- 3 connection.
- 4
- 5 2. The UE responds with EAP-Response / Identity (NAI). If UE uses its permanent NAI, it shall use
- 6 the IMSI-based Network Access Identifier (NAI) format specified in 3GPP TS 23.003 [12]. The
- 7 format of the NAI shall comply with the format specified in 3GPP TS 23.003 [12].
- 8
- 9 3. The HSGW forwards the unmodified NAI received in the EAP-Response/Identity message to the
- 10 EAP Server in the 3GPP AAA.
- 11
- 12 3a: The HSGW, as the authenticator, encapsulates the EAP payload in a AAA message and
- 13 forwards it, along with the access type (i.e., RAT type), and NAS-ID = {the FQDN of the HSGW}
- 14 to the 3GPP2 AAA Proxy. The HSGW shall also include the access network identity to assist the
- 15 3GPP AAA server in determining the access network name (See Step 4). The format of the
- 16 network identity is specified in TS 24.302 [18].
- 17
- 18 3b.The 3GPP2 AAA Proxy forwards the unmodified contents to the 3GPP AAA Server.
- 19
- 20 4. The 3GPP AAA Server will terminate the EAP protocol. If the UE identified itself with the
- 21 pseudonym, the 3GPP AAA server determines the real identity of the UE and derives the IMSI
- 22 from it. The 3GPP AAA Server checks that it has an unused authentication vector with AMF
- 23 separation bit = 1 and the matching access network identifier available for that subscriber. If not, a
- 24 set of new authentication vectors is retrieved from HSS using IMSI. In order to retrieve the new
- 25 vectors from the HSS, the 3GPP AAA server determines the network name and ensures that the
- 26 given access network is authorized to use the claimed name. The access network name determined
- 27 by the 3GPP AAA is included in the AT_KDF_INPUT attribute of the message sent to HSS.
- 28
- 29 5. The HSS calculates the AKA vector(s). The HSS then transforms this AKA vector as specified in
- 30 TS 33.402 [27].
- 31
- 32 6. The HSS returns the transformed AKA' vector(s), including RAND, AUTN, and XRES, IK' and
- 33 CK', to the 3GPP AAA. The 3GPP AAA Server stores the received AKA' vector(s).
- 34
- 35 7. New keying material is derived from IK' and CK' according to EAP-AKA' (see draft-arkko-eap-
- 36 aka-kdf [56]). A new pseudonym and/or re-authentication ID may be chosen and if chosen are
- 37 protected (i.e., encrypted and integrity protected) using keying material generated from EAP-
- 38 AKA'.
- 39
- 40 8. The 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC), AT_KDF,
- 41 AT_KDF_INPUT and two user identities (if they are generated): protected pseudonym and/or
- 42 protected re-authentication id in EAP Request/AKA'-Challenge message. The sending of the re-
- 43 authentication ID depends on the operator's policies on whether to allow fast re-authentication
- 44 processes or not. It implies that, at any time, the 3GPP AAA Server decides (based on policies set
- 45 by the operator) whether to include the re-authentication id or not, thus allowing or disallowing
- 46 the triggering of the fast re-authentication process. The 3GPP AAA Server may use a protected
- 47 success indication by including the AT_RESULT_IND attribute in the EAP Request/AKA'-
- 48 Challenge message, in order to indicate to the UE that it would like result indications in both
- 49 successful and unsuccessful cases.. The inclusion of the result indications for the protection of the
- 50 result messages depends on home operator's policies.
- 51
- 52 8a: The 3GPP AAA Server sends the EAP-Request / AKA'-Challenge and the other parameters to
- 53 the 3GPP2 AAA Proxy.
- 54
- 55 8b. The 3GPP2 AAA Proxy forwards the EAP-Request / AKA'-Challenge and other parameters to
- 56 the HSGW.
- 57
- 58 9. The HSGW sends the EAP-Request / AKA'-Challenge and other parameters to the UE.
- 59
- 60

10. The UE runs the AKA algorithms on the UE. The UE verifies that AUTN is correct and thereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, the terminal initiates a synchronization procedure (not shown in this example), c.f. draft-arkko-eap-aka-kdf [56]. If AUTN is correct, the UE computes RES, IK' and CK'. The UE derives required additional new keying material, including the key MSK, according to draft-arkko-eap-aka-kdf [56] and 3GPP TS 24.302 [18] from the new computed IK' and CK', and checks the received 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.
11. The UE calculates a new MAC value covering the EAP message with the new keying material. UE sends EAP Response/AKA'-Challenge containing calculated RES and the new calculated MAC value to the HSGW. The UE includes in this message the result indication if it received the same indication from the 3GPP AAA Server. Otherwise, the UE omits this indication.
12. The HSGW sends the authentication response to the EAP server.
- 12a: 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.
- 12b. The 3GPP2 AAA Proxy forwards the message to the 3GPP AAA Server.
13. The 3GPP AAA Server checks the received MAC and verifies the AT-RES value to the XRES value from the AKA vector received in step 6 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 8, it now associates these identities with the permanent identity of the UE.
- Steps 14 through 17 are conditional based on the EAP Server and the UE having indicated the use of protected successful result indications (see steps 8 and 10).
14. If the 3GPP AAA Server requested previously to use protected result indications and received the same result indications from the UE as in draft-arkko-eap-aka-kdf [56], the 3GPP AAA Server sends the message EAP Request/AKA'-Notification.
- 14a: The 3GPP AAA Server sends EAP Request/AKA'-Notification to the 3GPP2 AAA Proxy.
- 14b. The 3GPP2 AAA Proxy forwards it to the HSGW.
15. The HSGW sends EAP Request/AKA'-Notification to the UE.
16. The UE sends EAP Response/AKA'-Notification to the HSGW.
17. 17a: The HSGW encapsulates the EAP-Response / AKA'-Notification in a AAA message and sends it to the 3GPP2 AAA Proxy.
- 17b. 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".
18. 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 (draft-arkko-eap-aka-kdf [56]), in the underlying AAA protocol message (i.e., not at the EAP level).
- 18a: The 3GPP AAA Server sends The EAP-Success message and other parameters (e.g., AMBR) in a AAA message to the 3GPP2 AAA Proxy.
- 18b. The 3GPP2 AAA Proxy forwards the information including the subscription information elements (defined in 29.273 [22]) 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.

19. 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 9, 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 MACs or no response from the UE after a network request. In that case, the EAP AKA process will be terminated as specified in draft-arkko-eap-aka-kdf [56] and an indication shall be sent to the HSS.

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

EAP-AKA' Fast Re-Authentication shall be supported per draft-arkko-eap-aka-kdf [56] and as specified in TS 24.302 [18] and 3GPP TS 33.402 [27]. 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 the fast re-authentication for EAP-AKA' to the UE by sending the re-authentication identity to the UE.

5.4 IP Address Allocation

This section specifies IP address allocation in eHRPD.

5.4.1 General

The requirements and procedures of this section are per TS 23.401 [14] and TS 23.402 [15].

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. 1
3. Configure the 128-bits IPv6 address using IPv6 SLAAC (see RFC 4862 [51]). 2
4. IPv6 parameter configuration via Stateless DHCPv6. 3

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. 4

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. 5

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: 6

- 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 VSNCNCP procedures specified in section 10.1.4. 7
- 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 [29]) procedures, the HSGW shall not provide the IPv4 address for the UE as part of procedures used to establish the PDN connection. The HSGW shall respond to the UE by setting the PDN Address field to 0.0.0.0. After the PDN connection establishment procedure is completed, the UE initiates the IPv4 address configuration on its own using DHCPv4. See details in section 5.4.4). 8

The HSGW is responsible for delivering the IPv4 address and/or IPv6 prefix to the UE. 9

The HSGW shall support the following mechanisms: 10

- a. IPv4 address allocation during PDN connection establishment procedures (per section 8.2.1 and 10.3.1). 11
- b. IPv4 address allocation after PDN connection establishment procedures (e.g., via DHCPv4). 12

The eHRPD network shall also support the following mechanisms following the PDN connection establishment procedures: 13

- a. /64 IPv6 prefix allocation via IPv6 Stateless Address auto-configuration according to RFC 4862 [51]; 14
- b. IPv4 address allocation and IPv4 parameter configuration via DHCPv4 according to RFC 2131 [29] and RFC 4039 [49]. See call flows in Section 5.4.5.1 and Section 5.4.5.3 for details; 15
- c. IPv6 parameter configuration via Stateless DHCPv6 according to RFC 3736 [45]. 16

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 VSNCNCP message. The HSGW shall convey the assigned IPv6 prefix to the UE using Router Advertisement. 17

5.4.1.1 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 10.1.4.

For PMIPv6 stage 3 protocol details, refer to 3GPP TS 29.275 [23].

Note: TS 23.401 [14] 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 PBA is specified in TS 29.275 [23], "3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication option", which indicates to the HSGW that deferred allocation is used.

5.4.1.1.1 IP Address Allocation: VSNCP Configure-Request

INITIAL ATTACH

There are four 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.

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 10.1.4.1. 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 [23].

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

HANDOVER ATTACH

There are four parameters of significance to the IP address allocation process that 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.

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 10.1.4.1.1 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 [23].

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

5.4.1.1.2 IP Address Allocation: Proxy Binding Update

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 10.1.4.5.

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 [xx]) 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.

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.

5.4.1.1.3 IP Address Allocation: Proxy Binding Acknowledgement

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 [15] and TS 29.275 [23]). 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 Proxy Binding Acknowledgement (PBA) message.

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

1 deferred IPv4 address allocation, the Vendor-Specific Mobility Option of subtype “3GPP
2 Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication” is returned to
3 the HSGW in the PBA (see TS 29.275 section 12.1.1.5 [23]).
4

5 If the HSGW had indicated IPv4 and IPv6 capabilities in the PBU, but the P-GW decided to
6 allocate only IPv4 or IPv6, the P-GW also includes the Vendor-Specific Mobility Option of
7 subtype “3GPP Vendor-Specific PMIPv6 PDN Type Indication” in the PBA to indicate the
8 actual allocation and a cause value to indicate the reason for the change.
9

10 **HANDOVER ATTACH**

11 When the P-GW receives the PBU containing an indication for handover attach, it follows the
12 3GPP EPC procedures for handover (see TS 23.402 [15] and TS 29.275 [23]). If the P-GW
13 determines that the handover attachment to the APN cannot be completed, it will indicate that
14 via the Status field in a Proxy Binding Acknowledgement (PBA) message.
15

16 Assuming there are no errors, the P-GW returns a PBA message to the HSGW.
17

18 **5.4.1.1.4 IP Address Allocation: VSNCP Configure-Ack**

19 **INITIAL ATTACH and HANDOVER ATTACH**

20 If the HSGW receives a PBA from the P-GW with a Status field value indicating failure to
21 complete the requested PDN attach, the HSGW shall send a VSNCP Configure-Reject to the
22 UE.
23

24 When the HSGW receives the PBA from the P-GW indicating successful IP address
25 allocation, it examines the contents to determine what IP address(es) have been allocated to
26 the UE and constructs a VSNCP Configure-Ack message.
27

28 If the “IPv4 Address Acknowledgment option” option is present in the PBA, the HSGW shall
29 check whether a Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific
30 PMIPv6 DHCPv4 Address Allocation Procedure Indication" has been received in the PBA.
31

- 32 ▪ If no such deferred allocation indication was received, the IPv4 address shall be
33 copied to the “PDN Address” option in the VSNCP Configure-Ack message.
34
- 35 ▪ If such deferred allocation indication has been received, the IPv4 address 0.0.0.0
36 shall be inserted in the "PDN Address" option. (NOTE: In this case, the UE has
37 requested deferred IPv4 address allocation and it may request an IPv4 address via
38 DHCPv4.)
39

40 If the “IPv6 Home Network Prefix” option is present, the IID shall be copied to the “PDN
41 Address” option in the VSNCP Configure-Ack message. The UE shall use the IPv6 home
42 network prefix that it receives in the RA message, refer to section 5.4.3.
43

44 The PDN Type in the “PDN Address” option shall be set to indicate which address(es) is
45 contained in the “PDN Address” option.
46

47 If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN
48 Type Indication" is present in the PBA, the PDN type value is copied to the “PDN Type”
49 option in the VSNCP Configure-Ack message and to the PDN type field in the “PDN
50 Address” option in the VSNCP Configure-Ack message.
51

52 If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN
53 Type Indication" is present in the PBA, the HSGW shall copy the cause field value to the
54 “Address Allocation Cause” option in the VSNCP Configure-Ack message.
55

If the Vendor-Specific Mobility Option of subtype "3GPP Vendor-Specific PMIPv6 PDN Type Indication" is not present in the PBA, 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 [23].
- 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").

5.4.2 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 6 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 PMIPv6 Binding Acknowledgment (PBA) 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; therefore, the HSGW shall include the allocated IP address in the VSNCP Configure-Ack message sent to the UE.

See Sections 10.3.1 and 6.4.1 for more details.

5.4.3 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.

1 When the HSGW receives VSNCP Configure-Request, the HSGW triggers PMIPv6
2 procedures to the requested P-GW as specified in Section 6 if the UE is authorized to connect
3 to it. The HSGW shall forward the Protocol Configuration Options (PCO) that are requested
4 by the UE to the P-GW.

5
6 The P-GW allocates an IPv6 prefix and the IPv6 interface identifier to the UE during PDN
7 connection establishment. The P-GW sends the allocated IPv6 prefix and the IPv6 interface
8 identifier in the PBA to the HSGW. Upon receiving the PBA, the HSGW shall send a VSNCP
9 Configure-Ack message to the UE with the IPv6 interface identifier to the UE. Subsequently,
10 the HSGW shall send Router Advertisement message to the UE including the assigned IPv6
11 prefix received in the PBA.

12
13 After the UE has received the Router Advertisement message, it shall construct its full IPv6
14 address via IPv6 Stateless Address Autoconfiguration in accordance with RFC 4862 [51]. For
15 privacy, RFC 3041 [38], the UE may change the interface identifier used to generate full IPv6
16 addresses, without involving the network. The UE may use stateless DHCPv6 for additional
17 parameter configuration.

18
19 The detail call flow for IPv6 prefix allocation after the PDN connection establishment
20 procedure is provided in 5.4.5.4 below.

21
22 Stateless Address Autoconfiguration for IPv6 global and link local addresses are supported by
23 the UE by default. stateful address configuration using DHCPv6 is not supported in this
24 specification per TS 23.402 [15].
25

26 27 **5.4.4 IPv4 Address Allocation in eHRPD Access using DHCPv4**

28
29 This section specifies the case in which the UE requests deferred IPv4 address allocation.

30
31 The UE that supports IPv4 shall indicate it by setting the PDN Type option to IPv4 or IPv4v6
32 in the VSNCP Configure-Request message. The UE shall indicate that it wants deferred IPv4
33 address allocation using Address Allocation Preference contained in the PCO. If the UE
34 indicates using the Address Allocation Preference that it wants deferred IPv4 address
35 allocation, and the P-GW chooses to allow deferred allocation, the P-GW includes the
36 deferred IPv4 address allocation indicator (i.e., 3GPP Vendor-Specific PMIPv6 DHCPv4
37 Address Allocation Procedure Indication option) in the Proxy Binding Acknowledgement
38 message. Upon reception of a Proxy Binding Acknowledgement message with a deferred
39 IPv4 address allocation indicator included, the HSGW shall set the IPv4 address to 0.0.0.0 in
40 the VSNCP Configure-Ack message, even if an IPv4 address is assigned by the P-GW.
41

42
43 The HSGW shall forward the IPv4 default router address received from the P-GW to the UE
44 in the VSNCP Configure-Ack message.

45
46 The UE that requested deferred IPv4 address allocation may send the DHCPDISCOVER
47 message to the HSGW. If the UE supports RFC4039 [49], the UE shall send the
48 DHCPDISCOVER message with Rapid Commit option.
49

50
51 If the HSGW receives a DHCPDISCOVER message, the HSGW shall act as a DHCPv4 relay
52 agent and forward the DHCPv4 message within the PMIPv6 tunnel to the P-GW.

53
54 When the HSGW receives a DHCPDISCOVER message, if the HSGW had previously
55 received a PBA with the deferred IPv4 address allocation indicator and no IPv4 Address
56 Acknowledgement option, the HSGW also triggers PMIP procedures as specified in Section 6
57 to obtain the IPv4 address allocated to the UE, as well as the IPv4 default router address.
58
59
60

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 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 DHCPACK message from the HSGW, the UE shall configure its IP address with the IP address in the 'yiaddr' field.

5.4.5 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.

5.4.5.1 IPv4 Address Allocation during PDN Connection Establishment

Figure 13 illustrates an example call flow for IPv4 address allocation during PDN connection establishment.

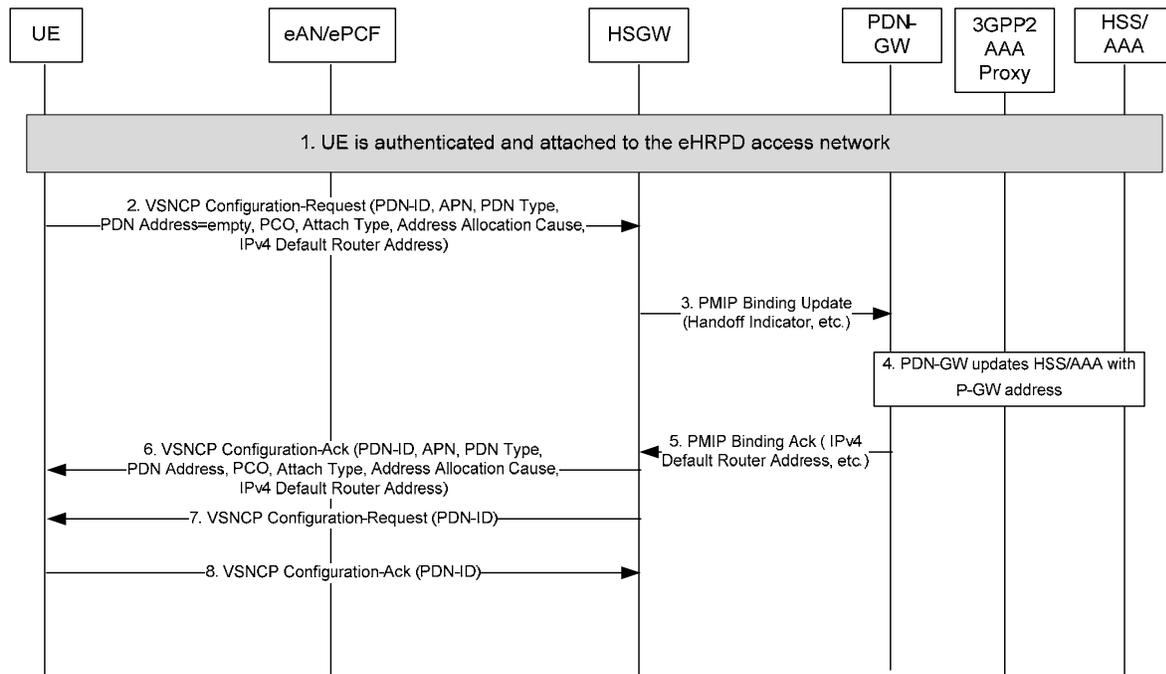


Figure 13 IPv4 address allocation during PDN connection establishment

1. The UE has performed successful authentication and is attached to the eHRPD access network.
2. The UE sends a VSNC Configuration-Request message over the main signaling 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.

- 1 3. Since the Attach Type is set to Initial Attach in this call flow, the HSGW selects a new P-GW
2 based on APN received from HSS/HAAA (for default PDN connection) or received from the
3 UE (for additional PDN connection). The HSGW sends a PMIPv6 Binding Update (PBU) to
4 the P-GW. See 3GPP 23.402 [15] and 29.275 [23].
5
- 6 4. The P-GW updates the 3GPP AAA Server/HSS with P-GW's identity (i.e., FQDN, or IP
7 address). See 3GPP 23.402 [15].
8
- 9 5. The P-GW responds with a PBA message to the HSGW. See 3GPP 23.402 [15] and 29.275
10 [23].
11
- 12 6. The HSGW sends a VSNCP Configure-Ack message (PDN-ID, APN, PDN Type, PDN
13 Address, IPv4 Default Router Address, PCO, and Attach Type) to the UE over the main
14 service connection. The PDN Address option contains an IPv4 address received in the PBA
15 (step 5).
16
- 17 7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in
18 RFC 3772 [47]. The information in the message includes the PDN-ID configuration option.
19 This message also includes the APN-AMBR if received from the HSS/AAA.
20
- 21 8. The UE responds with a VSNCP Configure-Ack message (PDN-ID). This message also
22 includes the APN-AMBR configuration option if received from the HSGW in the VSNCP
23 Configure-Request.
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

5.4.5.2 IPv4 Address Allocation with DHCPv4 Rapid Commit Option

Figure 14 illustrates an example call flow for IPv4 address allocation via using DHCPv4 Rapid Commit Option (see TS 23.402 [15]). 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.

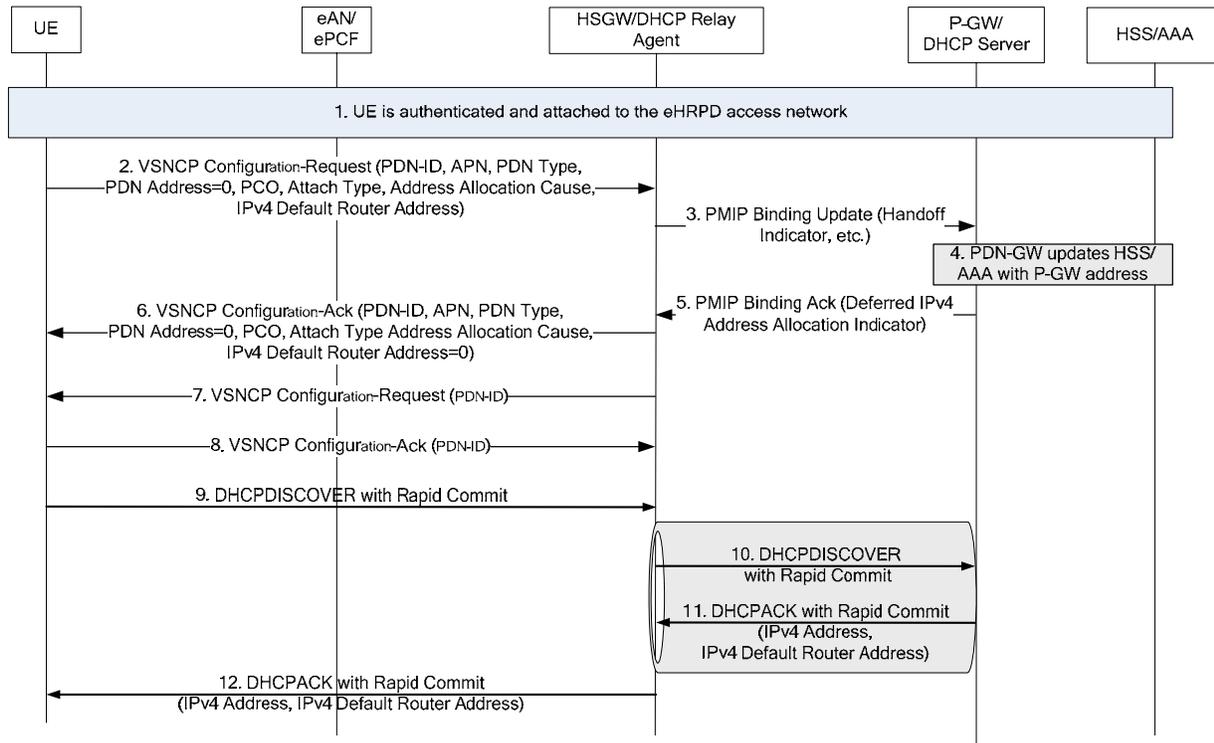


Figure 14 IPv4 Address Allocation using DHCPv4 with Rapid Commit Option

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 signaling 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) or received from the UE (for additional PDN connection). The HSGW sends a PBU to the P-GW. See 3GPP 23.402 and 29.275.
4. The P-GW updates the 3GPP AAA Server/HSS with PDN-GW’s identity (i.e., FQDN, or IP address). See 3GPP 23.402.

