ETSI TS 123 139 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP system - fixed broadband access network interworking;
Stage 2
(3GPP TS 23.139 version 19.0.0 Release 19)**

Reference
RTS/TSGS-0223139vj00

Keywords
GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This document specifies the Stage 2 system description for the interworking between a 3GPP system and a Fixed Broadband Access network defined by Broadband Forum to provide the IP connectivity to a 3GPP UE using a WLAN and a H(e)NB connected to a Fixed Broadband Access network.

The specification covers the system description mobility, Policy, QoS aspects between 3GPP and a Fixed Broadband Access network as well as the respective interactions with the PCC frameworks. This document specifies the detailed extension to EPC defined in TS 23.401 [2] and TS 23 402 [3] for supporting Fixed Broadband Access Network. The extension to PCC framework are specified in TS 23.203 [4].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.401: "GPRS Enhancements for E-UTRAN Access".

[3] 3GPP TS 23 402: "Architecture enhancements for Non-3GPP Accesses".

[4] 3GPP TS 23.203: "Policy and charging control architecture".

[5] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[6] Broadband Forum TR-203: "Interworking between Next Generation Fixed and 3GPP Wireless Access", August 2012.

[7] Broadband Forum TR-058: " Multi-service Architecture and Framework Requirements " September 2003.

[8] Broadband Forum TR-101: "Migration to Ethernet-based DSL Aggregation" April 2006.

[9] 3GPP TS 23.261: "IP Flow Mobility and seamless WLAN offload ".

[10] Broadband Forum TR-145: "Multi-service Broadband Network Functional Modules and Architecture", November 2012.

[11] Broadband Forum TR-134 Corrigendum 1: "Broadband Policy Control Framework (BPCF)", January 2013.

[12] 3GPP TS 25.467: "UTRAN architecture for 3G Home Node B (HNB); Stage 2".

[13] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[14] 3GPP TS 22.220: "Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".

[15] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[16] 3GPP TS 33.210: "Network Domain Security; IP network layer security".

[17] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[18] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[19] 3GPP TS 29.274: "General Packet Radio Service (GPRS); Evolved GPRS Tunnelling Protocol (eGTP) for EPS".

[20] Broadband Forum TR-092: "Broadband Remote Access Server (BRAS) Requirements", August 2004.

[21] Broadband Forum TR-124 Issue 2: "Functional Requirements for Broadband RG Devices".

[22] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[23] 3GPP TS 33.