- 1 5. The P-GW responds with a PBA message to the HSGW. The P-GW in this scenario includes
2 3GPP Vendor-Specific PMIPv6 DHCPv4 Address Allocation Procedure Indication option in
3 the Proxy Binding Acknowledgement message indicating that the UE requested deferred IPv4
4 address allocation. The P-GW in this case assigns and returns an IPv4 address and an IPv4
5 default router address to the HSGW as described in section 5.4.1.1.3. See 3GPP 23.402 [15]
6 and 29.275 [23].
7
- 8 6. The HSGW sends a VSNCP Configure-Ack (PDN-ID, APN, PDN Type, PDN Address, IPv4
9 Default Router Address, PCO, and Attach Type) message to the UE over the main service
10 connection. Note that the PDN address in VSNCP Configure-Ack contains the 0.0.0.0
11 address since the HSGW received a deferred IPv4 address allocation indicator in the Proxy
12 Binding Acknowledgement message in step 5. In the case that the UE had indicated IPv4v6
13 capabilities in step 2, but the HSGW indicated only IPv4 in the PBU in step 3, then the
14 HSGW sets the Address Allocation Cause option to “New PDN type due to subscription
15 limitation”.
16
- 17 7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in
18 RFC 3772 [47]. The information in the message includes the PDN-ID configuration option.
19 This message also includes the APN-AMBR configuration option if received from the
20 HSS/AAA.
21
- 22 8. The UE responds with a VSNCP Configure-Ack message. The information in the message
23 includes the PDN-ID configuration option. This message also includes the APN-AMBR
24 configuration option if received from the HSGW in the VSNCP Configure-Request.
25
- 26 9. The UE sends a DHCPDISCOVER message with the Rapid Commit option in broadcast to
27 the network to find available servers.
28
- 29 10. Upon receiving the DHCPDISCOVER with Rapid Commit message, the HSGW acting as a
30 DHCPv4 Relay Agent shall add its address in the GIADDR option and add the assigned UE
31 IP address (received from P-GW in the PBA message) in the "Address Request" option, and
32 relay the message in unicast within the PMIPv6 tunnel to the P-GW. The P-GW acts as a
33 DHCPv4 server.
34
- 35 11. When receiving the DHCPDISCOVER message, the P-GW should verify the GIADDR
36 option. Then the P-GW uses "Address Request" option to identify the UE binding and update
37 it with the 'client identifier' and 'chaddr' combination for subsequent DHCPv4 procedure.
38
39 The P-GW extends the IP lease offer and sends a DHCPACK message with the Rapid
40 Commit option to the HSGW. This message is sent through the PMIPv6 tunnel established
41 between the HSGW/MAG and the P-GW/LMA.
42
43
44
45
46
47 12. The HSGW forwards the DHCPACK with the Rapid Commit option to the UE.
48
49
50
51
52
53
54
55
56
57
58
59
60

5.4.5.3 IPv4 Address Allocation without DHCPv4 Rapid Commit Option

Figure 15 illustrates an example call flow for IPv4 address allocation by using DHCPv4 without the DHCPv4 rapid commit option (see TS 23.402 [15]). 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.

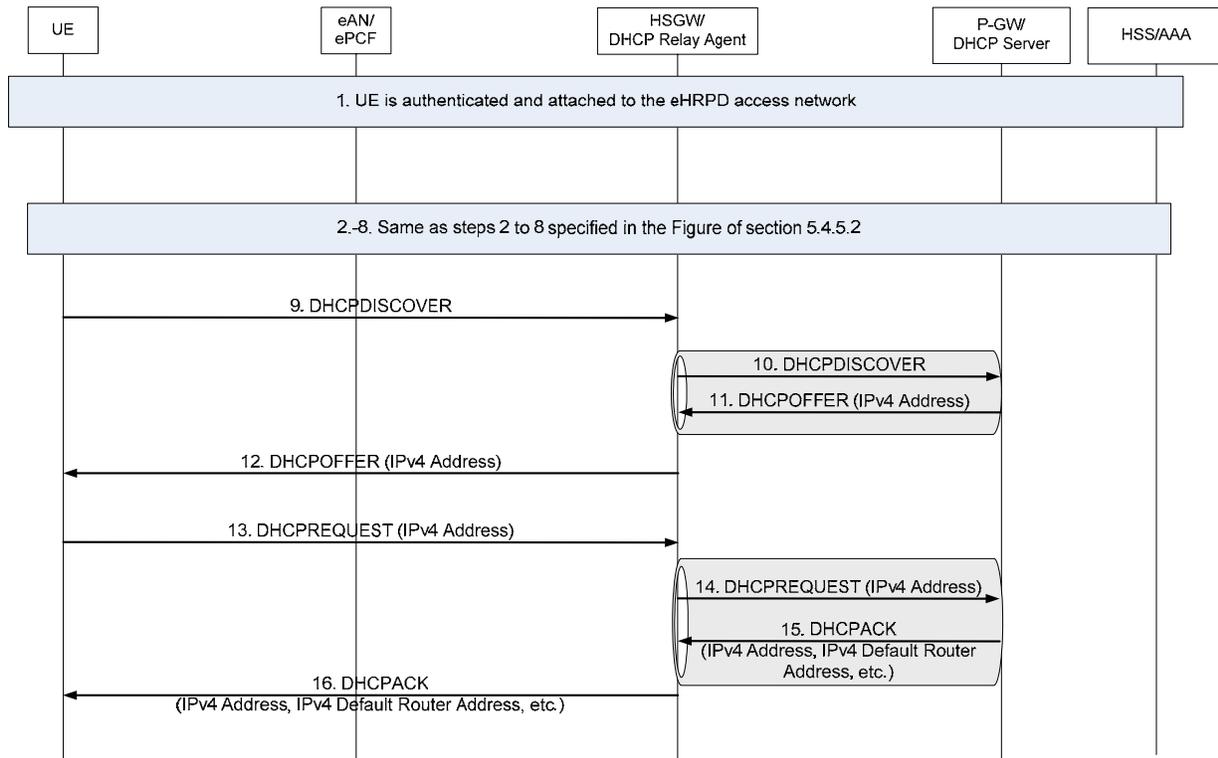


Figure 15 IPv4 Address Allocation using DHCPv4 without Rapid Commit Option

1. The UE has performed successful authentication and is attached to the eHRPD access network.
- 2-8. Steps 2 to 8 are same as steps 2 to 8 specified in section 5.4.5.2.
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.

1 After that the P-GW extends an IP lease offer and sending the DHCP OFFER with the
2 assigned UE IP address.

- 3
- 4 12. The HSGW acting as DHCPv4 Relay Agent relays the DHCPv4 message to the UE.
- 5
- 6
- 7 13. When the UE receives the lease offer, it sends a DHCPREQUEST message containing the
8 received IP address.
- 9
- 10 14. The HSGW acting as DHCPv4 Relay Agent relays the DHCPv4 message to the P-GW.
- 11
- 12
- 13 15. When the P-GW receives the DHCPREQUEST message from the UE, it sends a DHCPACK
14 message to the UE. This message includes the lease duration and any other configuration
15 information that the client might have requested.
- 16
- 17 16. The HSGW acting as DHCPv4 relay agent relays the DHCPv4 message to the UE.
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

5.4.5.4 IPv6 Address Allocation

Figure 16 below shows an example call flow for IPv6 address allocation.

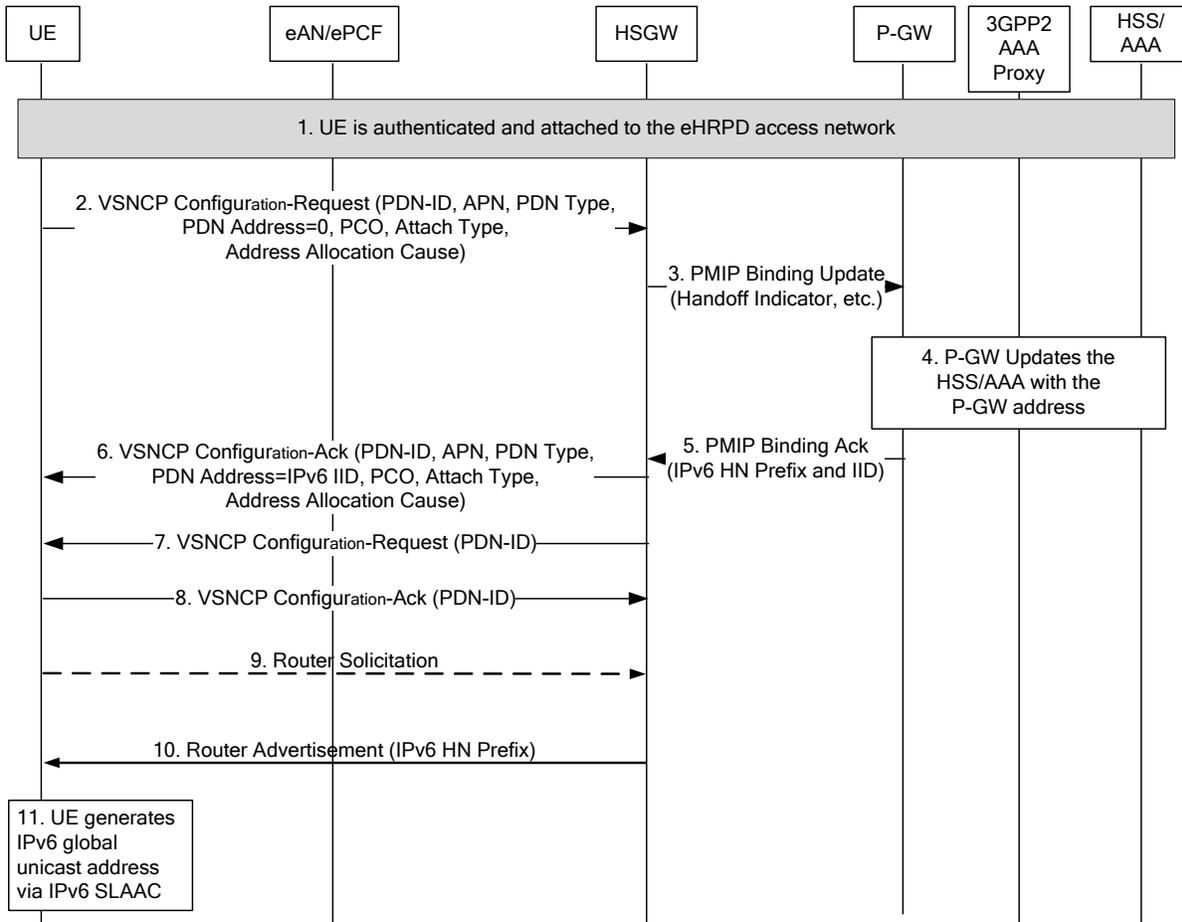


Figure 16 IPv6 Address Allocation

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 signaling 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 default PDN connection) or received from the UE (for additional PDN connection). The HSGW sends a PBU to the P-GW. See 3GPP 23.402 and 29.275.
4. The P-GW updates the 3GPP AAA Server/HSS with PDN-GW’s identity (i.e., FQDN, or IP address). See 3GPP 23.402.
5. The P-GW responds with a PBA to the HRPD Serving GW. See 3GPP 23.402 and 29.275.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- 1 6. The HSGW sends a VSNCP Configure-Ack message (PDN-ID, APN, PDN Type, PDN
2 Address, PCO, and Attach Type) to the UE over the main service connection. The PDN
3 Address Information contains the IPv6 interface ID in this example.
- 4 7. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in
5 RFC 3772 [47]. The message includes the PDN-ID configuration option. This message also
6 includes the APN-AMBR if received from the HSS/AAA.
- 7 8. The UE responds with a VSNCP Configure-Ack message that contains the PDN-ID
8 configuration option.
- 9 9. This step is optional. The UE may send a Router Solicitation (RS) message to the HSGW via
10 the eAN.
- 11 10. Upon receiving the Route Solicitation message or any time after step 8, the HSGW sends an
12 IPv6 Router Advertisement message (see RFC 4862 [51]) to the UE which includes the UE's
13 home network prefix.
- 14 11. The UE generates an IPv6 global unicast address via IPv6 stateless address auto-configuration
15 (see RFC 4862 [51]). The UE may use the interface ID received from step 6 to configure its
16 link local IPv6 address.
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

5.5 Quality of Service

The HSGW performs a number of Quality of Service related functions that are defined for the PDSN in X.S0011-D v1.0 [5]. 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-D v1.0 [5] 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 [13] and TS 23.402 [15]. For E-UTRAN/eHRPD interworking scenarios, that same paradigm is followed; hence, these functions are not performed in the HSGW.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

5.5.1 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 3GPP TS 23.401 [14]).

Figure 17 shows an example bearer mapping in eHRPD.

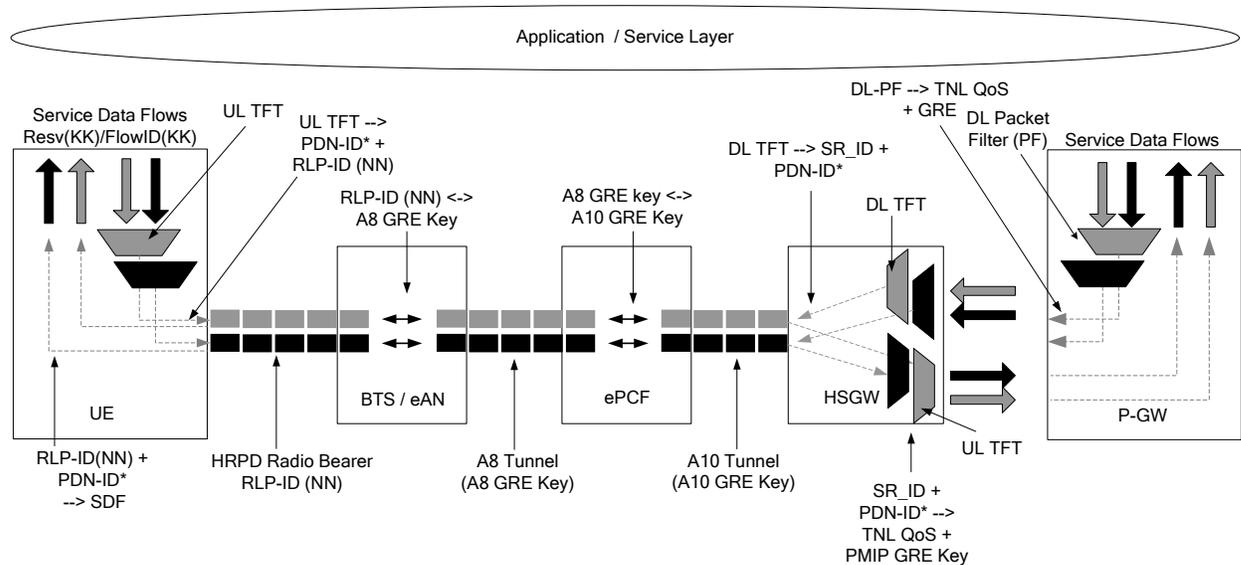


Figure 17 Sample Bearer Mapping in eHRPD

* 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 shall be 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 10.1.5 for the stage 3 details on the use of the BE auxiliary 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 10.1.5 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:

- UL TFTs in the UE bind one or more IP flows (SDFs) to an EPS bearer in the uplink direction.
- DL 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 one-to-one 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. QoS control between a HSGW and a P-GW is provided at the Transport Network Layer (TNL). 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 UL 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.

5.5.2 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.

5.5.3 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 [14] and TS23.402 [15] 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 10.1.2

5.5.3.1 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 [15] 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 18 by sending an RSVP Resv message to the UE.

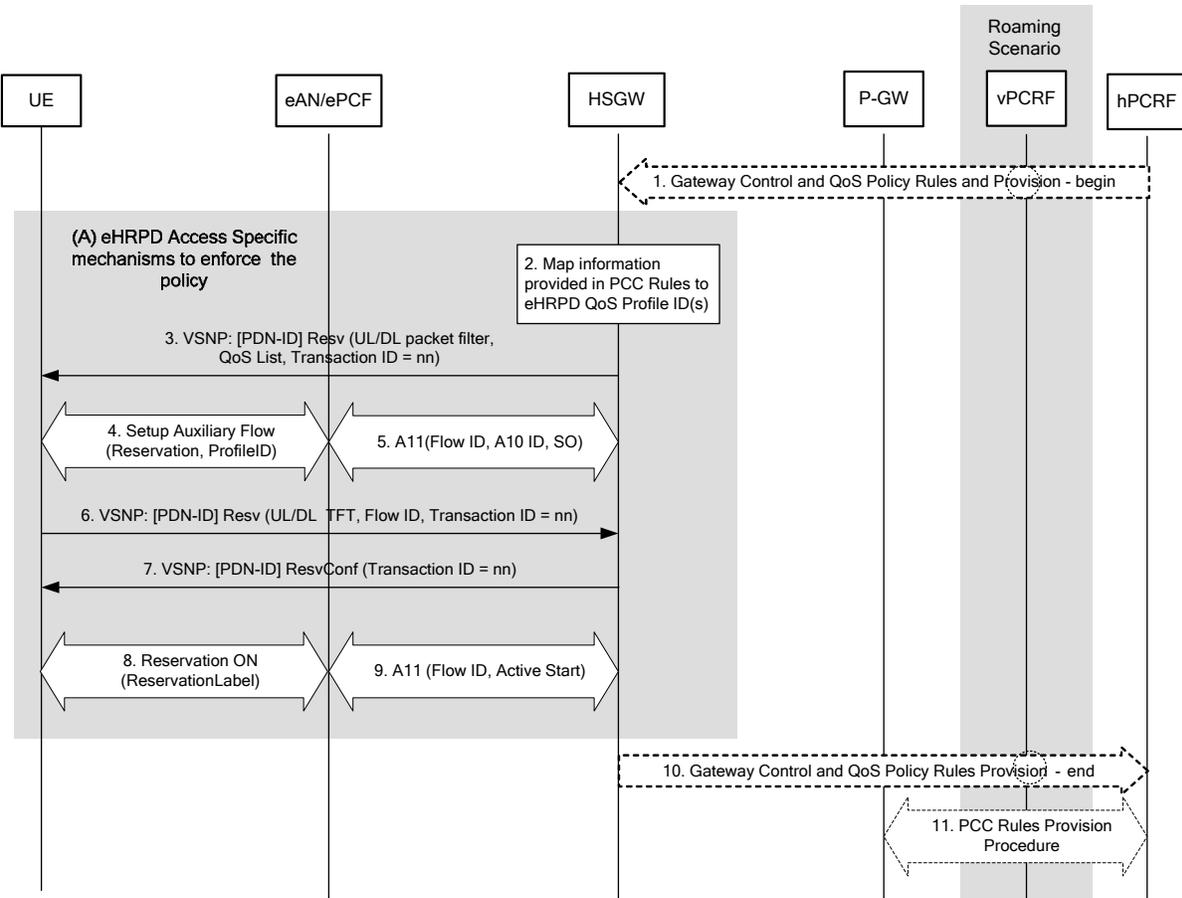


Figure 18 Network Initiated Dedicated Bearer Setup

Both the roaming and non-roaming scenarios are depicted in Figure 18. 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 [13] 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 [7]).
3. The HSGW sends an RSVP Resv message transported over the main service connection. As indicated in section 10, 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 UL/DL packet filter, the QoS list, and a Transaction ID. See section 10.1.6.7.1 for parameter details, and see Annex C for details on parameter mapping.
4. The UE performs the standard QoS establishment procedures defined in C.S0024-B [6] and in C.S0063-A [8]. 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.

- 1 5. If a new link flow is needed, a new A10 connection is also established. The eAN/ePCF sends
2 an A11-Registration Request message to the HSGW indicating the GRE key, the Requested
3 QoS information, and the Granted QoS information for the flow. The Granted QoS
4 information includes the FLOW_ID. If a new QoS link flow is not needed, the eAN sends an
5 A11-Registration Request message to the HSGW indicating the GRE key, FLOW_ID, and the
6 modified Granted QoS information for the existing connection (if required). The HSGW
7 examines the QoS granted to the UE and compare it to the QoS authorized for the UE in step
8 2. If there is a discrepancy, the HSGW applies operator policy and may, for example, remove
9 the flow or shut off all connectivity for the UE.
- 10 6. The UE sends an RSVP Resv message to the HSGW. The message includes the Flow ID for
11 the bearer connection, and the same DL/UL TFT and Transaction ID received in step 3. This
12 message can be sent in parallel with the start of the signaling in Step 4. The Transaction ID is
13 used to associate the returned Flow ID with the new bearer connection. This message is also
14 used as an acknowledgement to the RSVP Resv message in Step 3.
- 15 7. The HSGW acknowledges the delivery of the RSVP Resv message it received in Step 6 by
16 sending a ResvConf message to the UE.
- 17 8. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or
18 eAN) may trigger the transition to the open state.
- 19 9. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an
20 A11-Registration Request (Active Start) message to initiate the accounting for this bearer
21 connection.
- 22 10. Any time after Step 6 the HSGW responds to the PCRF indicating its ability to enforce the
23 rules provisioned to it in Step 1 and thus completing the GW Control and QoS Rules
24 Provision Ack procedure started in step 1
- 25 11. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [13]. The
26 PCRF provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules
27 Provision procedure specified in TS 23.203.

28 NOTE: Step 11 may occur before step 2 or may be performed in parallel with steps 1 and 10 if
29 acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details
30 please refer to TS 23.203 [13].

31 **5.5.3.2 Dedicated Bearer Deactivation**

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

37 **5.5.3.2.1 PCRF Initiated Dedicated Bearer Deactivation**

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

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

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

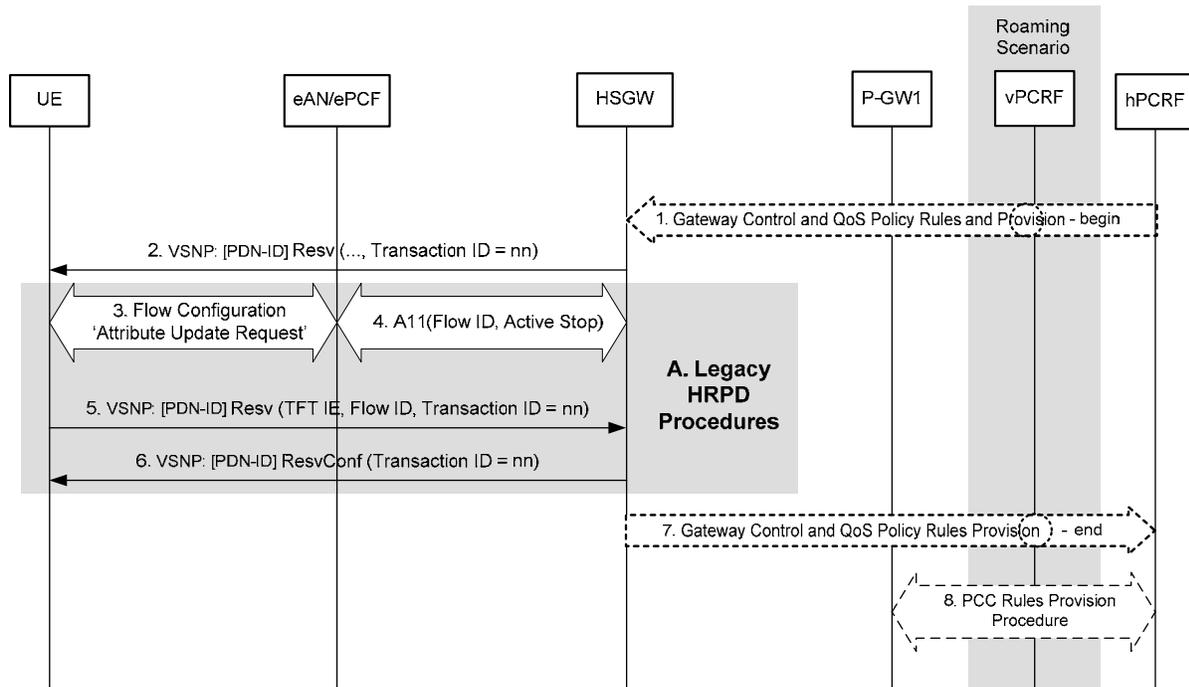


Figure 19 Dedicated Bearer Deactivation

1. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [13] 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-RRQ message to the HSGW indicating the removed Flow ID(s). If the last Flow ID(s) associated with the auxiliary A10 are removed, the auxiliary A10 itself will also be 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.

- 1 8. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203. The PCRF
2 provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules Provision
3 procedure specified in TS 23.203 [13].

4 NOTE: Step 8 may occur before step 1 or performed in parallel with steps 1 and 7 if
5 acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details
6 please refer to TS 23.203 [13].
7

8 **5.5.4 UE Initiated Dedicated Bearer Procedures for eHRPD**

9 **5.5.4.1 UE Initiated Resource Request, Modification and Release**

10 The UE requested bearer resource allocation and release model for eHRPD shall follow
11 TS23.203 [13] and TS23.402 [15]. In the PCC model the UE request resources which are in
12 turn granted and established by the network or modified and deleted depending on the nature
13 of the UE request.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

5.5.4.1.1 UE Requested Bearer Resource Allocation

The call flow in Figure 20 illustrates UE requested bearer activation procedures.

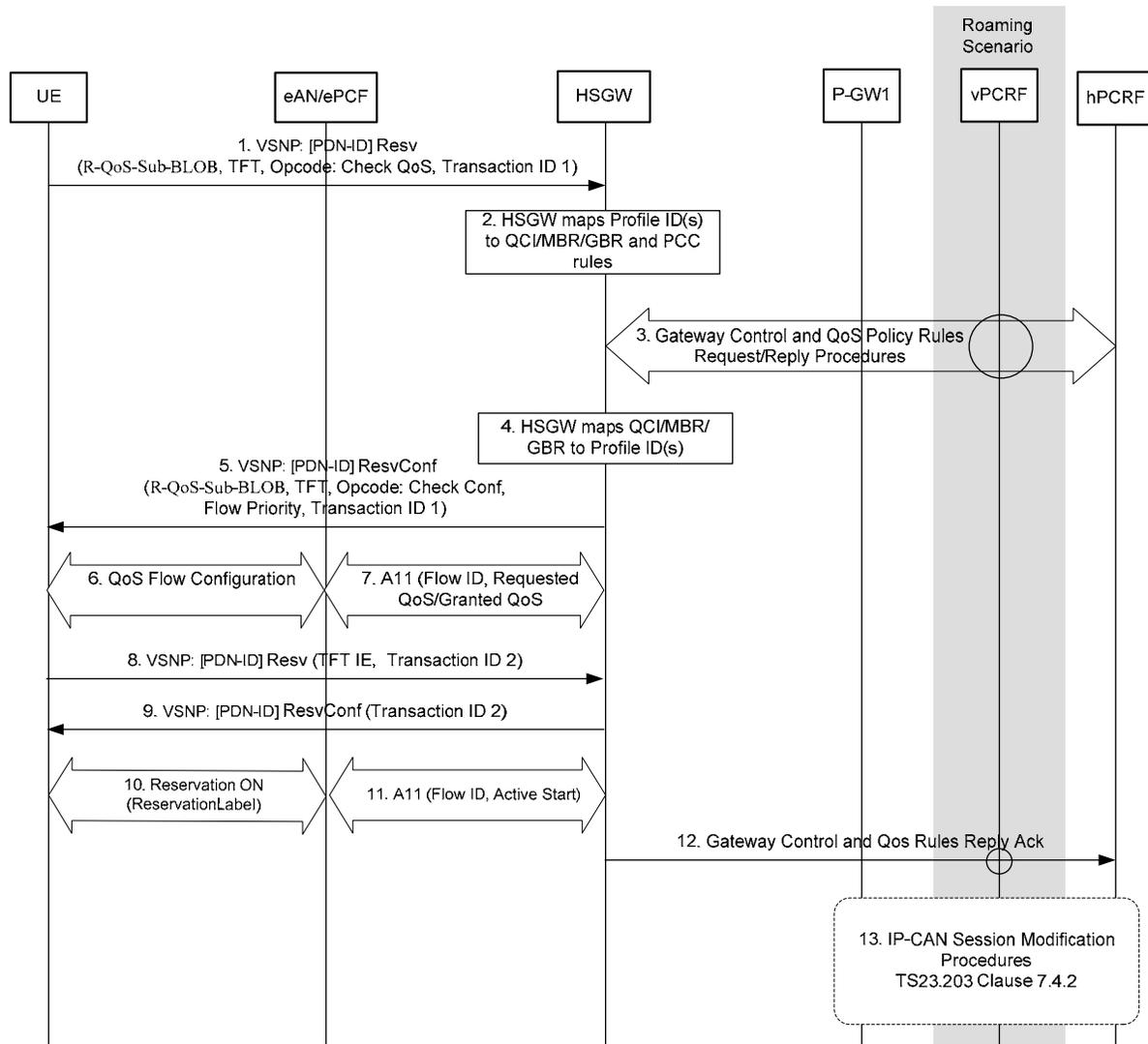


Figure 20 UE Requested bearer resource allocation

1. The UE sends a Resv message to the HSGW with OpCode set to 'Check QoS'. 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 R-QoS-Sub-BLOB. 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 shall use Gateway Control and QoS Rules procedures to validate UE requested QoS with the hPCRF. If the HSGW is deployed in a roaming scenario, the message including

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1 QCI/MBR/GBR(s) and packet filter(s) is sent to the vPCRF and the vPCRF forwards it to the
2 hPCRF.

- 3 4. The HSGW maps the validated policy rules into appropriate FlowProfileID(s) that are being
4 requested.
- 5
6 5. The HSGW sends a ResvConf message to the UE with OpCode set to 'QoS Check'. The Resv
7 message is an RSVP message transported over the main service connection. The ResvConf
8 message contains the UL/DL TFT, the authorized QoS R-QoS-Sub-BLOB, which is same or a
9 subset of the UE requested R-QoS-Sub-BLOB in step 1, and the same Transaction ID as in
10 the Resv message sent in step 1. This step is used as an acknowledgment of the Resv message
11 sent in step 1.
- 12
13 6. The UE performs the standard HRPD QoS establishment procedures defined in C.S0087 [10]
14 / C.S0063 [8] using the authorized FlowProfileID list from step 5. There are two possible
15 sequences that can occur at this step. If a new QoS link flow connection is needed to carry the
16 new flow over the air interface, then the eAN will setup a new air interface link flow. If the
17 eAN decides to carry the flow(s) on an existing link flow, it then reconfigures the parameters
18 of that link flow.
- 19
20 7. If a new link flow is needed, a new A10 connection is also established. The eAN sends an
21 A11-Registration Request message to the HSGW indicating the GRE key, the Requested QoS
22 information, and Granted QoS information for the flow. The A11 message includes the
23 FLOW_ID. If a new QoS link flow is not needed, the eAN sends an A11-Registration Request
24 message to the HSGW indicating the GRE key, FLOW_ID, and the modified Granted QoS
25 information for the existing connection (if required). The HSGW examines the QoS granted
26 to the UE and compare it to the QoS authorized for the UE in step 2. If there is a discrepancy,
27 the HSGW applies operator policy and may, for example, remove the flow or shut off all
28 connectivity for the UE.
- 29
30 8. The UE sends a Resv message to the HSGW to associate the selected Reservation with the
31 appropriate A10 connection and TFT. The message includes the Flow ID for the bearer
32 connection, and the same DL/UL TFT received in step 5. This message can be sent in
33 parallel with the start of the signalling in Step 6. The Transaction ID is different than that
34 used in steps 1 and 5 to avoid having the HSGW view this message as a repetition of the
35 message in step 1.
- 36
37 9. The HSGW acknowledges the Resv message with a ResvConf message.
- 38
39 10. Since by default the Reservation for the newly created bearer is in the Closed state, the UE (or
40 eAN) may trigger the transition to the open state.
- 41
42 11. Once the air interface reservation is transitioned to the Open state, the eAN will trigger an
43 A11-Registration Request (Active Start) message to initiate the accounting for this bearer
44 connection.
- 45
46 12. If steps 7 and 8 result in successful negotiation of QoS, the HSGW sends the
47 acknowledgement to the PCRF based on the QoS that was selected in step 2.
- 48
49 13. The IP CAN Session Modification Procedure may occur as the result of the Gateway Control
50 and QoS Rules Request message, either to forward an Event Report to the P-GW (PCEF) or to
51 issue revised PCC Rules and Event Triggers, or both an Event Report and a Rules and
52 Triggers provision. If an indication that resources have been acquired is not required then this
53 step may occur any time after step 3, above.
- 54
55
56
57
58
59
60

5.5.4.1.1.1 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 Policy Rules Provision - begin’ 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 Policy Rules Provision - begin’ from the PCRF for a packet filter and if the HSGW had already sent a ‘Gateway Control and QoS Policy Rules Request’ for the same packet filter, then the HSGW shall omit steps 2 – 6 in Figure 19 and shall acknowledge the request from the PCRF by sending a ‘Gateway Control and QoS Policy Rules Provision – end’ message.

The PCRF completes the UE requested packet filter clean up procedure by sending the ‘Gateway Control and QoS Policy 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 Policy Rules that are mapped to the packet filter and shall set the QoS rules to inactive state. If the QoS Policy 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.

5.5.4.1.2 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 21 below.

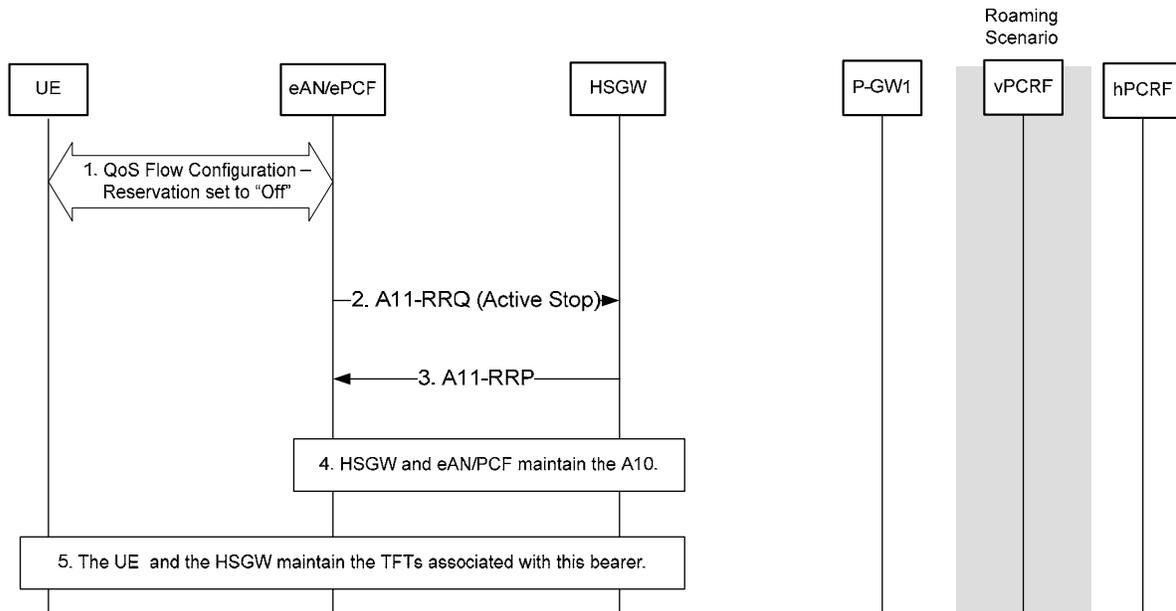


Figure 21 UE Requested Radio Bearer State Modification

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-RRQ 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.

5.6 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 22).

Per TS 23.401 [xx] and TS 23.402 [xx], 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.

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 22).

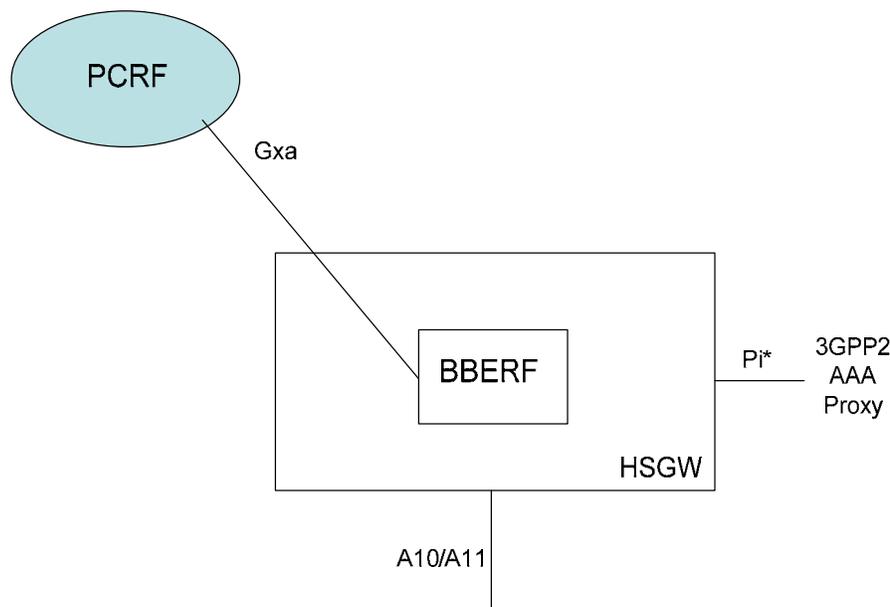


Figure 22 HSGW Policy Enforcement

5.6.1 Application of 3GPP PCC to the HSGW

The BBERF in the HSGW performs bearer binding and event reporting as defined in 3GPP TS 23.203 [13] and follows the framework defined in 3GPP TS 23.402 [15] 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 [13].

5.6.2 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 [15]:

1. Gxa shall be based on an evolution of the Gx application specified in 3GPP TS 29.212 [20].
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 3GPP TS 23.401 [14] and 3GPP TS 23.402 [15]. 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.

5.6.3 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 [14]. The charging functions in the HSGW, with associated interfaces shall be supported as specified in TS 32.240 [25]. 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 [25] and TS 32.251 [26].

The P-GW shall be able to provide charging functionality for each UE according to TS 23.203 [13].

5.6.4 Policy interworking during handovers

In the scenario where a handover from E-UTRAN to eHRPD is performed some policy interaction may be needed between the HSGW and the EPC PCRF (see TS 23.402 [15]).

5.6.5 Priority and Conflict Resolution

Priority and conflict resolution follows the principles described in 3GPP TS 23.203 [13].

5.6.6 Mapping of QoS parameters between 3GPP and 3GPP2

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 3GPP TS 23.401 [14].

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 to be the same as the GBR. No QoS mapping recommendations are provided for FlowProfileIDs reserved for proprietary of future use.

This QoS mapping capability provides the policy interworking used during session establishment and E-UTRAN to eHRPD handovers.

5.6.7 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 5.5.3, 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 5.5.4.1, 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.

5.7 S103 Interface: S-GW – HSGW

The S103 (User Plane interface) between the Serving GW (S-GW) and HSGW supports the forwarding of DL 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 [15].

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 [36] including the Key Field extension RFC 2890 [37]. The Key field value of each GRE

packet header uniquely identifies the PDN connectivity that the GRE packet payload is associated with.

5.7.1 S103 Protocol Stack

The protocol stack for S103 is:

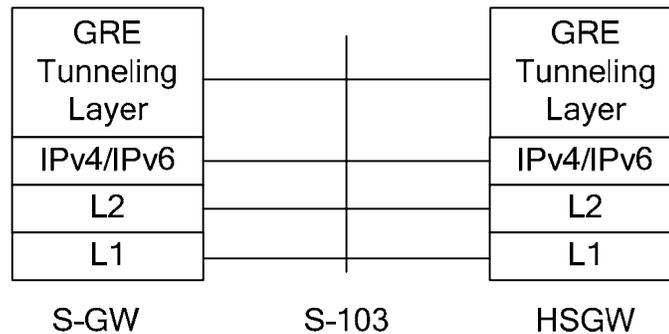


Figure 23 S103 Protocol Stack

5.7.2 S103 Procedures

The S103 interface is established to provide indirect data forwarding from the S-GW to the HSGW during handover from E-UTRAN to eHRPD. For stage 3 details, see TS 29.276 [24].

During the handover execution phase for handover 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) to forwarding the packets per PDN to the HSGW. This information is passed to the eAN/ePCF across the A11 interface; see section 9. 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) to forward user IP packets to the HSGW.

5.8 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 occurs), the UE shall perform LCP negotiation and EAP-AKA' authentication as specified in section 5.2. 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.

6 S2a Interface from the HSGW to the P-GW

6.1 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 [15].

6.2 HSGW Requirements

The HSGW shall act as the Mobile Access Gateway (MAG) as specified in RFC 5213 [52] and in draft-ietf-netlmm-pmip6-ipv4-support [55].

6.2.1 PMIPv6 Triggers

HSGW shall trigger PMIPv6 procedures as specified in this section.

6.2.1.1 PMIPv6 Registration Triggers

The HSGW shall trigger PMIPv6 registration procedures only when the UE is operating using the eHRPD radio. Additional conditions are listed below.

- When the HSGW receives a VSNCP Configuration-Request from the UE that requests PDN connection establishment and the attach type is initial attach, the HSGW shall perform P-GW selection as per TS 23.402 [12] and it shall trigger PMIPv6 registration for the corresponding PDN.
- When the HSGW receives a VSNCP Configuration-Request from the UE that requests PDN connection establishment and the attach type is handover attach, the HSGW shall select the P-GW for the PDN connection indicated by the current HSS data and it shall trigger PMIPv6 registration for the corresponding PDN.
- When the HSGW receives A11-Registration Request message with the tunnel mode indicator set to 0 or with Active Start airlink record and no tunnel mode indicator included, and if the UE previously setup one or more PDN contexts in the HSGW via the S101 tunnel while operating using the LTE radio, the HSGW shall trigger PMIPv6 registration for each PDN context setup by the UE and indicated by the current HSS data as being a current PDN connection.
- 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 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 5.4.4.
- When the HSGW receives a Hack message with context information TLVs as defined in Section 12.3.2, the HSGW shall trigger PMIPv6 registration for each PDN connection that was connected to the source HSGW.
- The HSGW shall trigger PMIPv6 re-registration for PDN connection(s) as needed to prolong the lifetime of existing PMIPv6 session(s).

6.2.1.2 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 AAA/HSS or PCRF requesting termination of a PDN connection, the HSGW shall perform PMIPv6 de-registration for the corresponding PDN.
- 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.

6.2.2 PMIPv6 Registration Process

The PMIPv6 registration process over S2a is described in TS 23.402 [15] and specified in TS 29.275 [23].

6.2.3. 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, 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 12).

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 10.1.7.

Note: Active eHRPD to E-UTRAN handoff is not supported in this version of this specification, and thus the procedure in the paragraph above is not applicable in this version to active eHRPD to E-UTRAN handoff.

6.3 P-GW Requirements

P-GW requirements are defined in TS 23.402 [15].

The P-GW supports the procedures of TS 29.275 [23].

6.4 Call Flows

6.4.1 S2a Connection Establishment with the Default PDN

PMIPv6 (see RFC 5213 [52] and TS 29.275 [23]) signaling is used to establish an S2a connection between the HSGW and the P-GW. The sample call flow below illustrates the establishment of the PMIPv6 based S2a connection when the UE attaches to the eHRPD access network for the first time.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

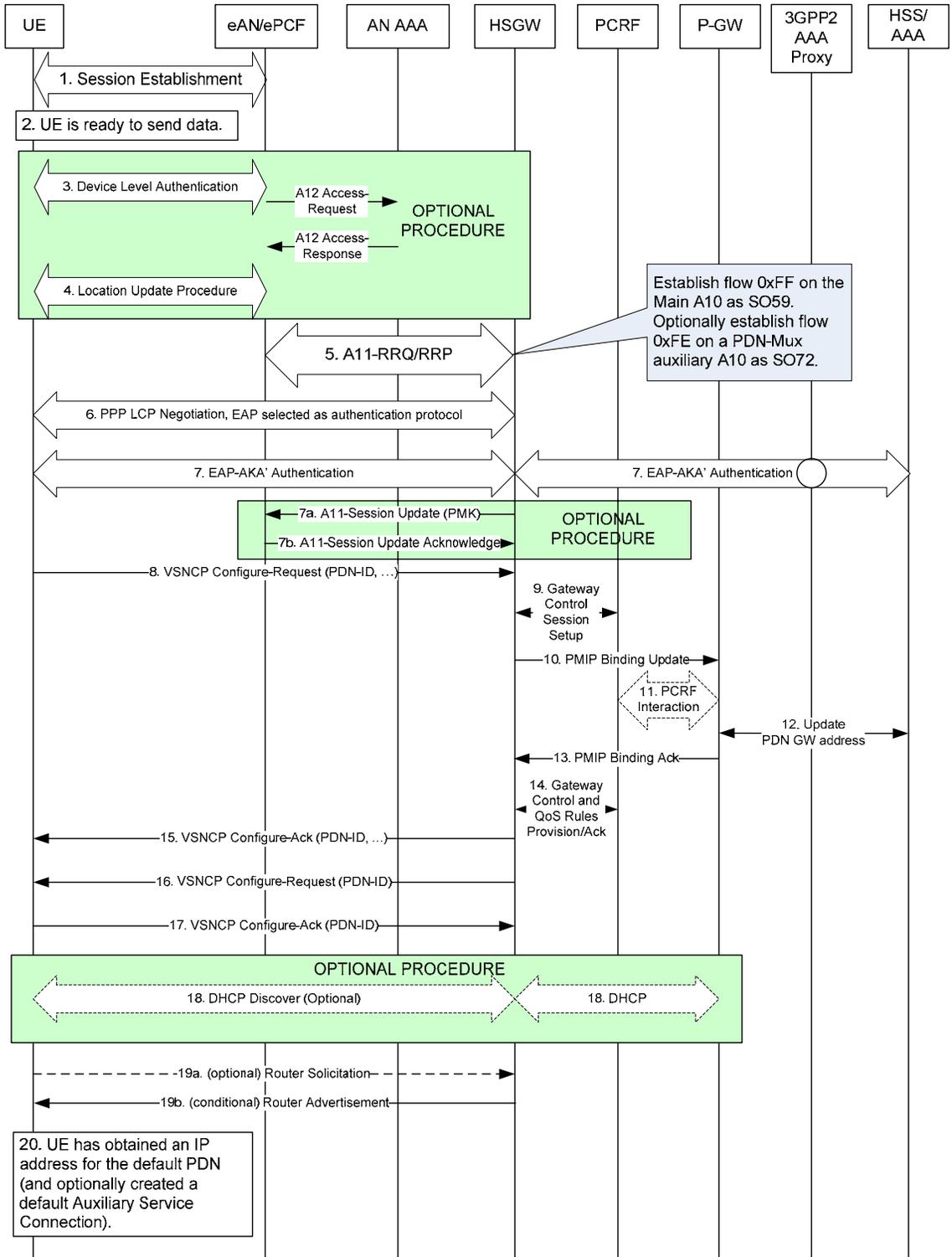


Figure 24 S2a Connection Establishment with the Default PDN

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. 1
4. (Optional) The UE may perform the eHRPD Location Update procedure. 2
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 service connection, and optionally set up the Best Effort (BE) auxiliary service connection. The A11-Registration Request is validated and the HSGW accepts the connection by returning an A11-Registration Reply message. 3
4
5
6
7
8
6. The UE and HSGW perform LCP negotiation and select EAP-AKA' as the authentication protocol. 9
10
11
7. The authentication procedures are initiated and performed involving the UE, the HSGW, the 3GPP2 AAA 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. 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. 12
13
14
15
16
17
18
19
20
21
 - 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-RRQ in step 5. 22
23
24
 - 7b. The eAN/ePCF responds with an A11-Session Update Acknowledge message. 25
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". The Address Allocation Preference option contained in the Protocol Configuration Options indicates whether the UE wants to perform the IP address allocation during the attach procedure or deferred IPv4 address allocation. PDN Type indicates the UE's IP capability (IPv4, IPv6 or IPv4/v6). Additional configuration options (e.g., IPv4 Default Router Address) are included depending upon the PDN Type. 26
27
28
29
30
31
32
33
34
9. The HSGW may perform Gateway Control Session Establishment procedure with the PCRF. 35
36
10. The HSGW sends a Proxy Binding Update to the P-GW in order to establish the new registration see TS 29.275 [23]. If the VSNCP message in step 8 contained an indication that the default APN is to be used, the HSGW uses the default APN to choose the P-GW. If the VSNCP message in step 8 contained an APN that is authorized to the user, the HSGW uses that APN to choose the P-GW. 37
38
39
40
41
42
11. The P-GW performs a PCRF interaction to retrieve the QoS policy parameters. 43
12. The P-GW sends an update message to the 3GPP AAA Server to update the UE profile with its address. The 3GPP AAA server acknowledges the updated P-GW address. 44
45
46
13. The P-GW responds with a Proxy Binding Acknowledgement PBA to the HSGW see TS 29.275 [23]. 47
48
49
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 3GPP TS 23.203 [13]. 50
51
52
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. 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-Rrequest. 53
54
55
56
57
58
59
60

- 1 16. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in
2 RFC 3772 [47]. The message includes the PDN-ID configuration option. This message
3 contains the APN-AMBR if received from the HSS/AAA.
- 4 17. The UE responds with a VSNCP Configure-Ack message.
- 5 18. (optional) The UE can now issue a DHCPv4 DISCOVER (optionally w/ rapid commit option)
6 message on the BE service connection provided the UE requested deferred IP address
7 allocation in Step 8.
- 8 19. 19a. The UE may send a Router solicitation message.
9 19b. The HSGW shall send a Router Advertisement message if the P-GW sends the IPv6
10 prefix to the HSGW.
- 11 20. The IP address allocation details are described in section 5.2.

12 Based on information stored at the UE or obtained from the network, the UE can start creating the
13 required auxiliary connections (needed for the bearer transport) for a particular QoS flow per
14 PDN. See section 10.3.

15 **6.4.2 S2a Connection Release**

16 See section 10.4 for call flows addressing PDN connection release.

17 **6.4.3 S2a Connection Establishment During Pre-Registration**

18 See section 13.1 for call flows addressing PDN connection establishment during pre-
19 registration.

20 **6.4.4 S2a Additional PDN Connection Establishment**

21 See section 10.3.1 for call flows addressing additional PDN connection establishment.

22 **6.4.5 S2a Connection Movement at Handover**

23 See sections 12.1, 12.2, and 13.1.2 for call flows addressing PDN connection movement at
24 handover.

25 **6.4.6 S2a Connection Release at De-Registration**

26 See section 11 for call flows addressing PDN connection release at de-registration.

7 STa Interface from the HSGW to the AAA

The HSGW interfaces to the 3GPP2 AAA Proxy using the Pi* interface. In this version of this specification, the Pi* interface is identical to the STa interface (TS 23.402 [15] and TS 29.273 [22]), since there are no 3GPP2 specific AVPs processed by the 3GPP2 AAA.

The Diameter protocol specified in RFC 3588 [43] is used on the Pi* interface.

The set of Diameter AVPs used on the STa interface are found in TS 29.273 [22].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

8 Gxa Interface from the HSGW to the PCRF

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

8.1 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 3GPP TS 23.402 [15].

The Gxa interface is based on an evolution of the Gx application specified in 3GPP 29.212 [20].

8.2 Stage 2 Flows

The protocol supported on the Gxa interface shall be Diameter. The Stage 2 procedures are specified in 3GPP TS 23.203 [13]. The HSGW shall implement the following procedures from TS 23.203 [13]:

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

See TS 23.203 [13] for the details of these procedures.

8.2.1 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 [15].

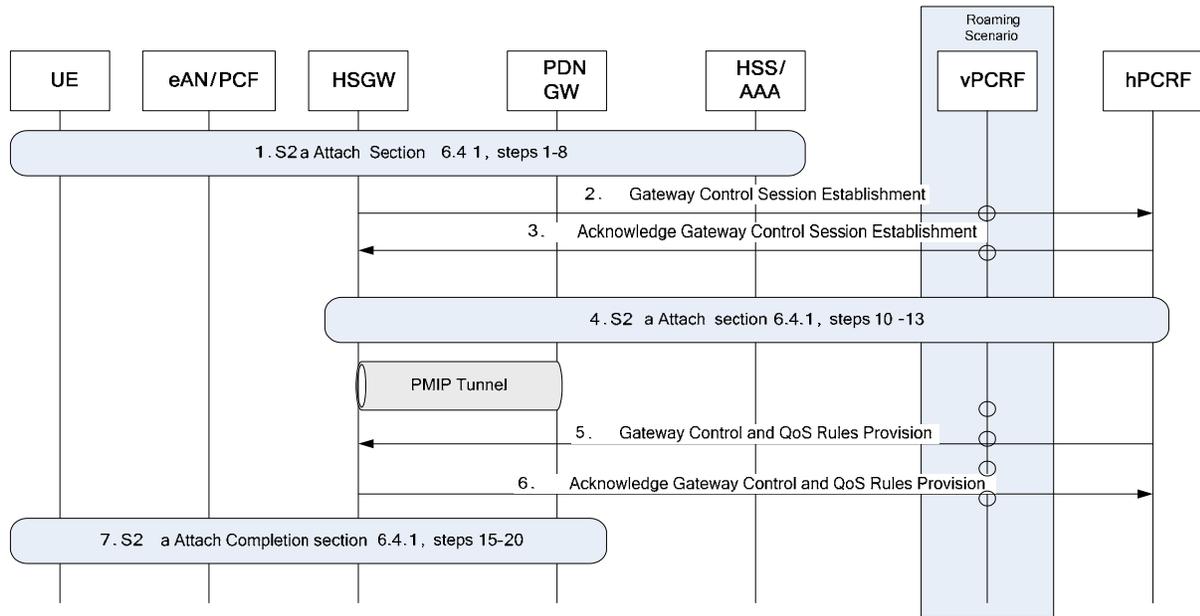


Figure 25 Initial attachment over S2a

The operational interaction steps between the gateways and the PCRF in the procedure in Figure 1 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 6.4.1, steps 1-8 is executed.
2. The HSGW initiates the Gateway Control Session Establishment Procedure with the hPCRF, as specified in TS 23.203 [13] 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. See 3GPP TS 23.203 [13] 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 and Event Triggers. 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 3GPP TS 23.203 [13] for more details.
4. The S2a attach procedure per section 6.4.1, 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 3GPP TS 23.203 [13] 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.

1 7. The S2a attach procedure per section 6.4.1, steps 15-20 is executed.

2 This procedure applies to the non-roaming, roaming, and local breakout cases. For the roaming
3 and local breakout cases, the vPCRF forwards messages between the HSGW and the hPCRF.
4

5 6 **8.3 Stage 3** 7

8 The Gxa reference point is located between the Policy and Charging Rules Function (PCRF)
9 and the HSGW Bearer Binding and Event Reporting Function (BBERF). The Gxa reference
10 point is used for:
11

- 12 - Provisioning, update and removal of QoS rules from the PCRF to the BBERF.
- 13 - Transmission of traffic plane events from the BBERF to the PCRF.
- 14 - Transmission of events reported by the PCEF (P-GW) to the BBERF via the PCRF.
15
16
17

18 The stage 3 information for the Gxa reference point is defined in 3GPP TS 29.212 [20].
19

20 Signaling flows related to the Gxa interface are specified in 3GPP TS 29.213 [21].
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

9 A11 Interface from the HSGW to 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.S0022-0 [3].

Flows showing the use of A11 messages for inter-eAN handoff are found in A.S0022 [3].

A message flow illustrating the use of A11 messages for pre-registration as used for E-UTRAN to eHRPD handoff is shown in section 13.1.

A message flow illustrating the use of A11 messages for handoff as used for E-UTRAN to eHRPD handoff is shown in section 13.1.2.

Flows showing the use of A11 messages for the initial attachment are found in A.S0022 [3].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

10 Interface between the HSGW and the UE

The HSGW and the UE use the PPP protocol with vendor extensions (see RFC 3772 [47]) 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 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 [7], C.S0063 [8] and C.S0087 [9]). 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 [7], C.S0063 [8] and C.S0087 [9]). 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-A [8]) 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 10.1.5). 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 within the VSNP header (see section 10.1.5). The eAN can map reservations with similar QoS from different PDNs onto the same auxiliary service connection of packet-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.

10.1 Main service connection between UE and HSGW

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

10.1.1 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 [10]. 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.

10.1.2 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
- VSNP signaling messages for establishment of EPS bearers and QoS mappings (RSVP)
- User IP packets are also carried over the main service connection per section 10.1.5

The encapsulation format for messages sent over the main service connection is provided in RFC 3748 [46] with the exceptions discussed in sections 10.1.4 and 10.1.5.

10.1.3 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

10.1.4.1 3GPP2 VSNCP Configuration Options

Configuration options shall be encoded as specified in RFC1661 [28]. Table 2 lists all the configuration options required for 3GPP2 VSNCP. A received configuration option that is unrecognized shall be considered unacceptable per RFC 1661 [28].

Table 2 VSNCP Configuration Options

Configuration Option	Type (decimal)	Configuration Option Length (octets)	Value
PDN Identifier	01	3	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.
Access point name	02	2-102	Value field of the Access Point Name IE as defined in TS 24.008 clause 10.5.6.1 [16].
PDN Type	03	3	Valid values are 1 – IPv4 2 – IPv6 3 – IPv4/IPv6 Value portion of the PDN Type IE as defined in 9.9.4.7 of TS 24.301 [16].
PDN address	04	3-15	Value portion of the “PDN Address” IE as defined in Section 9.9.4.9 of TS 24.301 [16]. 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.
Protocol configuration options	05	3-253	Value portion of the Protocol Configuration option value as defined in Section 9.9.4.8 of TS 24.301 [17] and in TS 24.008 [16].
Error Code	06	3	Error Code is used in Configure-Reject message when a PDN connection attempt is unsuccessful. See Table 3 for the supported error code values.
Attach Type	07	3	Valid values are 1 – “initial attach” to a PDN, 3 – “handover” attach to a PDN.
IPv4 Default Router Address	08	6	Encoded a 4-octet IPv4 address. Includes IPv4 Default Router address assigned by PDN gateway for the PDN.
Address Allocation Cause	09	3	See Table 4 for the supported Address Allocation Cause values.
APN-AMBR	10	4-8	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 3GPP TS 24.301 [17].

Table 3 Error Code values

Value – General Description	Explanation of Use
0 - General Error	Used when there is no other specific error code available to report the failure.
1 - Unauthorized APN	Requested APN is not authorized for this user.
2 - PDN Limit Exceeded	Number of PDN for this connection has exceeded the maximum allowed limit.
3 - No P-GW Available	No P-GW address available to establish the PDN connection.
4 - P-GW Unreachable	P-GW is not reachable or not responding.
5 - P-GW Reject	PDN connection attempt rejected by P-GW.
6 - Insufficient Parameters	Request does not have sufficient parameters to proceed.
7 - Resource Unavailable	HSGW does not have sufficient resource to proceed with the request.
8 - Admin Prohibited	PDN connection request is administratively prohibited at the HSGW.
9 - PDN-ID Already In Use	The PDN-ID received in a VSNCP Configure-Request is already in use for a PDN connection.
10 - Subscription Limitation	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.
11 - PDN connection already exists for this APN	A PDN connection has previously been created for the APN specified in the VSNCP Configure-Request message.

Table 4 Address Allocation Cause values

Value (decimal)	Description
00	Null value – used on VSNCP Configure-Request sent by the UE to initiate attachment or handover.
255	Success.
xx	All values supported in TS 29.275 clause 12.1.1.3 [23].

10.1.4.1.1 Configuration Option Data Format

This section specifies the data format for the VSNCP Configuration Options specified in Table 2.

Table 5 Configuration Option Data Format

0	8	16	24	31
Type	Length	Configuration Option Data		
Configuration Option Data				

Type: As specified in Table 2.

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 2.

10.1.4.2 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
- Protocol Configuration Options (PCO)
- Attach Type

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 [12]). 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.

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 [16]) 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 [16]) of the PCO option, when sent in the Configuration Request from UE to HSGW. In addition the UE may also include other parameters defined in the Protocol Configuration Options (TS 24.008 [16]), for example, username and password for authentication with an external AAA server may be included.

1 If the PDN Type is IPv4 or IPv4v6, the UE shall include the IPv4 Default Router Address
 2 Configuration Option. If the *Attach Type* is *Initial*, the value shall be set to 0.0.0.0. If the
 3 *Attach Type* is *Handoff*, the value shall be set to the IPv4 address currently assigned as the
 4 IPv4 default router address.
 5

6 During PDN connection setup, the HSGW shall send this message to the UE. The HSGW
 7 shall send VSNCP Configure-Request only after receiving VSNCP Configure-Request from
 8 the UE. When the HSGW sends this message, the following configuration options are
 9 mandatory.
 10

- 11 - PDN Identifier (This value is copied from the corresponding VSNCP Configure-
 12 Request from the UE.)
 13

14 The UE/HSGW shall ignore unrecognized configuration options present in the VSNCP
 15 Configure-Request. The VSNCP Configure-Reject message shall not be sent for such
 16 requests, if the UE/HSGW can proceed with the PDN connection attempt with available
 17 parameters in the request. The UE/HSGW shall not include those unrecognized parameters in
 18 the VSNCP Configure-Ack message sent in response to the VSNCP Configure-Request.
 19
 20

21 **10.1.4.3 3GPP2 VSNCP Configure-Ack**

22 The HSGW uses this message to respond to a VSNCP Configure-Request message from the
 23 UE, if the PDN connection attempt is successful. The HSGW shall include all acceptable
 24 configuration options present in the corresponding VSNCP Configure-Request message in the
 25 VSNCP Configure-Ack message. The "PDN Address" option shall be included and shall
 26 contain the IPv4 address (if the UE indicated that it wants to obtain the IPv4 address during
 27 PDN connection setup procedures) and/or IPv6 prefix plus IID assigned to the UE for the
 28 PDN by P-GW. For the case where the UE requested and was granted deferred IP address
 29 allocation the IPv4 address field shall be set to 0.0.0.0. The UE shall use the IPv6 prefix
 30 received in the Router Advertisement to create an IPv6 address per clause 4.7.1 in TS 23.402
 31 [15].
 32
 33
 34
 35

36 If the HSGW successfully connects to the default APN, it shall include the APN name of the
 37 default APN in the Access Point Name configuration option.
 38

39 If the UE included the IPv4 Default Router Address Configuration Option in the VSNCP
 40 Configuration-Request message and the P-GW did not return an IPv4 default router address in
 41 the Proxy Binding Acknowledgement, the HSGW shall set the value of the IPv4 Default
 42 Router Address Configuration Option to 0.0.0.0. If the P-GW returned an IPv4 default router
 43 address, the HSGW shall set the value of the IPv4 Default Router Address Configuration
 44 Option to the returned address.
 45

46 The HSGW shall fill in the requested parameters based on the PBA received from the P-GW
 47 in the PBA. The network may indicate its selected mode of bearer control mode using
 48 *Selected Bearer Control Mode* of the PCO option. If this field is not included, then the UE
 49 shall select the default bearer control mode of 'MS only'. If the *MS Support of Network*
 50 *Requested Bearer Control indicator* indicates that the UE doesn't support network initiated
 51 QoS, then the network sets the *Selected Bearer Control Mode* of the PCO option to be 'MS
 52 only mode'. Otherwise, the network sets the mode based on network policy.
 53
 54

55 The UE/HSGW shall validate the Configuration Option values received in the VSNCP
 56 Configure-Ack message. If the UE/HSGW finds the values not acceptable for the PDN
 57 connection, it may decide to terminate the PDN connection.
 58
 59
 60

10.1.4.4 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.

Instead, if the PDN connection is successful, the HSGW changes values of configuration options received in the VSNCP Configure-Request in the VSNCP Configure-Ack message it sends to the UE.

The UE sends a VSNCP Configure-Ack message in response to a VSNCP Configure-Request message, if the received VSNCP Configure-Request is acceptable.

10.1.4.5 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 Configuration-Request from the HSGW if unacceptable Configuration Options are included in the VSNCP Configuration-Request. The Options field is filled with only 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. The configuration options that are included shall not be reordered or modified in any way as specified in RFC 1661 [28]. In addition, the following parameter shall indicate the reason for the failure.

- Error Code

The HSGW may use all error codes specified in Table 3. The UE may use error codes 0 and 6 as specified in Table 3.

10.1.4.6 3GPP2 VSNCP Terminate-Request

The UE and the HSGW use this message to initiate explicit PDN Connection release. The following configuration options are mandatory.

- PDN Identifier

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 PDN is already attached to the UE. 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.

10.1.4.7 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

10.1.4.8 3GPP2 VSNCP Code-Reject

This message is used as specified in RFC1661 [28]. The following configuration options are mandatory.

- PDN Identifier

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

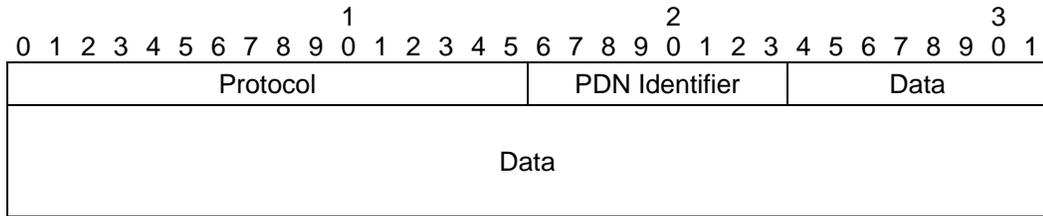
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

10.1.5 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 RFC3772 [47].

VSNP packet format is shown in Table 6.

Table 6 3GPP2 VSNP packet format



- Protocol 0x005b as defined in RFC3772.
- 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.
- Data IPv4 or IPv6 datagrams.

10.1.6 RSVP Protocol

The following RSVP messages [see RFC 2205 [31]] shall be used between the UE and the HSGW to support QoS establishment:

- Resv message
- ResvConf message
- ResvErr message.

RSVP messages shall be carried over the main service connection using the VSNP protocol (see section 10.1.5) by setting the Protocol field to 0x005b (see RFC3772 [47]). RSVP Resv messages shall contain the TFT Information Element that includes Packet Filter List and the QoS List (as required) associated with the specific PDN identified by PDN-ID.

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.S0063 [8].

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 is the source address of the Router Advertisement message sent by the HSGWs (MAGs). The Link Local Address of the HSGW shall be set by the P-GW/LMA and shall not change while the PDN connection is established, as per section 6.8 and 9.3 of RFC 5213 [52].

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 shall be set by the P-GW/LMA in the IPv4 Default-Router Address Option in the corresponding PBA for a given UE (see RFC 5213 [52]), and it shall not change while the PDN connection is established. The HSGW shall set its address to the IPv4 default router address received in the PBA. The UE learns the IPv4 default router address via the VSNCP configuration option in the HSGW initiated VSNCP Configure-Request 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 for RSVP signaling.

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 [16]. 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.

10.1.6.1 Requirements for QoS Updates

10.1.6.1.1 HSGW requirements

During an inter-HSGW handoff with context transfer, if the QoS policy received from the S-HSGW during the context transfer doesn't match with the QoS policy obtained from the PCRF, and if the selected Bearer Control Mode is 'MS/NW mode', 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 mode', 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.

10.1.6.1.2 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.

10.1.6.2 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-D [5].

If the UE receives a ResvErr message from the HSGW, 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 [20]. 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.

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. 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 Flow Identifier in the QoS list. 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". Otherwise, 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.

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-D v1.0 [5] 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 [8]. The UE shall then set up the TFTs as specified in Annex B in X.S0011-D v1.0 [5] using the same Flow ID(s) 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-D v1.0 [5][5] 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 [8].

Note: Use of the BCM mechanism is for further study for inter-RAT handoff.

10.1.6.3 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:

- Initiate flow request with QoS specified,
- Initiate the deletion of 'all' packet filters for TFTs specified in the list of flow identifiers,
- 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-D [5]. 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-D [5]. 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 from the HSGW and set operation code to ‘Replace packet filters in existing TFT’, as specified in X.S0011-D [5]. 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.

Note: Use of the BCM mechanism is for further study for inter-RAT handoff.

10.1.6.4 Resv Message

Resv message is specified in Annex B.1 of X.S0011-D chapter 4 [5]. 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 10.1.6.7.1.

10.1.6.5 ResvConf Message

The format of the ResvConf Message shall follow Annex B.2 of X.S0011-D chapter 4 [5] 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 10.1.6.7.1.

10.1.6.6 ResvErr Message

ResvErr message is specified in Annex B.3 of X.S0011-D chapter 4 [5].

The TFT Error Code value defined below in Table 7 shall be supported in addition to those defined in Annex B.3 of X.S0011-D chapter 4 [5].

Table 7 TFT Error Codes

TFT Error Code	Description	Reason
10000000	Unsuccessful TFT processing	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.
10000001	Invalid IP address	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.
10000010	FlowProfileIDs not supported by the UE	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.
10000011	Invalid PDN-ID in TFT	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.
10000100	QoS Check procedure needs to be performed	Sent from the HSGW to the UE to indicate that the UE needs to perform the check QoS procedure for the QoS and associated Packet Filters(s).

10.1.6.7 Reliable Delivery of RSVP Messages

The HSGW and UE shall follow the requirements of X.S0011-D 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.

10.1.6.7.1 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 below:

Table 8 3GPP2 OBJECT

										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Length										3GPP2 Class										C-Type																			
Transaction ID																																							
IE List																																							
Padding as necessary																																							

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 is as follows.

Table 9 3GPP2 OBJECT- IE List

										1																				2																				3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9										
Length										IE Type #																																																	
IE Data																																																											
IE Data										Padding																																																	

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 10 3GPP2 OBJECT- IE Type #

IE Type #	IE Type# value
TFTIPv4	0
TFTIPv6	2

IE Data: This field is specified in section 10.1.6.7.1.1. Only one IE Data shall be included in each IE.

10.1.6.7.1.1 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 11 TFT IPv4 IE Type# = 0

										1																				2																				3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9										
UE IPv4 address																																																											
D	Reser ved	N S	SR_ID	Reserved					P	TFT Operation Code					Number of Packet filters																																												
Packet filter list																																																											
QoS List																																																											

Table 12 TFT IPv6 IE Type# = 2

1										2										3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
UE IPv6 address																															
UE IPv6 address																															
UE IPv6 address																															
UE IPv6 address																															
D	Reser ved	N S	SR_ID	Reserved					P	TFT Operation Code					Number of Packet filters																
Packet filter list																															
QoS List																															

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. The table below indicates TFT Operation Codes that are used in addition to the TFT Operation Codes specified in X.S0011-D [5].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Table 13 TFT OpCodes

OpCode	Action	Description
00000110	QoS Check	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.
10000000	Initiate Flow Request	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.
10000001	QoS Check Confirm	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.
10000010	Initiate Delete Packet Filter from Existing TFT	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.
10000011	Initiate Replace packet filters in existing TFT	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.

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-D Chapter 4 [5].

Packet Filter List: The packet filter list contains a variable number of packet filters. It shall be encoded same as defined in X.S0011-D Chapter 4 [5] 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-D [5].

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-D [5].

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 14 shows the format of the QoS List.

Table 14 QoS List Layout

0	1	2	3	4	5	6	7
MSB							LSB
QoS List Length (MSB)							
QoS List Length (LSB)							
Flow Identifier 1							
R_QOS_SUB_BLOB_LEN 1							
R_QOS_SUB_BLOB 1							
...							
Result Code 1							
Flow Identifier 2							
R_QOS_SUB_BLOB_LEN 2							
R_QOS_SUB_BLOB 2							
Result Code 2							
...							
Flow Identifier N							
R_QOS_SUB_BLOB_LEN N							
R_QOS_SUB_BLOB N							
----- Result Code N							

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-D [xx]. The VERBOSE field shall be set to ‘0’. The FlowProfileIDs are listed in this parameter in descending order of precedence.

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 below.

Table 15 Result Code Values

Result Code	Description	Reason
00000000	Successful	The HSGW uses this code if the HSGW includes one or more authorized FlowProfileIDs associated with the corresponding Flow Identifier.
00000001	UE Initiated QoS is not authorized	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.
Others	Reserved	

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

10.1.7 Always On service in eHRPD

The HSGW shall support the Always On service for the PPP sessions in the eHRPD system. All users in the eHRPD system are treated as Always On users by default at the HSGW. The HSGW shall implement the PPP inactivity timer which is locally provisioned in the HSGW and it shall be applicable to all PPP sessions in the HSGW. The HSGW shall not implement PPP session timer.

The PPP inactivity timer is a 4-octet unsigned integer. The value of this timer represents the maximum number of consecutive seconds that a PPP session can remain idle before it is torn down.

The HSGW shall set the default value of 0 for PPP inactivity timer for all PPP sessions. The value of 0 indicates infinity. When the timer is set to infinity, the PPP session is not torn down by the HSGW if the UE remains inactive indefinitely. However, the PPP inactivity timer default value is overridden on a per PPP session basis when the HSGW receives a Diameter Idle-Timeout AVP from the AAA during EAP authentication phase. For such PPP sessions, the HSGW shall have a PPP inactivity timer that is set to the value in the corresponding Idle-Timeout AVP and the HSGW shall implement the procedures described in X.S0011-002-D [5]. In eHRPD, all the PPP sessions receive Always On service by default. Hence the “Always On” attribute as specified in X.S0011-002-D [5] is not used by the HSGW. The UE and HSGW shall follow the procedures for inactivity timer as defined in X.S0011-D [5].

If the PPP inactivity timer is overridden by the Idle-Timeout AVP from the AAA, the HSGW shall perform the procedures specified in X.S0011-002-D section 3.2.1.10 [5] to determine the link status and terminate the PPP connection if necessary.

The HSGW should implement a configurable UE Context Maintenance timer, which is locally provisioned in the HSGW. The value of this timer represents the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down. When the Context Maintenance timer expires, the HSGW shall release the LCP context, authentication context, and the A10 connections.

The HSGW starts the UE Context Maintenance timer for a UE session upon receiving a PMIPv6 Binding Revocation Indication (BRI) from a P-GW with revocation trigger = “Inter-MAG Handoff - different Access Types” for the UE session. The HSGW shall reset the UE Context Maintenance timer upon receipt of a new PMIPv6 Binding Revocation Indication (BRI) from a PDN-GW with revocation trigger = “Inter-MAG Handoff - different Access Types” for the UE session. If the PPP inactivity timer for the session expires at the HSGW while the UE Context Maintenance timer is still running for an UE session, the HSGW shall stop the UE Context Maintenance timer expiry and release the UE context.

10.2 Auxiliary service connections between UE and HSGW

In the evolved HRPD system multiple auxiliary service connections¹ 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 PDN-Mux.
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 the example below.

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.

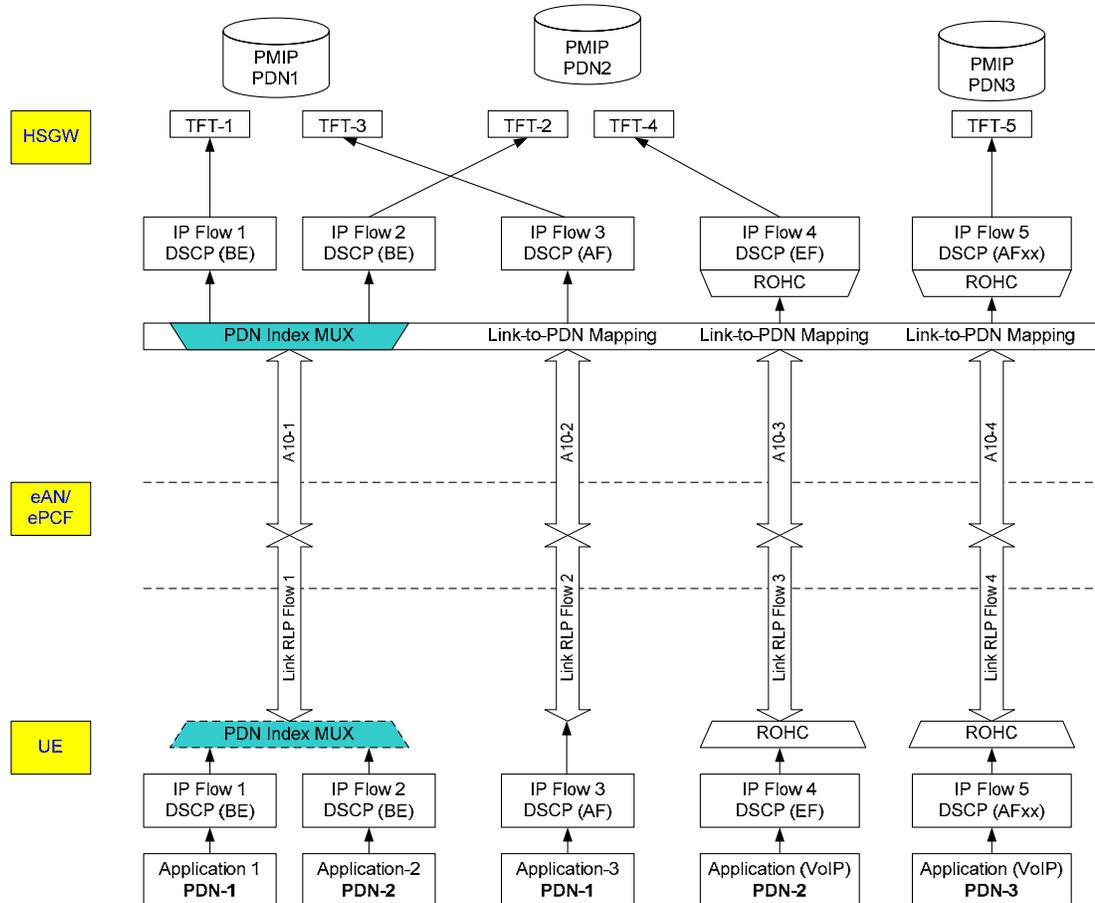


Figure 26 Auxiliary service connections

The above figure 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.

10.2.1 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. When a source HSGW passes context to a target HSGW during a handoff procedure, all PDN-IDs, the APNs associated with the PDNs, the P-GW address(es), and the uplink GRE key(s) used for each PDN are included in the context transferred to the target HSGW.

10.3 Use of the VSNCP Protocol

10.3.1 UE Requested PDN Connectivity

The UE requested PDN connectivity procedure for eHRPD is depicted in Figure 27. 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 created for the default bearer of the default PDN as described in Section 6.4.1. 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. Proxy Mobile IP is used on PMIP-based S2a interface.

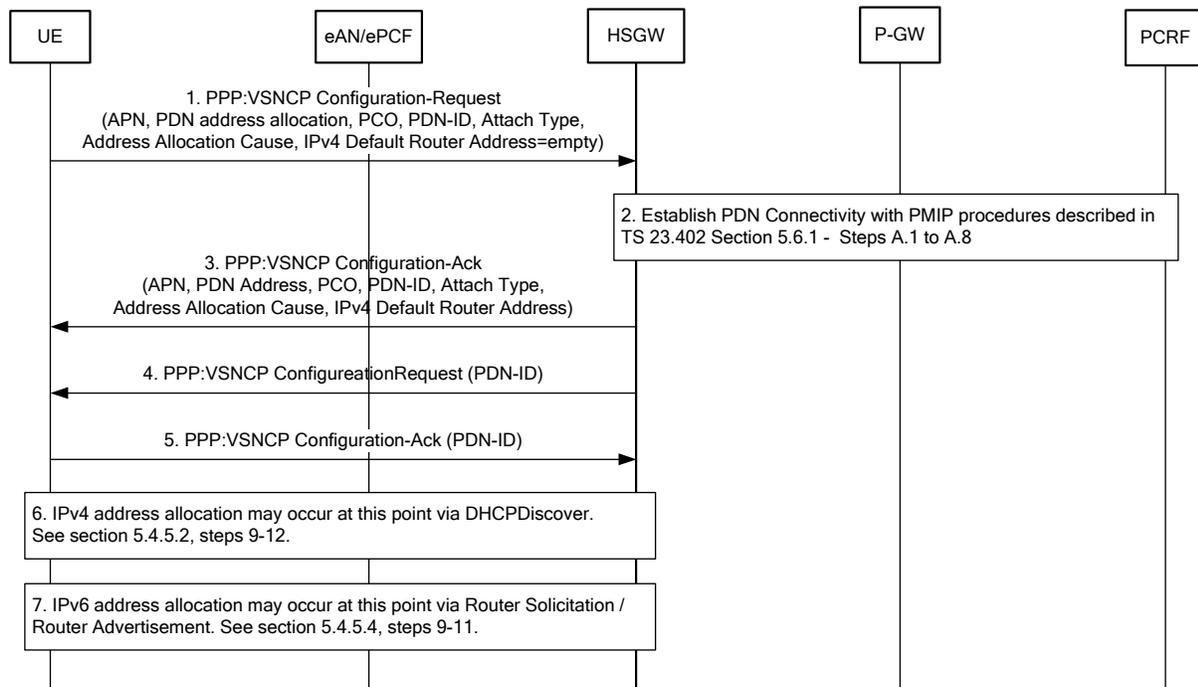


Figure 27 UE Requested Additional PDN Connectivity

1. When the UE wants to establish connectivity to an additional PDN, it will send the VSNCP Configure-Request message (APN, PDN Address, PDN Type, Protocol Configuration Options, and Attach Type). 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 bearers established to support connectivity to the additional PDN may support IPv4 and IPv6. The HSGW verifies that the APN provided by UE is allowed by subscription.
2. The HSGW triggers the procedures for UE requested additional PDN connectivity described in TS 23.402 Section 5.6.1 Steps A.1 through A.8 inclusive TS 23.402 [15]. 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, and Attach Type) message to the UE.

- 1 4. The HSGW sends a VSNCP Configure-Request message to complete the protocol specified in
2 RFC 1661 [28].
- 3 5. The UE responds with a VSNCP Configure-Ack message.
- 4 6. IPv4 address allocation may occur at this point using the procedure shown in section 5.4.5.2 steps
5 9-12.
- 6 7. IPv6 address allocation may occur at this point using the procedure shown in section 5.4.5.4 steps
7 9-11.

10.4 Non-optimized inter-RAT handoff requirements.

13 If the UE is attached to one or more PDNs in E-UTRAN, and if the mobile performs a
14 handoff to eHRPD, then the UE shall perform handoff attach to each of the PDN connections
15 in eHRPD.
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

11 Session Release Call Flows

This section provides the message flows for the different session release scenarios.

11.1 UE Initiated Detach and UE-Requested PDN Disconnection Procedure

The procedures for the UE/HSGW initiated detach and UE-requested PDN disconnect are based on the procedures in Clause 6.4.1 in TS23.402 [15]. The eHRPD radio specific portion of this procedure is described in A.S0022 [3].

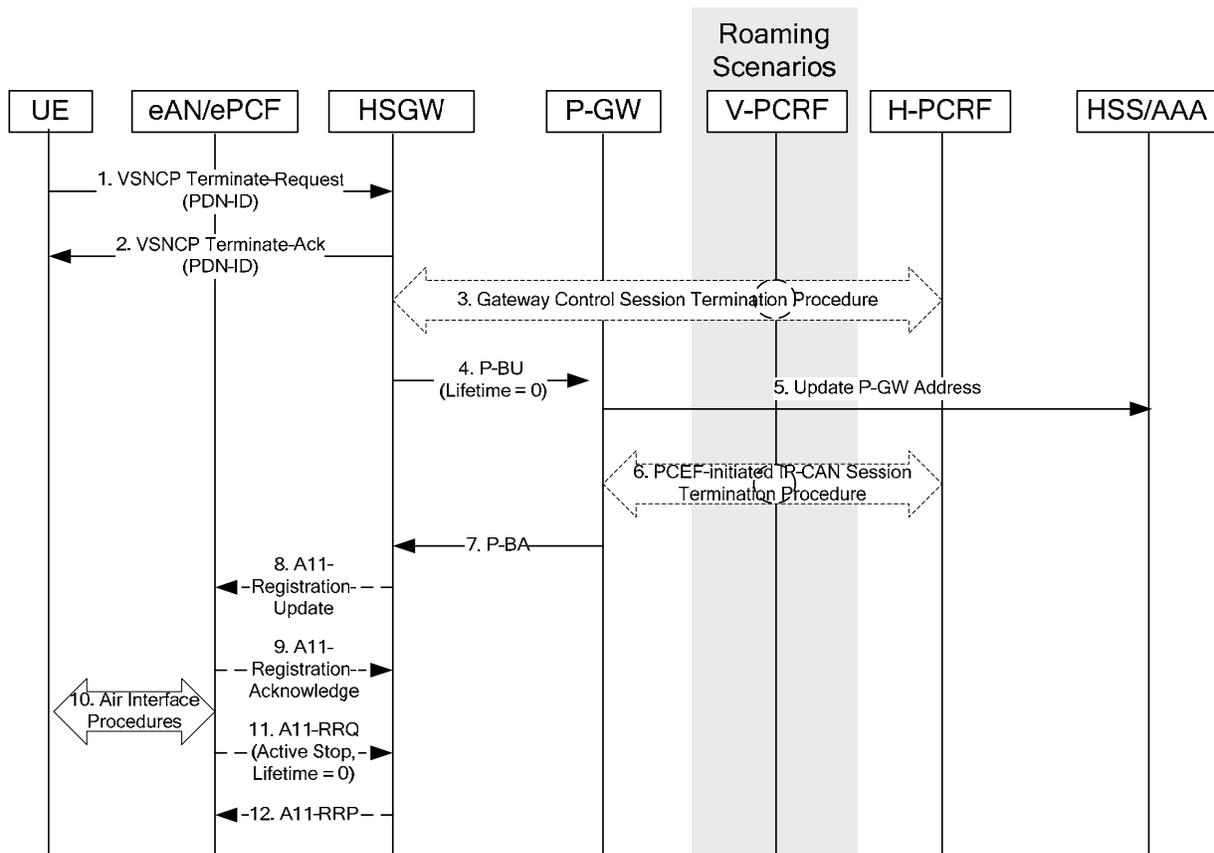


Figure 28 UE initiated detach procedure and PDN-disconnection

For the detach procedure and in case of connectivity with multiple PDNs, steps 1 through 7 are repeated for each PDN the UE wishes to detach from.

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.

- 1 3. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as
2 specified in TS 23.203 [13]. The HSGW no longer applies QoS policy to service data flows for
3 this UE.
- 4 4. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero,
5 indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN
6 is needed in order to determine which PDN to deregister the UE from, as some P-GWs may
7 support multiple PDNs.
- 8 5. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN
9 corresponding to the UE's PDN connection.
- 10 6. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP
11 CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [13].
- 12 7. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends PBA
13 (MN NAI, APN, lifetime=0) to the HSGW.
- 14 8. If all associated PDN connections are released, the HSGW may send an A11-Registration Update
15 message to initiate with the ePCF the release of the dedicated A10 sessions for the UE.
- 16 9. The ePCF responds with an A11-Registration Acknowledge message.
- 17 10. The UE/eAN may initiate HRPD QoS/connection release for the connections associated with the
18 released PDN.
- 19 11. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release
20 A10 session and an Active Stop.
- 21 12. The HSGW responds with A11-Registration Reply with lifetime zero.
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

11.2 Network Initiated Detach and PDN Disconnection Procedure

This section describes the message flows for the PDN connection release due to HSS or AAA initiated release procedures. The HSS can initiate the PDN disconnection 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.

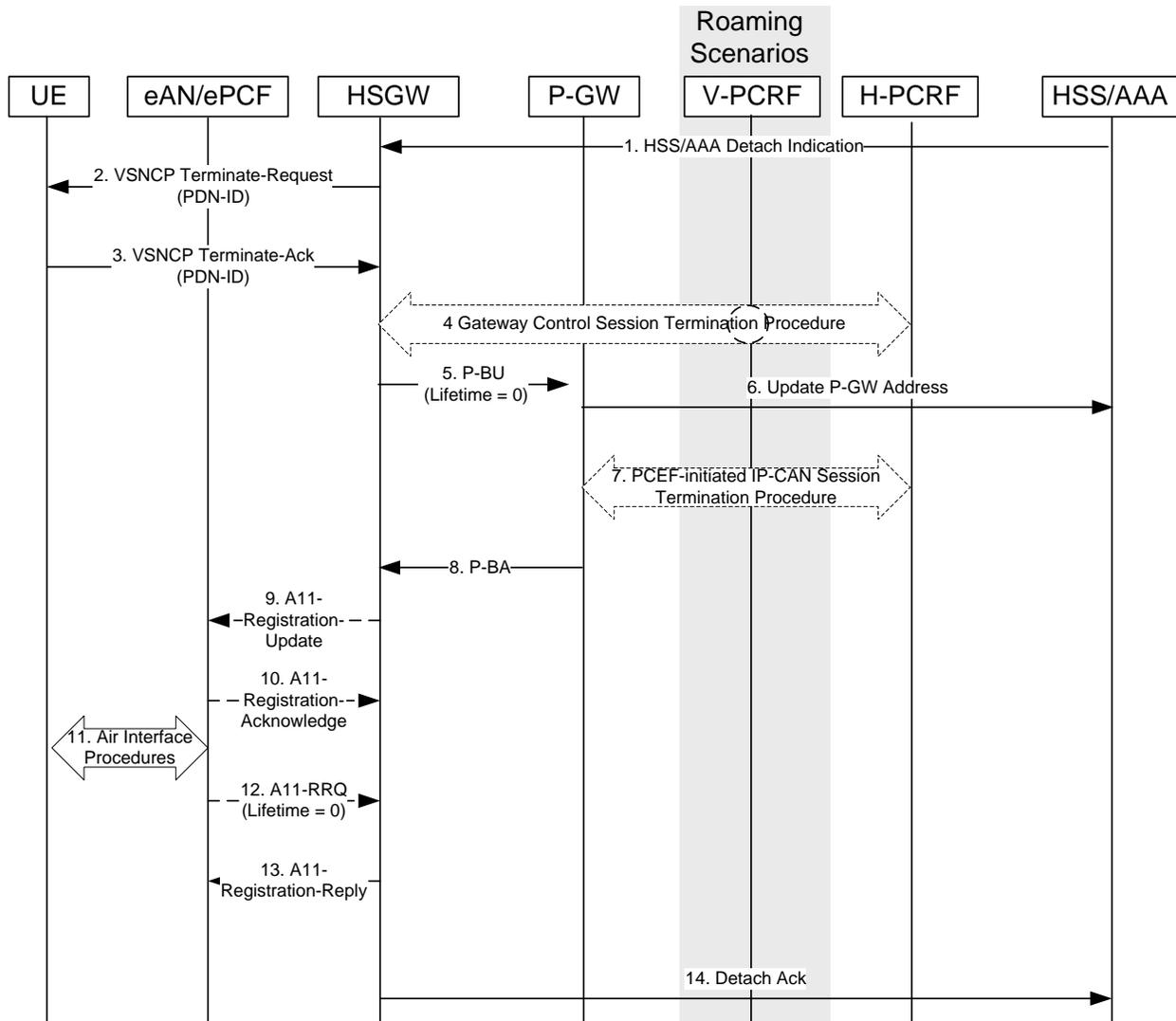


Figure 29 Network initiated detach procedure and PDN-disconnection

1. The HSS/AAA sends a Detach Indication message to the HSGW to detach the UE from the network.

Steps 2 → 8 are repeated for each APN to which the UE is attached and which is to be disconnected.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- 1 2. The HSGW sends a VSNCP Terminate-Request to the UE. The request contains the PDN-ID of
2 the PDN with which the connection is to be terminated.
- 3 3. The UE sends a VSNCP Terminate-Ack to the HSGW to indicate that it received the request to
4 terminate a connection to a PDN.
- 5 4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as
6 specified in TS 23.203 [13]. The HSGW no longer applies QoS policy to service data flows for
7 this UE.
- 8 9. The HSGW sends a PBU (MN NAI, APN, lifetime=0) to the P-GW with lifetime value set to zero,
10 indicating de-registration. The MN NAI identifies the UE to deregister from the P-GW. The APN
11 is needed in order to determine which PDN to deregister the UE from, as some P-GWs may
12 support multiple PDNs.
- 13 6. The P-GW informs the HSS/AAA to remove the P-GW identity information and APN
14 corresponding to the UE's PDN connection.
- 15 7. The P-GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP
16 CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [13].
- 17 8. The P-GW deletes existing entries implied in the PBU from its Binding Cache and sends a PBA
18 (MN NAI, APN, lifetime=0) to the MAG.
- 19 9. If all associated PDN connections are released, the HSGW sends an A11-Registration Update
20 message to initiate with the ePCF the release of the dedicated A10 sessions for the UE. This step
21 may occur immediately after Step 3.
- 22 10. The ePCF responds with an A11-Registration Acknowledge message.
- 23 11. The UE/eAN may initiate HRPD connection release for the connections associated with the
24 released PDN.
- 25 12. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to release
26 A10 session and an Active Stop.
- 27 13. The HSGW responds with A11-Registration Reply with lifetime zero.
- 28 14. The HSGW sends a Detach Ack to the HSS/AAA.
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

12 Inter-HSGW Handoff

This section defines optimized handoff procedures for eHRPD. A diagram of an eHRPD network during optimized handoff is shown in Figure 30 below.

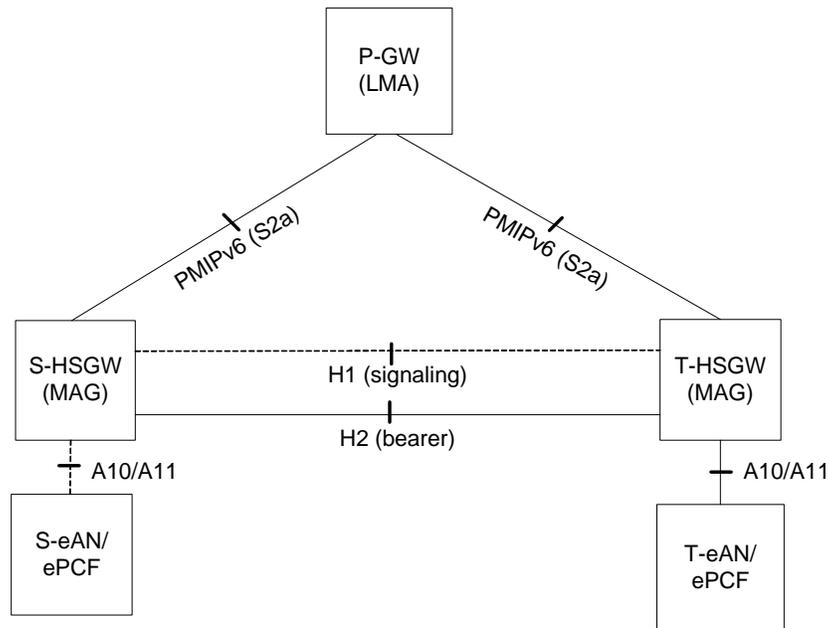


Figure 30 Inter-HSGW Interworking Architecture in eHRPD

Two HSGWs are depicted in Figure 30, 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 (PMIPv6-based) interface. During an inter-HSGW optimized handoff, 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 optimized handoff procedures consist of three elements: H2 tunneling, H1 context transfer, and proxy Mobile IP binding update via the S2a interface. The H2 tunnel setup procedure and the context transfers happen in parallel. The proxy Mobile IP procedure in the T-HSGW happens after context transfer.

When the UE moves to the serving area of a new eAN/ePCF and the eHRPD session is successfully transferred from the Serving eAN/ePCF to the Target eAN/ePCF, if the Serving HSGW is not reachable from the Target eAN/ePCF, then the Target ePCF selects a Target HSGW for the session and provides to the Target HSGW during the A10 session establishment the Serving HSGW H1 IP address information received from the Serving

1 eAN/ePCF. The Target HSGW initiates context transfer of the HSGW session state from the
2 Serving HSGW.
3

4 The H2 tunnel is established as a result of a trigger from the lower layers (A11 interface) at
5 the Target HSGW, and is used to carry IP packets that may be header and/or payload
6 compressed. The detail procedures for the establishment, context transfer, and release of the
7 H2 tunnels are specified in the following sub-sections.
8
9

10 **12.1 Optimized Handoff**

11 This section describes inter-HSGW optimized handoff call flows for eHRPD.
12
13

14 **12.1.1 Call Flows**

15 Example call flows for inter-HSGW optimized handoffs for eHRPD are illustrated below. For
16 inter-eAN/ePCF dormant and active handoff, the existing interfaces of A13/A16 can be used.
17 The signaling interface between the HSGWs is used for context transfer, such as UE's IP
18 address(es), TFTs, PPP state, etc. The data interface is used for UL and DL data transfer for
19 the UE from S-HSGW to T-HSGW during handover.
20
21
22

23 Figure 31 illustrates an example call flow for an eHRPD inter-HSGW handoff when the
24 eHRPD session is in connected-state and the S-eAN/ePCF cannot include sectors from the T-
25 eAN/ePCF in the Active Set.
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

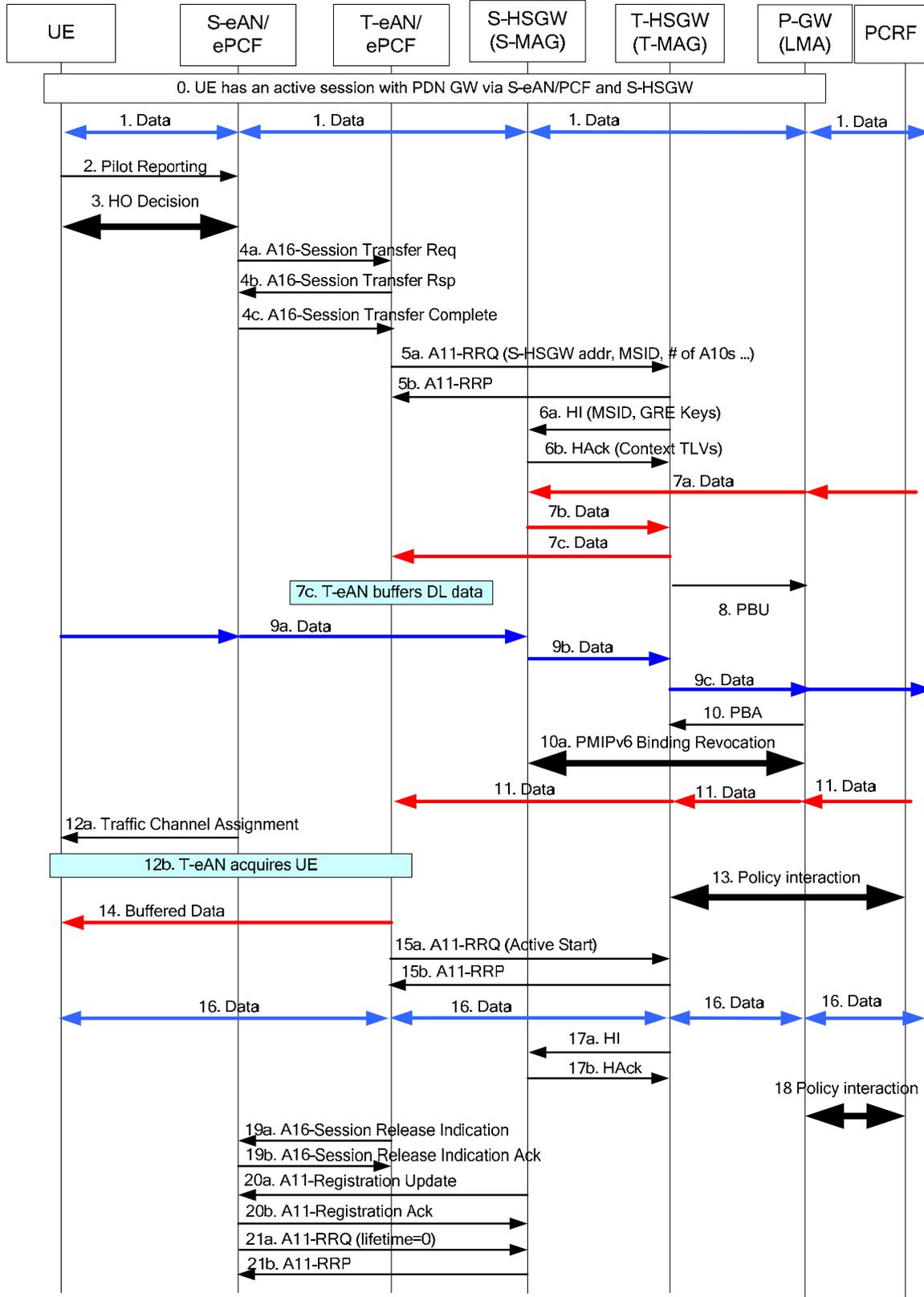


Figure 31 Inter-HSGW Active Handoff

The steps in Figure 31 are described below.

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 reports pilot strength to the serving eAN/ePCF (S-eAN/ePCF).
 3. The S-eAN/ePCF determines the need for handing off the UE to the target eAN/ePCF (T-eAN/ePCF).
 4.
 - a. The S-eAN/ePCF sends A16-Session Transfer Request message to the T-eAN/ePCF to request the eHRPD session transfer for the UE. The A16-Session Transfer Request message shall include the Session State Information Records of the eHRPD session. For details see [3].
 - b. The T-eAN/ePCF accepts the request by sending A16-Session Transfer Response message to the S-eAN/ePCF.
 - c. The S-eAN/ePCF sends an A16-Session Transfer Complete message to the T-eAN/ePCF. Since some Session State Information Records may be changed after A16-Session Transfer Request has been sent, this message shall include Session State Information Records that have been changed from session indicated by the A16-Session Transfer Request message as modified by the session changes in the A16-Session Transfer Response message.
 5.
 - a. The T-eAN/ePCF sends an A11-Registration Request message to the T-HSGW to signal the handoff. The message includes the S-HSGW's IP address, MSID of the UE, and sets the A10 connections for the UE, etc. The T-eAN/ePCF sends this message anytime after step 4a.
 - b. The T-HSGW accepts the connection and sends A11-Registration Reply Message back to the T-eAN/ePCF with an accept indication.
 6.
 - a. Triggered by step 5a, the T-HSGW sends a Handover Initiate (HI) message (see draft-ietf-mipshop-pfmipv6 [53]) 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 UL data to the T-HSGW and one GRE tunnel for forwarding the DL data to the T-HSGW.
 - b. The S-HSGW sends a Handover Ack (HACK) message to the T-HSGW with the session context information TLVs as defined in section 12.4.2. 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, 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, P-GW address, and GRE key for UL traffic to the P-GW is included in the context that is transferred.
 7.
 - a. The S-HSGW extracts the DL packets from the PMIPv6 tunnel from the P-GW and forwards the DL packets to the T-HSGW over the DL GRE tunnel.
 - b. A PDN-ID is added in front of the packet and the packet is sent as received from the P-GW.
 - c. The T-HSGW performs necessary packet processing operation for these DL packets and forwards them to the T-eAN/ePCF. The DL 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.
 8. Triggered by step 6b, 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.
 9.
 - a. The UL data packets that the UE is still sending over the S-eAN/ePCF are received at the S-HSGW.

- b. These packets are forwarded by the S-HSGW to the T-HSGW. 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). The S-HSGW also forwards any control plane packets, e.g., RSVP, DHCPv4 etc., from the UE that is sent over the S-eAN/ePCF to the T-HSGW.
- c. The T-HSGW performs all necessary packet processing operations for these UL packets. In this specification it is not required for the T-HSGW to wait for the PBA as specified in RFC 5213 [52], therefore the HSGW forwards these packets to the P-GW. The UL packets are sent to the T-HSGW over the UL GRE tunnel. The S-HSGW copies the payload of the GRE packet it receives over the A10 tunnels and adds an SRID in front of the A10 payload and puts this as the payload of the UL GRE tunnel.
- Note: The SRID will be the same after the Handover for each service connection, and that the T-HSGW will be able to correlate the traffic with a particular A10 based on the SRID it receives with the packet.
10. The P-GW/LMA updates its BCE, switches the data path to the T-HSGW (new MAG) and returns a PBA to the T-HSGW to indicate successful operation. Anytime after step 10, the P-GW may perform a Registration Revocation procedure with the S-HSGW.
 - a. The P-GW sends a BRI to the S-HSGW and receives an acknowledgement.
 11. Now that the BCE is updated and the data-path is switched, the DL 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.
 12. a. The S-eAN/ePCF sends a Traffic Channel Assignment message to instruct the UE to switch to the new Active Set. This step can occur anytime after step 4b.
 13. b. The T-eAN/ePCF acquires the UE. The T-eAN may begin transmitting data to the UE upon completion of this step.
 14. 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 6b.
 15. The T-eAN/ePCF starts emptying its buffer and it delivers the buffered DL packets to the UE.
 - a. Anytime after Step 12, the T-eAN/ePCF sends A11-Registration Request message to T-HSGW which includes an Active Start Airlink record. This is to indicate that the data path is now established.
 - b. The T-HSGW sends A11-Registration Reply message to the T-eAN/ePCF.
 16. At this time, both UL and DL traffic for the UE are going through the target system. The UE can begin to send UL packets as soon as step 12 happens. Also, the T-HSGW begins forwarding DL data directly received from the P-GW anytime after step 10.
 17. a. 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.
 - b. 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 8).
 19. a. 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.

1 b. The S-eAN/ePCF sends an A16-Session Release Indication Ack message to the T-eAN/ePCF.

2 20. a. After step 17b, the S-HSGW sends A11-Registration Update message to S-eAN/ePCF to
3 request tearing down the bearer connection with the S-eAN/ePCF.

4 b. The S-eAN/ePCF sends A11-Registration Ack message to the S-HSGW.

5 21. a. The S-eAN/ePCF sends A11-Registration Request message (with lifetime=0) to S-HSGW to
6 tear down the bearer between with the S-eAN/ePCF.

7 b. The S-HSGW sends A11-Registration Reply message to the S-eAN/ePCF to confirm the de-
8 registration process.

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.2 Dormant Handoff

This section describes inter-HSGW dormant handoff call flows for eHRPD.

12.2.1 Call Flows

Figure 32 illustrates an example call flow for an eHRPD inter-HSGW dormant handoff.

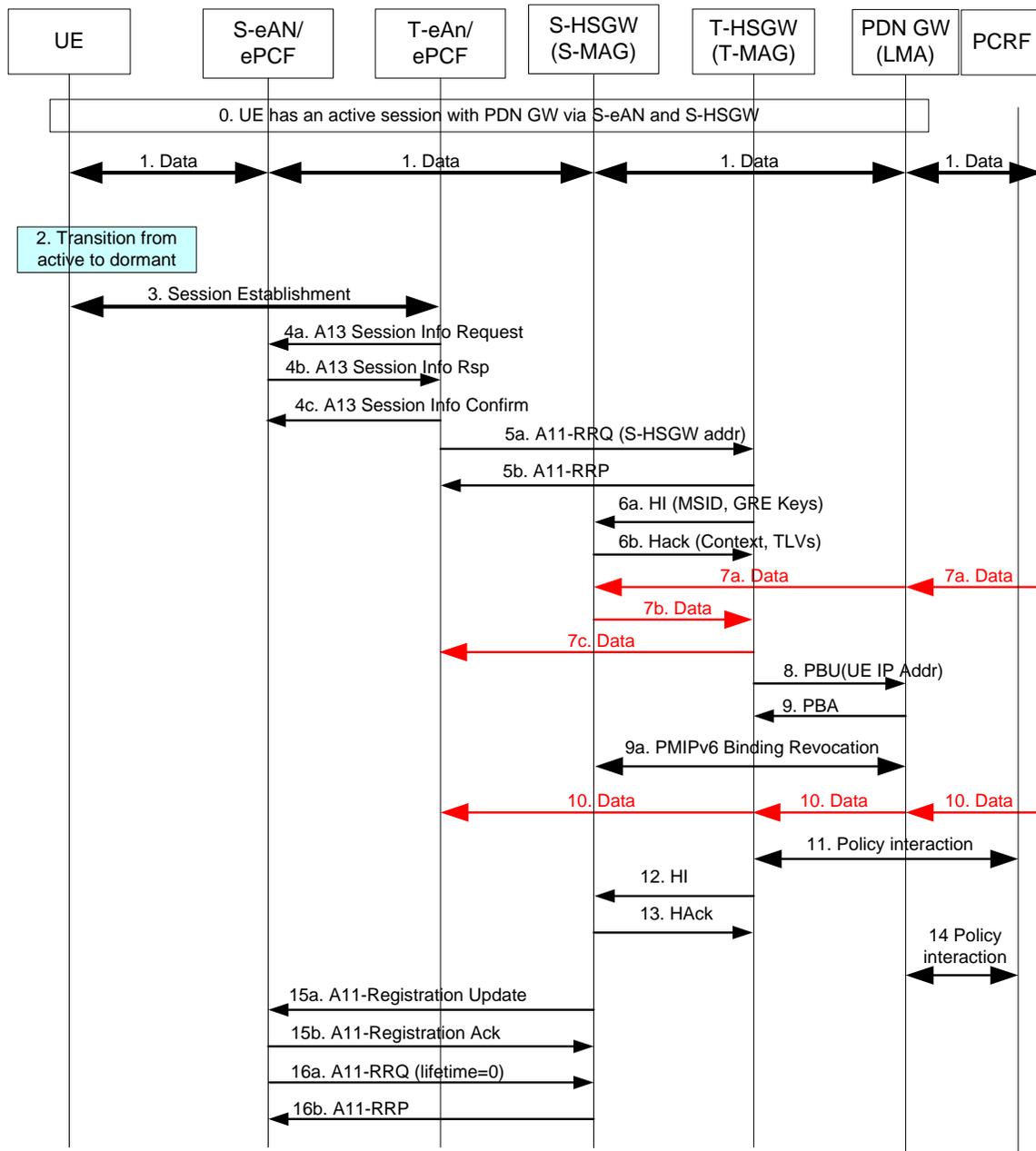


Figure 32 Inter-HSGW Idle Handoff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- 1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
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 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.
 - a. 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.
 - b. 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.
 - c. 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.
 - a. The T-eAN/ePCF sends A11-Registration Request message to the T-HSGW to signal the handoff. The request includes the S-HSGW's IP address MSID of the UE, and sets the A10 connections for the UE, etc. The T-eAN/ePCF sends this message anytime after step 4a.
 - b. The T-HSGW accepts the connection and sends A11-Registration Reply Message back to the T-eAN/ePCF with an accept indication.
 6.
 - a. Triggered by step 5a, the T-HSGW sends a Handover Initiate (HI) message, see draft-ietf-mipshop-pfmipv6 [53], 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 UL data to the T-HSGW and one GRE tunnel for forwarding the DL data to the T-HSGW.
 - b. The S-HSGW sends a Handover Ack (HACK) message to the T-HSGW with the session context information TLVs as defined in section 12.4.2. 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, 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, P-GW address, and GRE key for UL traffic to the P-GW is included in the context that is transferred.
 7.
 - a. The S-HSGW extracts the DL packets from the PMIPv6 tunnel from the P-GW and forwards the DL packets to the T-HSGW over the DL GRE tunnel.
 - b. A PDN-ID is added in front of the packet and the packet is sent as received from the P-GW.
 - c. The T-HSGW performs necessary packet processing operation for these DL packets and forwards them to the T-eAN/ePCF. The DL 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.
 8. Triggered by step 6b, 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.

9. The P-GW/LMA updates its BCE, switches the data path to the T-HSGW (new MAG) and returns a PBA to the T-HSGW to indicate successful operation. Anytime after step 10, the P-GW may perform a Registration Revocation procedure with the S-HSGW.
 - a. The P-GW sends a BRI to the S-HSGW and receives an acknowledgement.
10. Now that the BCE is updated and the data-path is switched, the DL 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.
11. 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 6b.
12. 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.
13. 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.
14. 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 8).
15.
 - a. After step 6a, 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.
 - b. The S-eAN/ePCF sends an A11-Registration Ack message to the S-HSGW.
16.
 - a. 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.
 - b. The S-HSGW sends an A11-Registration Reply message to the S-eAN/ePCF to confirm the de-registration process.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.3 Intra-eHRPD Handover with HSGW Relocation without Context Transfer

Inter-HSGW handover without context transfer is an optional procedure.

The UE performs handover to a Target eAN where the Target eAN selects a T-HSGW. Since there is no trust relationship between the T-HSGW and S-HSGW, the T-HSGW requires the UE to perform LCP and attach procedure 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.

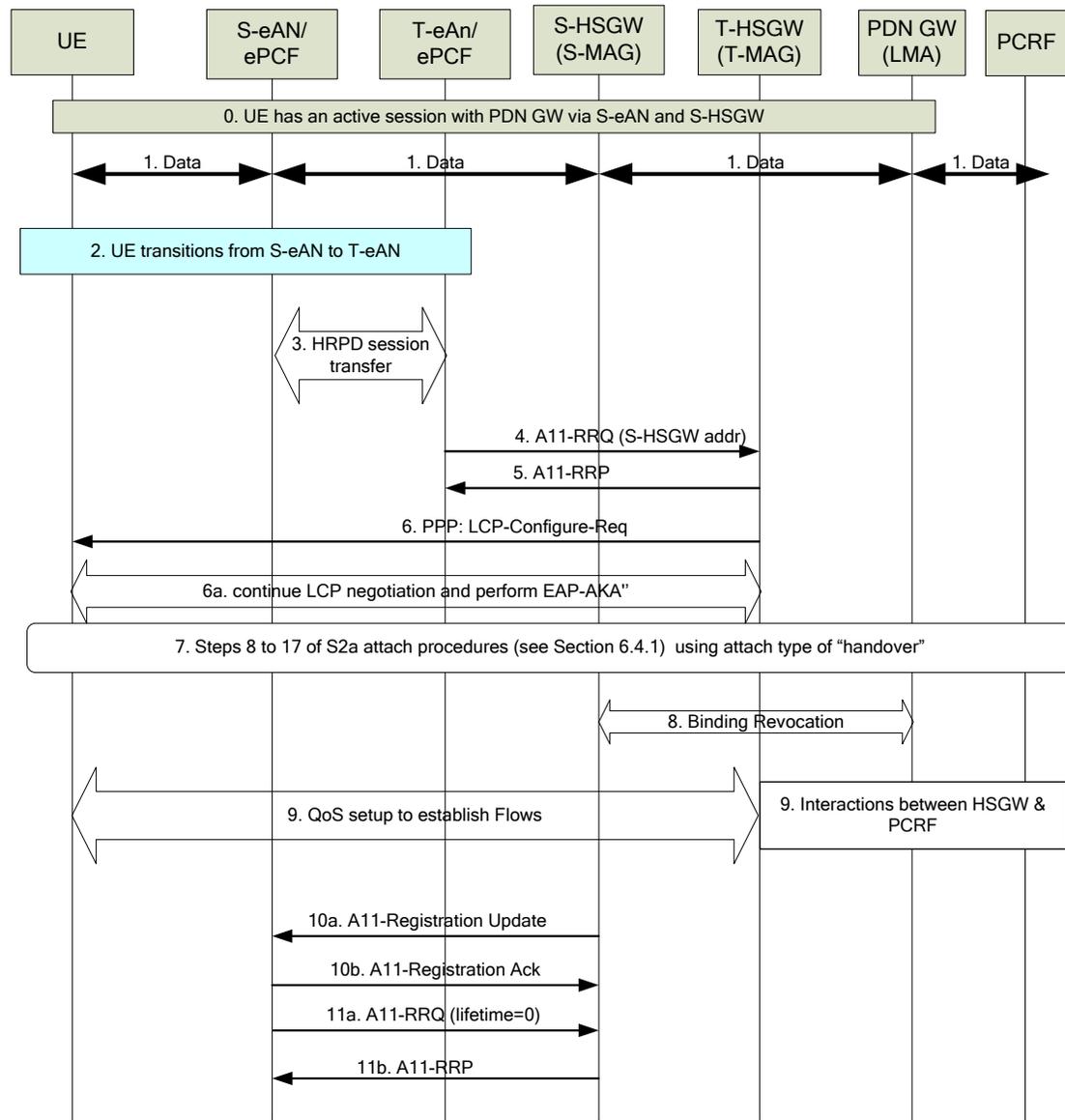


Figure 33 Intra-eHRPD Handover with HSGW Relocation without Context Transfer

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
 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
 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
 3. The eHRPD session is transferred from S-eAN/ePCF to T-eAN/ePCF. 4
 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
 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
 6. Because the T-HSGW does not have an authentication context for the UE, the T-HSGW sends an LCP Configure Request to the UE. 7
 - a. The UE, HSGW, and AAA Server continue the LCP negotiation procedures. EAP-AKA' is executed as the authentication protocol. 8
 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 6.4.1. The following changes are required to the flow in Section 6.4.1: 9
 - i. Step 8 in Section 6.4.1: 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. 10
 8. The P-GW sends a PMIPv6 Binding Revocation Indication to the S-HSGW and receives an acknowledgement. 11
 9. If the Selected Bearer Control Mode of the PCO option is set to is 'Network only mode' or 'MS/NW mode', 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. 12
- Steps 7-9 are repeated for each PDN connection that the UE had on the S-HSGW. 13
10. a. 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. 14
 - b. The S-eAN/ePCF sends an A11-Registration Ack message to the S-HSGW. 15
 11. a. 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. 16
 - b. The S-HSGW sends an A11-Registration Reply message to the S-eAN/ePCF to confirm the de-registration process. 17

12.4 Inter-HSGW Stage 3

The protocol used for inter-HSGW handover is as per draft-ietf-mipshop-pfmipv6 [53]. For inter-HSGW handover signaling purposes, the reactive handover procedure as described in this document applies. Also, the Mobility Header-based messages shall be used between the HSGWs. The Vendor Specific Option as defined in this document shall be used to carry the context parameters needed for eHRPD. The vendor ID shall be set to 5532 (3GPP2). The vendor specific parameters are defined in the TLV format as per section 12.4.2. 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.

12.4.1 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 handover, 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 5.2.2.3.

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.

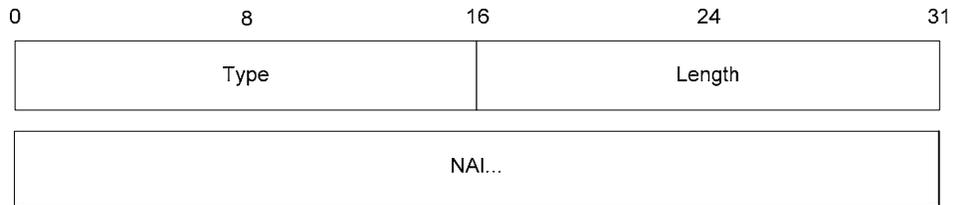
12.4.2 Context Parameter TLVs

This section defines the TLVs that are needed for context transfer between the S-HSGW and T-HSGW. Per draft-ietf-mipshop-pfmipv6 [53], the ‘Length’ field in these TLVs includes the length of the ‘Type’ and the ‘Length’ fields as well.

12.4.2.1 User NAI

This TLV is of the following format. It carries the NAI of the user.

Table 16 User NAI TLV



Type: 1

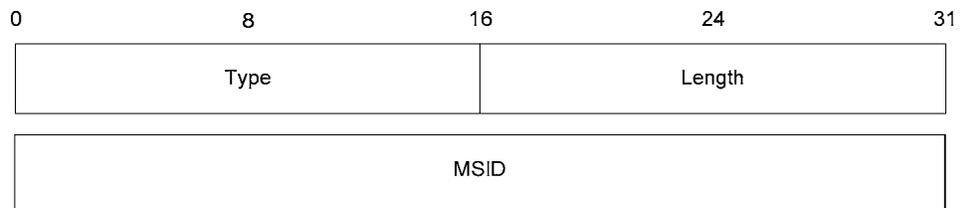
Length: ≤ 74 octets

NAI: This is the NAI associated with the user which is received during EAP authentication. The format as specified in TS 23.003 [12].

12.4.2.2 User MSID

This TLV is of the following format. It carries the MSID of the user.

Table 17 User MSID TLV



Type: 2

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 [4].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.4.2.3 LCP Info

This TLV contains the parameters negotiated via the LCP during PPP connection establishment between the HSGW and the UE.

Table 18 LCP Info TLV

0	8	16	24	31
Type				Length
HP	UP	HA	UA	Reserved
HSGW-Magic Number				
UE-Magic Number				
HSGW-MRU			UE-MRU	
HSGW-Auth-Proto			UE-Auth-Proto	

Type: 3

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). 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). 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). 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 [28].

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 [28].

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 [28].

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 [28].

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 [28].

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 [28].

12.4.2.4 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 [29].

Table 19 CCP Info TLV

0	8	16	24	31
Type		Length		
HSGW-Comp-Proto		UE-Comp-Proto		

Type: 4

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.

12.4.2.5 VSNCP State and Common Info

This TLV contains the list of PDN IDs established with VSNCP.

Table 20 VSNCP State and Common Info TLV

0	8	16	24	31
Type		Length		
List of PDN IDs				

Type: 5

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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.4.2.6 PDN Info

This TLV contains the PDN specific common info. This TLV shall be repeated for each connected PDN at the S-HSGW.

Table 21 PDN Info TLV

0	8	16	24	31
Type		Length		
PDN ID		Reserved		
APN				

Type: 6

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 [18].

12.4.2.7 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.

Table 22 PCO Info TLV

0	8	16	24	31
Type		Length		
PDN ID		Reserved		
PCO				

Type: 7

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 [16].

12.4.2.8 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.

Table 23 PDN Address Info TLV

0	8	16	24	31
Type		Length		
PDN ID	PDN Type	DHCP	Reserved	
IPv6 Prefix				
IPv6 Prefix				
IPv6 IID				
IPv6 IID				
IPv6 LLA				
IPv4 Address				
IPv4 Default Router Address				

Type: 8

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1 IPv4 Address has been assigned, the IPv4 Address and IPv4 Default Router Address fields
2 carry non-zero PDN Addresses.

3 DHCP-bit: When set, this bit indicates that DHCPv4 is used to allocate the UE's IPv4
4 address.

5
6 Reserved: Reserved for future use. Set to all 0s.

7 IPv6 Prefix: This field (8 octets long) carries the IPv6 prefix associated with the PDN
8 connection of the UE.

9
10 IPv6 IID: This field (8 octets long) carries the IPv6 interface identifier assigned to the UE.

11 IPv6 LLA: This field (16 octets long) carries the IPv6 link-local address assigned by the
12 P-GW used by the HSGW on the access link shared with the UE.

13
14 IPv4 Address: This field (4 octets long) carries the IPv4 Address is assigned to the UE.

15
16 IPv4 Default Router Address: This field (4 octets long) carries the UE's IPv4 default router
17 address.

18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.4.2.9 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.

Table 24 PMIPv6 Info TLV

0	8	16	24	31
Type		Length		
PDN ID	TT	Reserved		
LMA IPv6 Address				
LMA IPv6 Address				
LMA IPv6 Address				
LMA IPv6 Address				
LMA IPv4 Address				

Type: 9

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.

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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

12.4.2.10 ROHC Configuration Info

This TLV contains the parameters negotiated for ROHC compression.

Table 25 ROHC Configuration Info TLV

0	8	16	24	31
Type		Length		
CM	Reserved-1		Reservation Label (FlowID)	
Forward/Reverse-MAX-CID		Forward/Reverse-MRRU		
LC	Reserved-2		Forward/Reverse Profile-Count	
Forward/Reverse Profiles				

Type: 10

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.

Reservation Label (Flow ID): This is the Flow ID 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 or 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 [39].

12.4.2.11 ROHC IR Info

This TLV contains the ROHC IR packet received from the UE for a given Flow ID of the UE.

Table 26 ROHC IR Info TLV

0	8	16	24	31
Type		Length		
Reservation Label (FlowID)		Reserved		
ROHC IR Packet				

Type: 11

Length: ≥ 8 octets

Reservation Label (Flow ID): This is the Flow ID associated with this ROHC parameter set.

Reserved: Reserved for future use. Set to all 0s.

ROHC IR Packet: ROHC IR packets for the associated Flow ID, as per RFC 3095 [39].

12.4.2.12 QoS Info

This TLV contains the parameters related to QoS for the UE.

Table 27 QoS Info TLV

0	8	16	24	31
Type		Length		
FlowID		Granted FlowProfileID		
Updated FlowProfileID		Requested FlowProfileIDs		

Type: 12

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-D [5].

Updated FlowProfileID:

This is the most recently sent updated FlowProfileID for the Flow ID. See: X.S0011-D [5].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Requested FlowProfileIDs:

This is the list of requested QoS for the Flow ID. See: X.S0011-D [5] . Each FlowProfileID in the list is two octets long.

12.4.2.13 TFTv4 Info

This TLV contains the parameters related to IPv4 TFT for the UE.

Table 28 TFTv4 Info TLV

0	8	16	24	31
Type		Length		
TFT IPv4 IE Type # = 0...				

Type: 13

Length: > 4 octets

TFT IPv4 IE Type #0: This is the IPv4 TFT object as defined in X.S0011-D [5] .

12.4.2.14 TFTv6 Info

This TLV contains the parameters related to IPv6 TFT for the UE.

Table 29 TFTv6 Info TLV

0	8	16	24	31
Type		Length		
TFT IPv6 IE Type # = 2...				

Type: 14

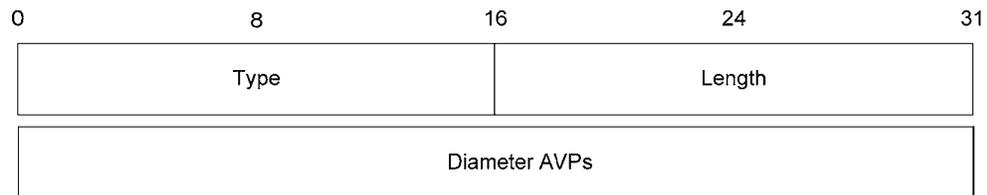
Length: > 4 octets

TFT IPv6 IE Type #0: This is the IPv6 TFT object as defined in X.S0011-D [5] .

12.4.2.15 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 [22].

Table 30 AAA Profile Info TLV



Type: 15

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.

12.4.2.16 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.

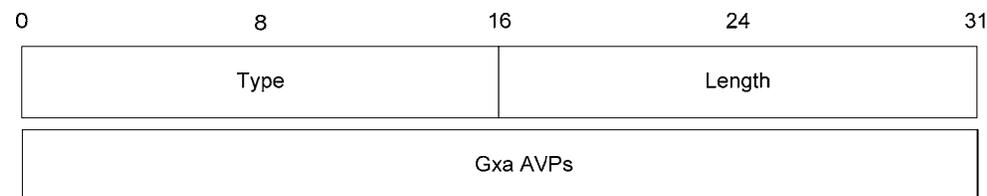


Table 31 Gxa Info TLV

Type: 16

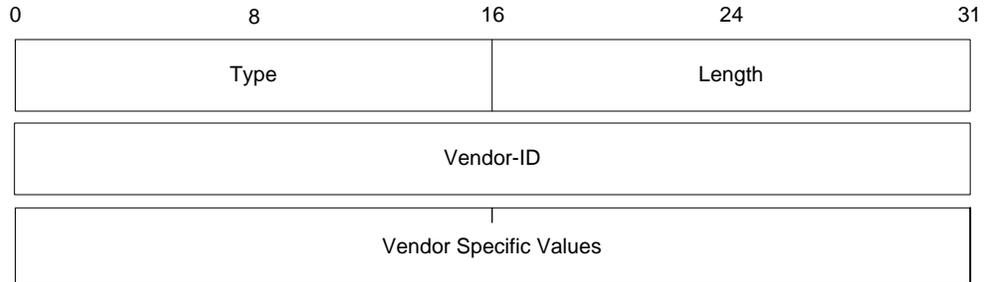
Length: > 4 octets

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 [20].

12.4.2.17 Vendor Specific Info

This TLV contains the parameters required by specific vendor's implementation.

Table 32 Vendor Specific Info TLV



Type: 17

Length: > 4 octets

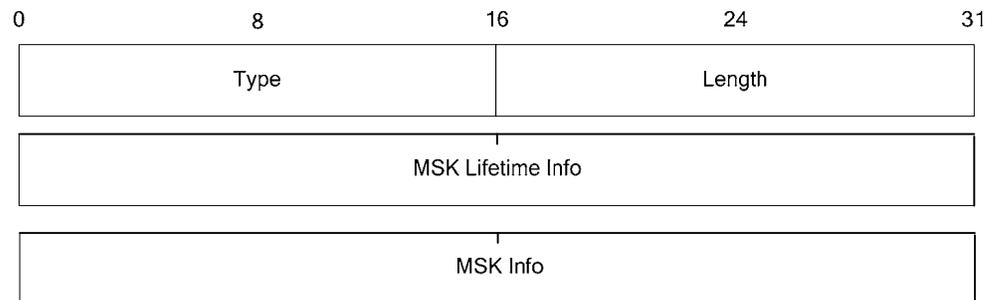
Vendor-ID: This is vendor identifier for the vendor that has a specific use of this TLV.

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.

12.4.2.18 MSK Info

This TLV contains the MSK Info AVPs.

Table 33 MSK Info TLV



Type: 18

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.

13 Handoff FROM E-UTRAN to eHRPD

Figure 34 and Figure 35 show E-UTRAN to eHRPD active mode handoff handover flows for both non-roaming and roaming scenarios. Figure 36 and Figure 37 show E-UTRAN to eHRPD idle mode handoff flows in the same eHRPD eAN and a different eHRPD eAN respectively. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 tunnel is established between the SGW and the P-GW in the evolved packet core. The flows for pre-registration and E-UTRAN to eHRPD handover phase are shown in the following figures.

13.1 Active Mode Handoff

13.1.1 eHRPD Pre-registration via E-UTRAN

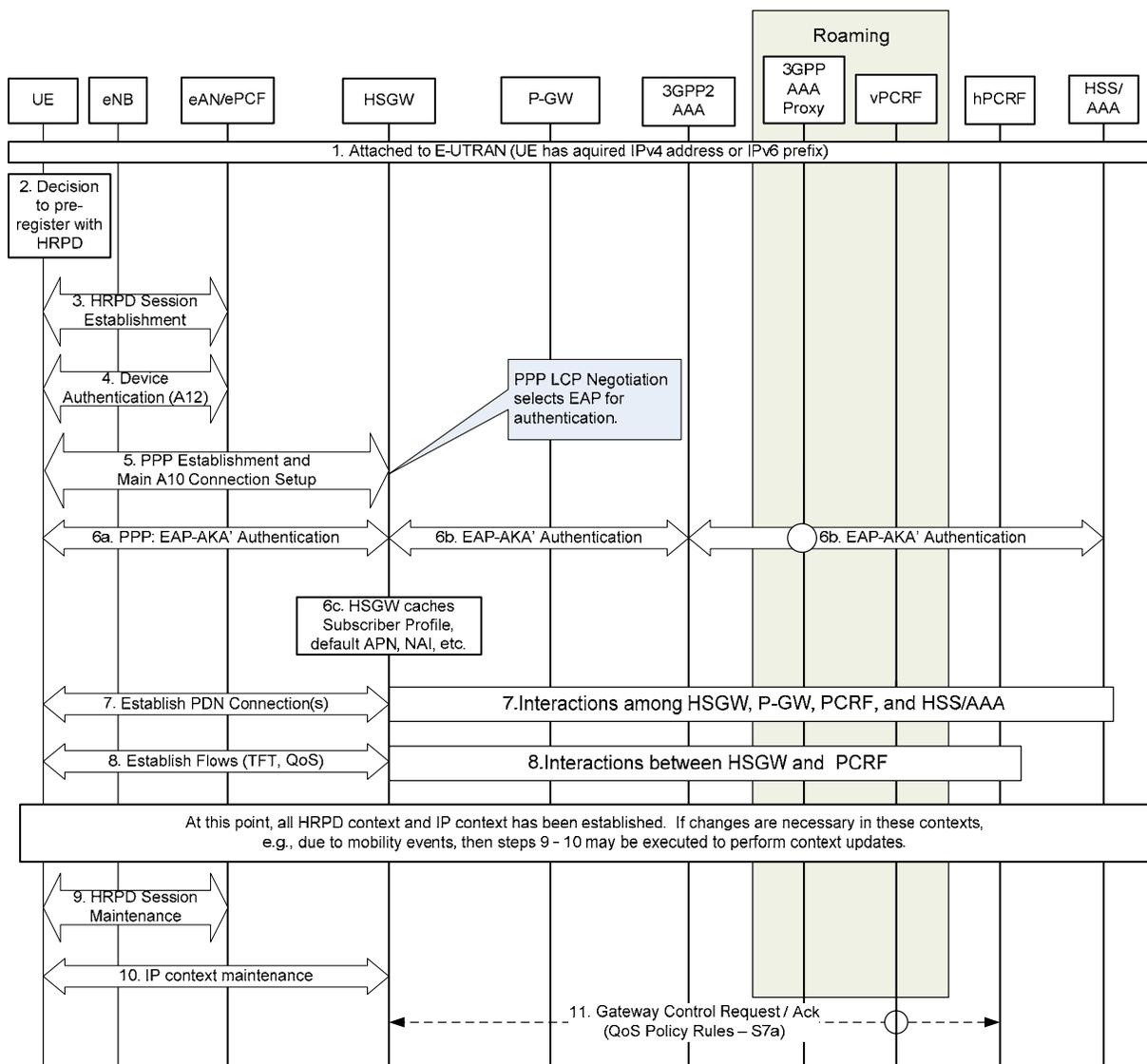


Figure 34 eHRPD Pre-registration via E-UTRAN

1. The UE is initially attached to the E-UTRAN network. It has a PMIPv6 tunnel on the S5 interface (non-roaming) or the PMIP-based S8 interface (roaming). The UE acquires IPv4 address(es) and/or IPv6 prefix(es) through the PMIPv6 registration process. Data flows between the UE and the P-GW through the eNodeB and the SGW.
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.
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.S0022-0 [3].
5. The eHRPD eAN/ePCF establishes the main A10 connection with the HSGW by exchanging A11-RRQ/RRP messages. The A11-Registration Request message contains an indication that the access is occurring through the S101 tunnel. For details refer to A.S0022-0 [3]. This information is used by the HSGW to determine that PMIP bindings do not need to be triggered. 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 5.2. 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 P-GW address to the eHRPD system in this step (upon successful authentication and authorization).
c. The HSGW stores the P-GW IP address and default APN, QoS profile and other user context information received from the 3GPP AAA/HSS server.
7. The UE exchanges VSNCP messages with the HSGW for all PDNs (See section 6.4.1 for details) that it currently has attachments to within E-UTRAN. The VSNCP-Configure-Request sets the Attach Type to "handoff". Also, the UE includes the IP address(es) it obtained via LTE in the VSNCP-Configure-Request. The PBU(s) will be sent to complete the PDN attachment setup(s) when the UE completes a handover to eHRPD. Interactions occur among the HSGW and PCRF per 3GPP specifications (TS23.402 [15] 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.
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 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 IP service context between the UE and the HSGW. This is accomplished by signaling those changes between the UE and HSGW via S101 tunneling.
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 [13]. The HSGW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [13].

13.1.2 Handover Phase

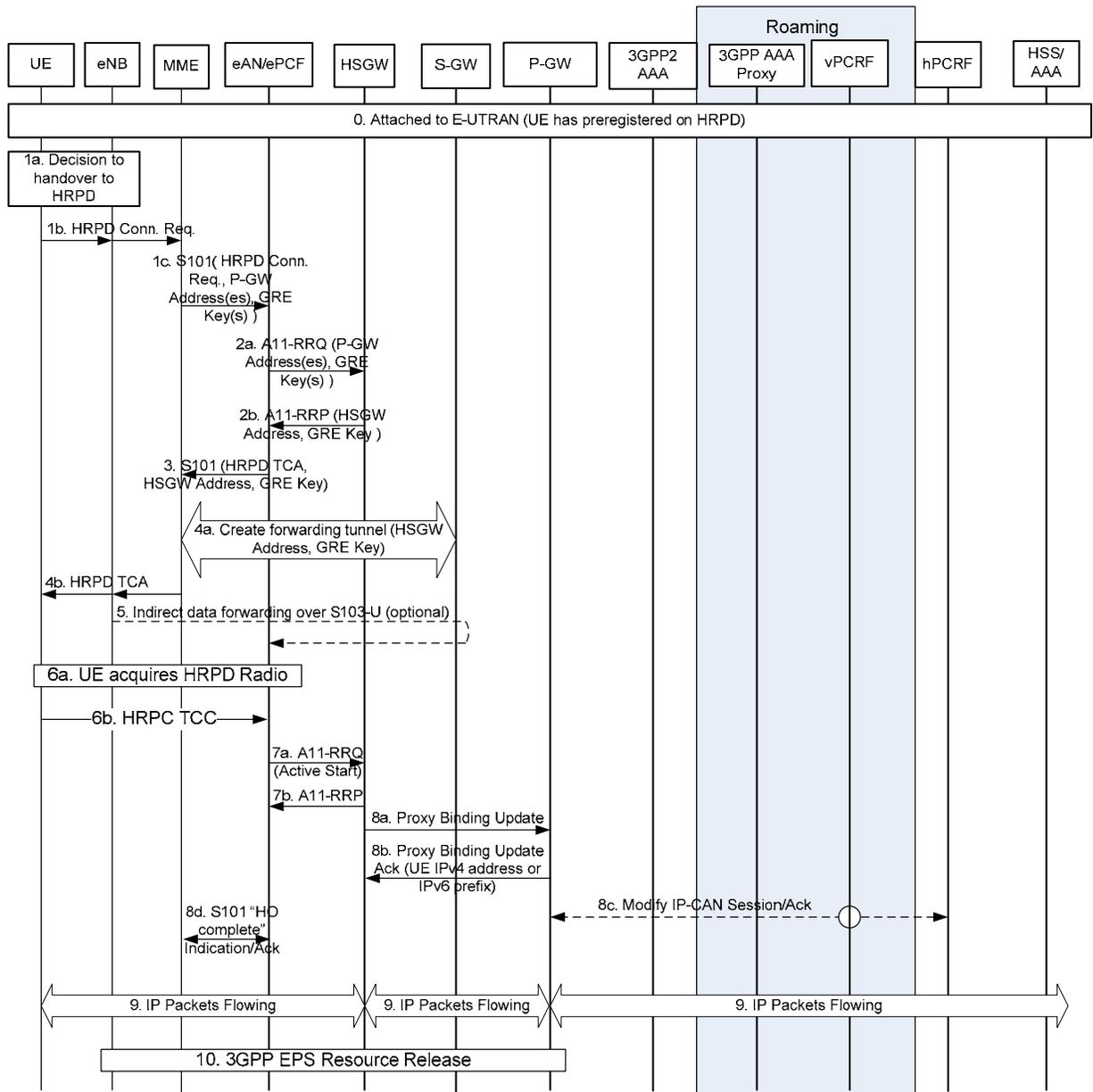


Figure 35 E-UTRAN to eHRPD Handover

1. a. E-UTRAN receives CDMA measurement reports from the UE and makes a HO decision.
- b. 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 A.S0022-0 [3] for details.
- c. 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 UL 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 UL data to the right UE, if the HSGW decides to send UL data even before the PBA is received in step 8b (note that the P-GW as defined in 23.402 is equipped to receive data with the same GRE key even before updating the binding).

2. a. The eHRPD eAN/ePCF allocates the requested radio resources and sends an A11-RRQ 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 now operating on the eHRPD radio.
- b. The HSGW responds with an A11-RRP containing a forwarding address (i.e., HSGW IP address and GRE key(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 and GRE key(s) for data forwarding.
4. a. The MME configures resources for indirect data forwarding and signals the HSGW IP address and GRE key(s) to the Serving GW. The Serving GW confirms data forwarding resources.
- b. 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 SGW to be sent to the HSGW over the S103 interface.
6. a. L2 attach is completed (i.e., the UE acquires the eHRPD radio).
- b. The UE sends a Traffic Channel Completion (TCC) message to the eHRPD eAN/ePCF.
7. a. The eHRPD eAN/ePCF sends an A11-RRQ carrying an Active Start airlink record and the indicator that the UE is now operating on the eHRPD radio to the HSGW.
- b. The HSGW responds to the eHRPD eAN/ePCF with an A11-RRP. If data forwarding via the S103 interface is supported, the HSGW includes an IP address and GRE key to receive forwarded data.
8. a. Triggered by step 7a (see section 6.2.1 for details), the HSGW/MAG sends a PBU(s) to establish a PMIPv6 tunnel(s) with the P-GW(s)/LMA(s) the UE is associated with.
- b. 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 to the HSGW/MAG, including the IP address(es)/prefix(es) allocated for the UE. The PMIPv6 tunnel is now setup.
- c. The P-GW/LMA 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.
- d. The eHRPD eAN/ePCF signals handover 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, SGW, and P-GW release resources. See A.S0022-0 [3], including sending a PMIPv6 BRI message from the P-GW to the S-GW as specified in 3GPP TS 29.275 [23]. See also TS 23.402 [15].

13.2 Idle Mode Handoff

13.2.1 Idle Mode Mobility from E-UTRAN to eHRPD (Same eAN/ePCF)

This procedure is used in the case the UE has a dormant PPP session in the target HSGW through the pre-registration procedure.

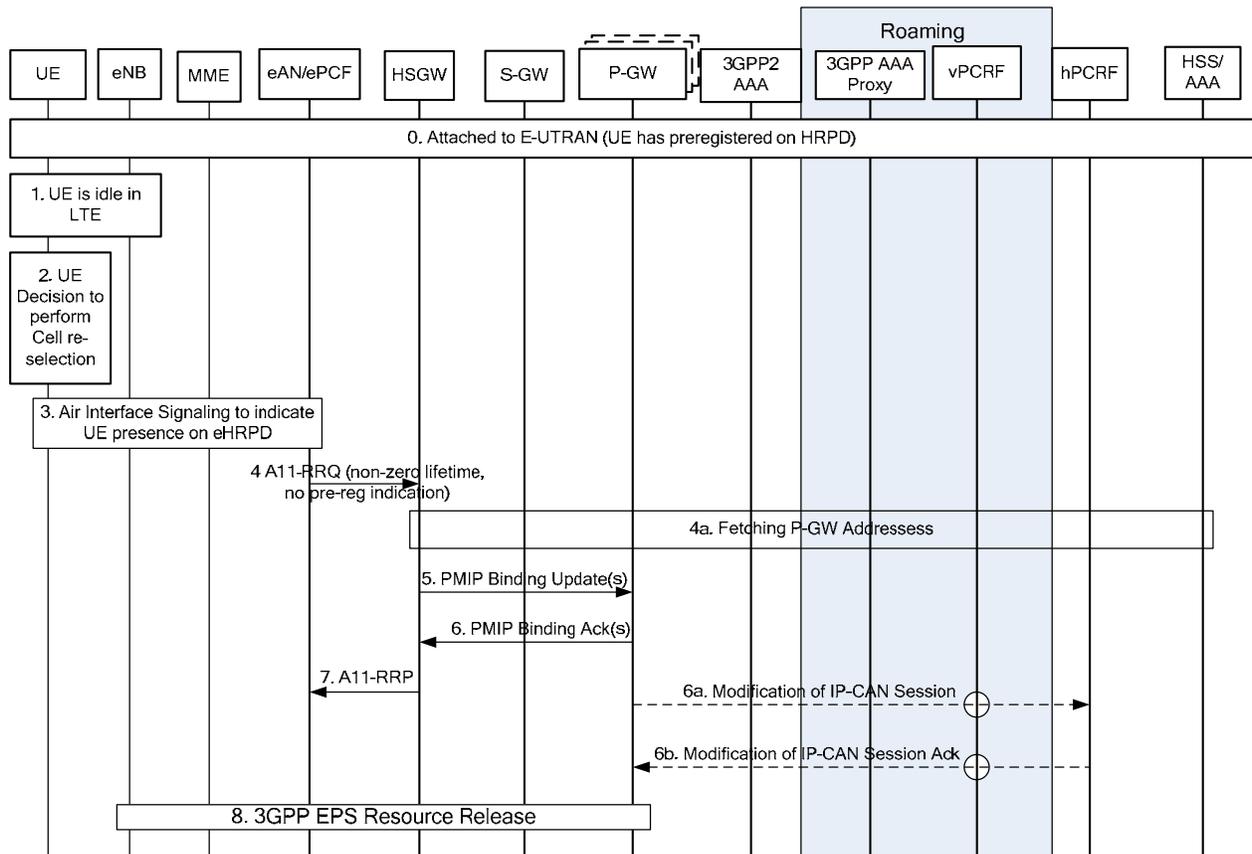


Figure 36 E-UTRAN to eHRPD mobility in idle mode (same eAN/ePCF)

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 AN, either through the pre-registration procedure or previous eHRPD attachment
2. The UE is in idle mode. Based on some trigger, the idle 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 (including as soon as the UE has completed pre-registration).
3. The UE follows 3GPP2 procedures to inform the eHRPD AN the UE has performed an inter-technology idle mode mobility event and is now tuned to eHRPD.

NOTE: If the UE has not created radio bearers and corresponding A10 connections, the eAN simply notes that the UE is present, and steps 4-8 will be skipped.

4. Since the eHRPD session is in this subnet, and since A10 connections already exist, the eHRPD eAN sends an A11-Registration Request for all A10s. This A11-RRQ contains the “tunnelled mode indicator” set to ‘0’ to indicate to the HSGW that the UE is operating on the eHRPD radio.

1 If the Tunnel Mode Indicator is not present, then the HSGW shall always assume that the UE is
2 operating on the eHRPD radio, and thus all PMIP bindings for the UE should be established.

3 4a. The HSGW fetches the P-GW identity for all the active PDN connections from the 3GPP AAA
4 Server

5
6 5~6. Upon receipt of the A11-Registration Request message for eHRPD session with nonzero lifetime
7 timer and the Tunnel Mode Indicator is set to '0' or is not present, the HSGW determines that it
8 does not have a PMIPv6 binding(s) for this UE and exchanges PBU/PBA messages with the
9 appropriate P-GW(s). The UE address information in PMIPv6 BA returns the IP Address assigned
10 to the UE. At this point the user plane is switched in the P-GW towards the eHRPD access
11 network via the HSGW.

12
13 6a-6b. The P-GW sends an Indication of IP-CAN Session Modification message to the PCRF and
14 PCRF acknowledges. Since steps 6 and 6a are both triggered by the PBU in step 5, steps 6 and 6a
15 may occur in parallel.

16 NOTE: For multiple PDN connections, steps 5-6 and 6a-6b are performed for each PDN connection.

17
18 7. The HSGW sends A11-Registration Reply to acknowledge the eHRPD access. The A11-
19 Registration Request message is validated and, if new A10 connections are being established, the
20 HSGW accepts the A10 connections by returning an A11-Registration Reply message with an
21 accept indication. This step may occur any time after step 4.

22
23 8. At any time after step 6, the P-GW shall initiate resource allocation deactivation procedure in
24 E-UTRAN as defined in TS 23.402 subclause 5.6.2.2 [15].

25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

13.2.2 Idle Mode Mobility from E-UTRAN to eHRPD (Different eAN/ePCF)

This procedure is used in the case the UE has a dormant eHRPD session in a different eHRPD eAN, either through the pre-registration procedure or previous eHRPD attachment.

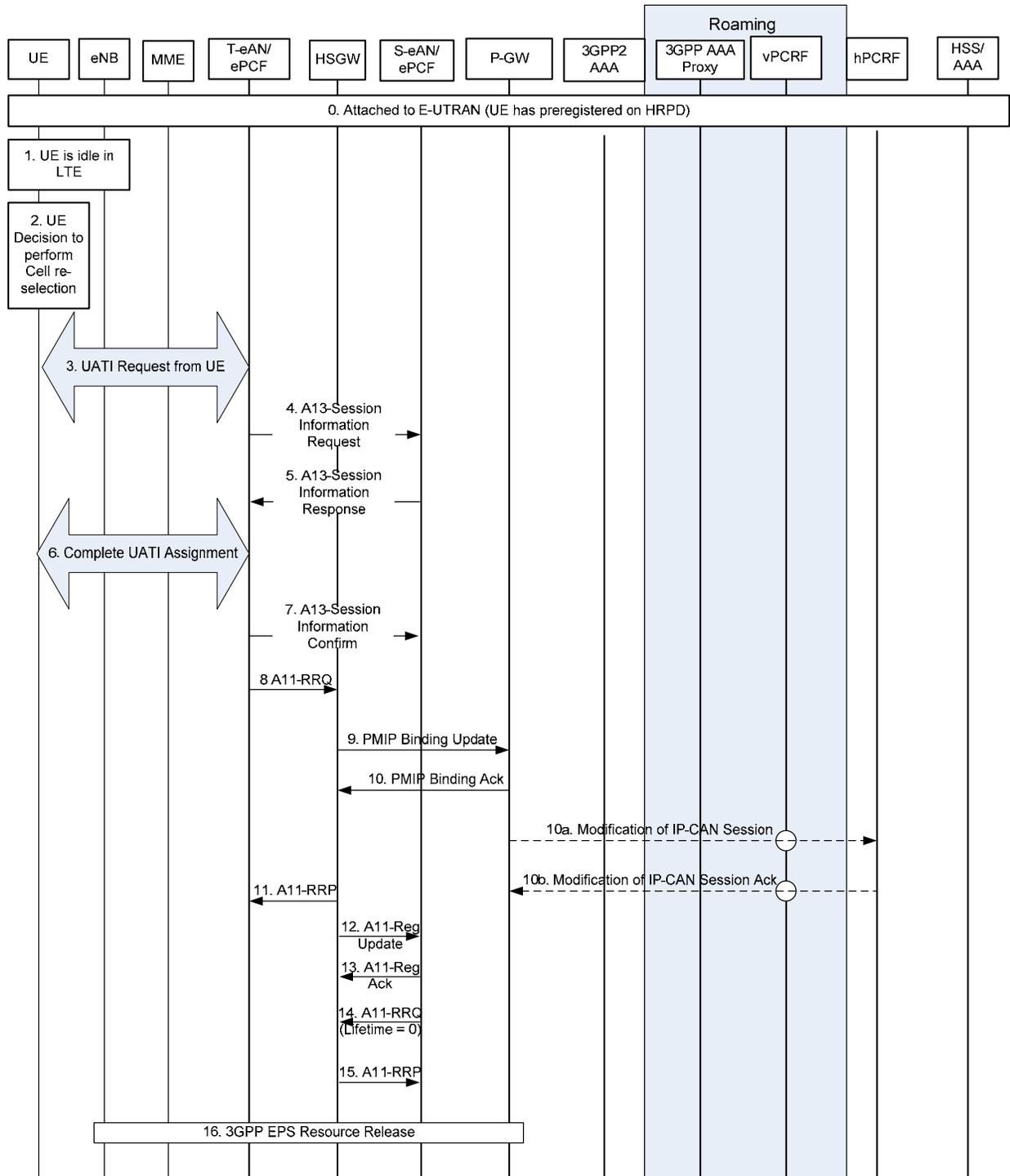


Figure 37 E-UTRAN to eHRPD mobility in idle mode (different eAN/ePCF)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

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 source eHRPD AN, either through the pre-registration procedure or previous eHRPD attachment.
 2. The UE is in idle mode. Based on some trigger, the idle 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 (including as soon as the UE has completed pre-registration).
 3. The UE and target eAN initiate UATI assignment in the new eAN/ePCF.
 4. The target eAN/ePCF sends an A13-Session Information Request to the source eAN/ePCF to retrieve the context of the session.
 5. The source eAN/ePCF sends an A13-Session Information Response to the target eAN/ePCF to provide the context of the session.
 6. The UE and target eAN complete UATI assignment.
 7. The target eAN/ePCF informs the source eAN/ePCF that it now has control of the UE via an A13-Session Information Confirm message.
 8. Since the eHRPD session was not previously in this subnet, the A10 connections must be created to the target eAN/ePCF. The target eAN/ePCF sends an A11-Registration Request with a non-zero lifetime and Tunnel Mode Indicator set to '0' or without a Tunnel Mode Indicator to cause the HSGW to move all A10s. This A11-RRQ contains the Tunnel Mode Indicator set to '0' to indicate to the HSGW that the UE is operating on the eHRPD radio, and thus all PMIP bindings for the UE should be established. 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.
 - 9-10. Upon receipt of the A11-Registration Request message for eHRPD session with nonzero lifetime timer and Tunnel Mode Indicator set to '0' or the Tunnel Mode Indicator is not present, the HSGW determines as specified in Section 6.2.1 that it does not have a PMIPv6 binding(s) for this UE and exchanges PBU/PBA messages with the P-GW(s) (P-GW address received from the 3GPP AAA Server). The 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.
 - 10a-10b. The P-GW sends an Indication of IP-CAN Session Modification message to the PCRF and PCRF acknowledges. Steps 10 and 10a may occur in parallel.
- NOTE: For multiple PDN connections, steps 9-10 and 10a-10b are performed for each PDN connection.
11. The HSGW sends A11-Registration Reply with an accept indication. This step may occur any time after step 8.
 12. The HSGW sends an A11-Registration Update to initiate closure of the A10s for the UE with the source eAN/ePCF.
 13. The source eAN/ePCF acknowledges by sending an A11-Registration Ack.
 14. The source eAN/ePCF sends an A11-Registration Request with lifetime=0 for all A10s.
 15. The HSGW send an A11-Registration Reply to acknowledge the removal of the A10s by the source eAN/ePCF.
 16. At any time after step 10, the P-GW shall initiate resource allocation deactivation procedure in E-UTRAN as defined in TS 23.402 subclause 5.4.5.2 [15].

14 Non-Optimized Active Handoff and Idle Mode Mobility

This section includes procedures for non-optimized handoff. That is, S101 tunneling is not used to perform the handoff into or from eHRPD.

14.1 Non-Optimized Active Handoff or Idle Mode Mobility from E-UTRAN to eHRPD using PMIPv6 based S5 and S2a

The steps involved in the handover from E-UTRAN to eHRPD system are depicted below for the case of non-roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 tunnel is established between the S-GW and the P-GW in the evolved packet core. The call flow is based on the non-optimized handoff procedures for E-UTRAN to non-3GPP access described in TS 23.402 Clause 8.2.2 [15]. At the beginning of this call flow, the UE may be active or idle. This call flow assumes that the UE does not have a previously established PPP session.

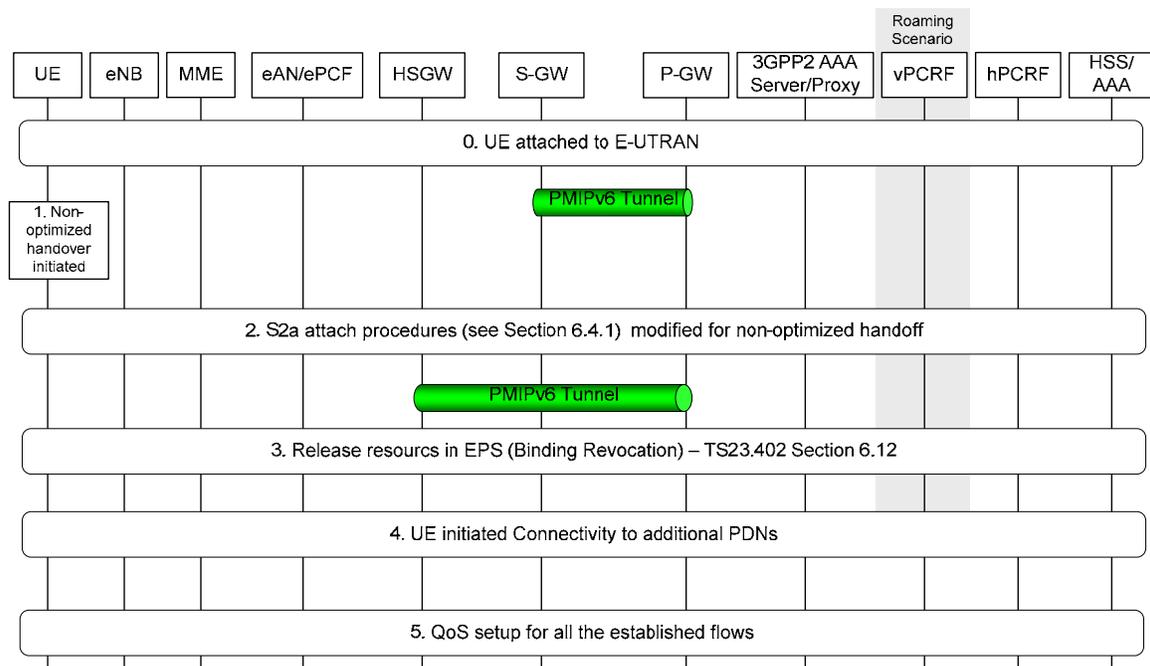


Figure 38 E-UTRAN to eHRPD non-optimized handoff between PMIPv6 S5 and S2a

0. The UE is attached to E-UTRAN.
1. The UE is attached to the 3GPP Access and has a PMIPv6 tunnel on the S5 interface. Non-optimized handover procedures are triggered. The UE tunes to HRPD radio.
2. The UE and the eHRPD network perform the steps for eHRPD session establishment and default PDN bearer establishment. These steps are described in Section 6.4.1. If eHRPD session is previously established between UE and eAN/ePCF, then steps 1 to 4 of Section 6.4.1 are omitted. The following changes are required to the flow in Section 6.4.1:

- 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10
 - 11
 - 12
 - 13
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 22
 - 23
 - 24
 - 25
 - 26
 - 27
 - 28
 - 29
 - 30
 - 31
 - 32
 - 33
 - 34
 - 35
 - 36
 - 37
 - 38
 - 39
 - 40
 - 41
 - 42
 - 43
 - 44
 - 45
 - 46
 - 47
 - 48
 - 49
 - 50
 - 51
 - 52
 - 53
 - 54
 - 55
 - 56
 - 57
 - 58
 - 59
 - 60
- i. Step 8, 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.
 - ii. Step 11, the P-GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [13]. The Event Report indicates the change in Access Type.
3. Resources are released in EPS as per TS23.402, clause 6.12 [15].
 4. If required, the UE may connect to additional PDNs.
 5. If the *Selected Bearer Control Mode* is set to 'MS/NW mode', then the network initiates QoS update procedures based on the QoS policy received from the PCRF. Otherwise, the UE performs the UE initiated QoS update procedures to setup UE initiated QoS.

14.2 Non-Optimized Mobility from eHRPD to E-UTRAN using PMIPv6 based S5 and S2a

For non-optimized mobility from eHRPD to E-UTRAN, the procedures are defined in 23.402, Section 8.2.1. This interaction is invisible to eHRPD, with the exception of the procedures associated with the release of eHRPD resources, as defined in 23.402 Section 6.12 [15].

These release procedures are as follows:

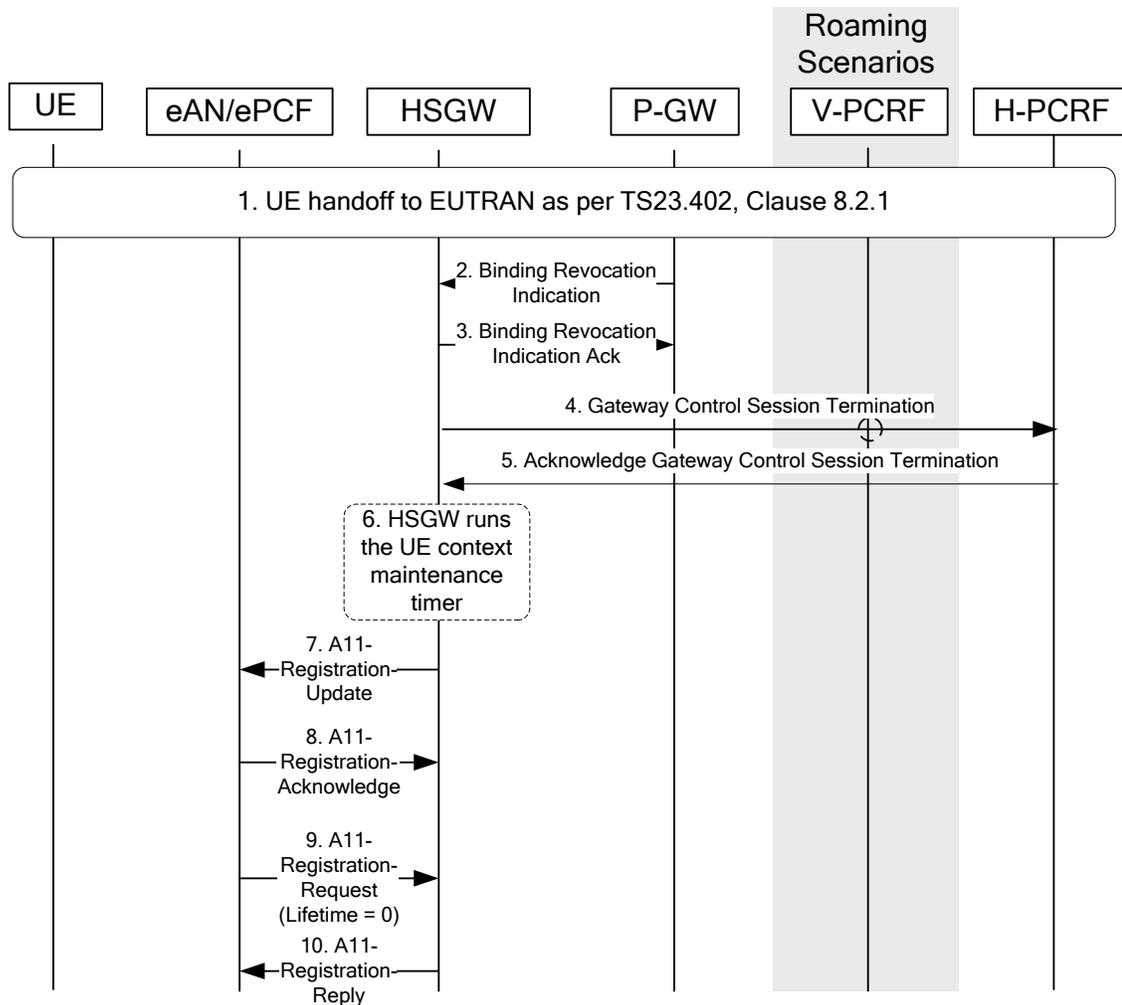


Figure 39 eHRPD to E-UTRAN non-optimized handover between PMIPv6 S2a and S5 (Resource Release)

1. The UE handoff to E-UTRAN as per TS23.402, Clause 8.2.1 [15].
2. The P-GW sends a Binding Revocation Indication message to the trusted non-3GPP IP access as defined in draft-ietf-mext-binding-revocation-00 [53].
3. The HSGW returns a Binding Revocation Indication Acknowledgement message to the P-GW. This message can be sent any time after step 2.

- 1 4. The HSGW initiates the Gateway Control Session Termination Procedure with the PCRF as
2 specified in TS 23.203 [13].
- 3 5. The PCRF responds to the HSGW with Acknowledge Gateway Control Session Termination
4 message.
- 5 6. The HSGW may start the UE Context Maintenance timer and follow the procedure of section
6 6.2.3 and 10.1.7.
- 7 7. Upon expiry of the UE Context Maintenance timer, if it is started, the HSGW sends an A11-
8 Registration Update message to initiate with the ePCF the release of the A10 session for the
9 UE.
- 10 8. The ePCF responds with an A11-Registration Acknowledge message.
- 11 9. The eAN/ePCF sends an A11-Registration Request with the lifetime value set to zero to
12 release the A10 session.
- 13 10. The HSGW responds with A11-Registration Reply with lifetime zero.
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

15 Annex A (Informative) – Mapping QoS between 3GPP and 3GPP2

In section 5.6.6, 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 EPC 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 9 standard QCIs (see TS 23.203 [13]). 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 [7]). 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 1). 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).

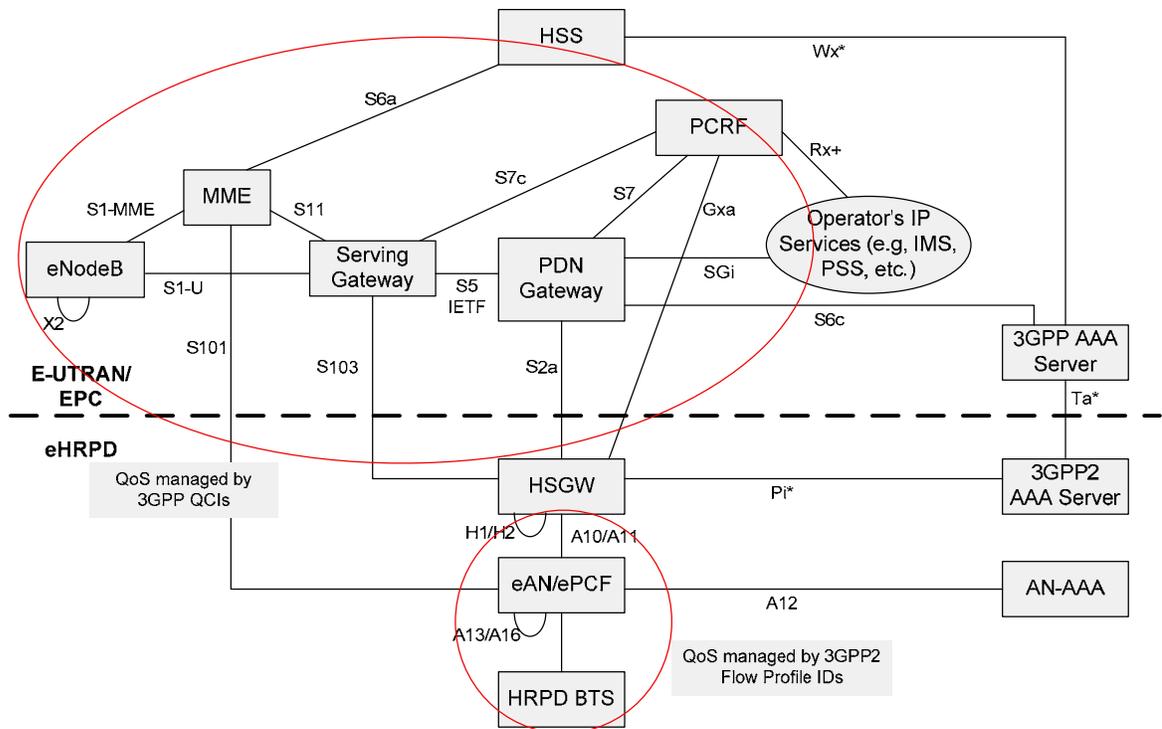


Figure 40 Flow ID and QCI Applicability

When mapping from 3GPP to 3GPP2, a twofold mapping strategy is recommended:

1. Associate 3GPP QCIs to 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 34.

Table 34 Example of QoS Mapping

QCI	Resource Type (bit rate included if GBR)	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services	eHRPD Flow-ProfileID	eHRPD Flow Description
1	GBR (32.8 kbps ¹)	2	100 ms	10 ⁻²	Conversational Voice	0x0100	Conversational Rate Set 1 Speech
1	GBR (32.8 kbps ²)	2	100 ms	10 ⁻²	PTT Voice	0x0118	PTT Rate set 1 Speech (maximum of 6 frames bundled)
1	GBR (37.6 kbps ¹)	2	100 ms	10 ⁻²	Conversational Voice	0x0101	Conversational Rate Set 2 Speech
2	GBR (24 kbps)	4	150 ms	10 ⁻³	Conversational Video (Live Streaming)	0x0300	Conversational Video Streaming

QCI	Resource Type (bit rate included if GBR)	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services	eHRPD Flow-ProfileID	eHRPD Flow Description
2	GBR (32 kbps)	4	150 ms	10^{-3}	Conversational Video (Live Streaming)	0x0301	Conversational Video Streaming
2	GBR (40 kbps)	4	150 ms	10^{-3}	Conversational Video (Live Streaming)	0x0302	Conversational Video Streaming
2	GBR (48 kbps)	4	150 ms	10^{-3}	Conversational Video (Live Streaming)	0x0303	Conversational Video Streaming
2	GBR (64 kbps)	4	150 ms	10^{-3}	Conversational Video (Live Streaming)	0x0305	Conversational Video Streaming
3 ³	GBR	3	50 ms	10^{-3}	Real Time Gaming	0x0005	Real Time Gaming
4	GBR (24 kbps)	5	300 ms	10^{-6}	Non- Conversational Video (Buffered Streaming)	0x030c	Video Streaming
4	GBR (64 kbps)	5	300 ms	10^{-6}	Non- Conversational Video (Buffered Streaming)	0x030e	Video Streaming
4	GBR (128 kbps)	5	300 ms	10^{-6}	Non- Conversational Video (Buffered Streaming)	0x0311	Video Streaming
5	Non-GBR	1	100 ms	10^{-6}	PTT Control Signaling	0x0503	Real Time Control Signaling
5	Non-GBR	1	100 ms	10^{-6}	IMS Signaling	0x0500	Conversational Control Signaling

QCI	Resource Type (bit rate included if GBR)	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services	eHRPD Flow-ProfileID	eHRPD Flow Description
6	Non-GBR	6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)	0x0000	Best effort
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming	0x0600	Interactive Gaming
8		8	300 ms	10^{-6}	TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)	0x0000	Best effort
9		9				0x0000	Best effort

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,

16 Annex B (Informative) – Mapping Gxa Parameters between 3GPP and 3GPP2

The non-3GPP information received across the Gxa interface is illustrated in the table along with an indication if it is required and how it is used in eHRPD.

Table 35 Mapping Gxa Parameters between 3GPP and 3GPP2

Attribute Name	Reference (29.212 Clause)	Description	Access type	eHRPD Mapping	Need on Gxa for eHRPD access
3GPP-SGSN-Address	3GPP TS 29.061 [11]	For GPRS the IPv4 address of the SGSN	3GPP-GPRS	No mapping required.	No
3GPP-SGSN-IPv6-Address	3GPP TS 29.061 [11]	For GPRS the IPv6 address of the SGSN	3GPP-GPRS	No mapping required.	No
3GPP-User-Location-Info	3GPP TS 29.061 [11]	Indicates details of where the UE is currently located (e.g., SAI or CGI)	3GPP	No mapping required.	No
Allocation-and-Retention-Priority	5.3.32	Indicates a priority for accepting or rejecting a bearer establishment or modification request and dropping a bearer in case of resource limitations.	All	No mapping required.	Yes
Bearer-Control-Mode	5.3.23	Indicates the PCRF selected bearer control mode.	All	No mapping required.	Yes
Called-Station-ID	IETF RFC 4005 [12]	The address the user is connected to (i.e., the PDN identifier).	All	No mapping required.	Yes
CC-Request-Number	IETF RFC 4006 [9]	The number of the request for mapping requests and answers	All	No mapping required.	Yes
CC-Request-Type	IETF RFC 4006 [9]	The type of the request (initial, update, termination)	All	No mapping required.	Yes
Event-Trigger	5.3.7	Reports the event that occurred on the BBERF.	All	No mapping required.	Yes
Flow-Description	3GPP TS 29.214 [10]	Defines the service flow filter parameters for a QoS rule	All	The HSGW maps the 'flow-description' to the packet filter field in the TFT.	Yes
Framed-IP-Address	IETF RFC 4005 [12]	The IPv4 address allocated for the user.	All	No mapping required.	Yes
Framed-IPv6-Prefix	IETF RFC 4005 [12]	The IPv6 address prefix allocated for the user.	All	No mapping required.	Yes
Guaranteed-Bit Rate-DL (note 1)	5.3.25	Defines the guaranteed bit rate for downlink.	All	HSGW uses this in the selection of appropriate FlowProfileID	Yes
Guaranteed-Bit Rate-UL (note 1)	5.3.26	Defines the guaranteed bit rate for uplink.	All	HSGW uses this in the selection of appropriate FlowProfileID	Yes
IP-CAN-Type	5.3.27	Indicates the type of Connectivity Access Network that the user is connected to.	All	HSGW sets this value to 3GPP2 (4)	Yes

Attribute Name	Reference (29.212 Clause)	Description	Access type	eHRPD Mapping	Need on Gxa for eHRPD access
Max-Requested-Bandwidth-DL (note 2)	3GPP TS 29.214 [10]	Defines the maximum authorized bandwidth for downlink.	All	HSGW uses this in the selection of appropriate FlowProfileID	yes
Network-Request-Support	5.3.24	Indicates whether the access network supports the network requested bearer control mode or not.	All	No mapping required.	Yes
Precedence	5.3.11	Indicates the precedence of QoS rules or packet filters.	All	HSGW maps this to the TFT evaluation precedence value.	Yes
PCC-Rule-Status	5.3.19	Describes the status of one or a group of QoS rules.	All	No mapping required.	Yes
QoS-Class-Identifier	5.3.17	Identifies a set of IP-CAN specific QoS parameters	All	See Annex A.	Yes
QoS-Information	5.3.16	Defines the QoS information for a resource, QoS rule or QCI	All	HSGW shall use the values in this AVP to determine the appropriate FlowProfileID. See Annex A.	Yes
RAI	3GPP TS 29.061 [11]	Contains the Routing Area Identity of the SGSN where the UE is registered	3GPP-GPRS	No mapping required.	No
RAT-Type	5.3.31	Identifies the radio access technology that is serving the UE.	All	The HSGW sets this AVP to '2001' to indicate HRPD access RAT.	Yes
Subscription-Id	IETF RFC 4006 [9]	The identification of the subscription (i.e., IMSI)	All	HSGW uses the IMSI obtained from A11 messaging to map to this AVP	Yes
TFT-Filter	5.3.13	See 29.212	All	HSGW maps the TFT filter information from Gxa to the TFT filter sent using RSVP signaling to/from UE.	Yes
TFT-Packet-Filter-Information	5.3.14	See 29.212	All	No mapping required.	No
ToS-Traffic-Class	5.3.15	See 29.212	All	HSGW may include this in the TFT sent to or received from the UE.	Yes.
Tunnel-Header-Filter	5.3.34	Defines the tunnel (outer) header filter information of a tunnelled IP flow.	Non-3GPP	No mapping required.	Yes.
Tunnel-Header-Length	5.3.35	Indicates the length of the tunnel (outer) header.	Non-3GPP	No mapping required.	Yes
Tunnel-Information	5.3.36	Defines the tunnel (outer) header information for an IP flow.	Non-3GPP	No mapping required.	Yes
User-Equipment-Info	IETF RFC 4006 [9]	The identification and capabilities of the terminal (IMEISV, etc.)	All	HSGW sets this to indicate that	Yes

Attribute Name	Reference (29.212 Clause)	Description	Access type	eHRPD Mapping	Need on Gxa for eHRPD access
		When the User-Equipment-Info-Type is set to IMEISV(0), the value within the User-Equipment-Info-Value is a UTF-8 encoded decimal.		the UE provides an IMSI MN-ID.	

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.

17 Annex C (Informative) – Mapping STa Parameters between 3GPP and 3GPP2

Table 36 Mapping STa Parameters between 3GPP and 3GPP2

STa : Diameter AVP	A11 : RADIUS VSA	Remarks	Sent to eAN	Direction
3GPP2-Max-Per-Flow-Priority-For-User	Maximum Per Flow Priority for the User	Indicates the maximum priority that may be assigned to a user's packet flow.	Yes	AAA → HSGW
3GPP2 Information	Authorized FlowProfileID(s) for the User	The values in Auth-profile-Id-Forward, Auth-profile-Id-Reverse, and Auth-profile-Id- Bi-Direction in the grouped AVP 3GPP2 Information are extracted by HSGW and put into the respective sub-types of the VSA Authorized Flow Profile IDs for the User.	Yes	AAA → HSGW
3GPP2-Inter-User-Priority	Inter-User Priority		Yes	AAA → HSGW
AMBR	Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic	This is supposed to be the UE-AMBR from HSS subscription profile.	Yes	AAA → HSGW
Subscriber-Priority	Service Option Profile	The values in 3GPP2-Max-Inst-Per-Service-Option, 3GPP2-Max-Svc-Inst-Link-Flow-Total AVPs from grouped AVP Subscriber-Priority is extracted by HSGW and put into the respective values/sub-types in Service Option Profile VSA.	Yes	AAA → HSGW
Subscriber-Priority	Allowed Persistent TFTs	The value in 3GPP2-Allowed-Persistent-TFTs AVP in the grouped AVP Subscriber-Priority is extracted and used by the HSGW.	No	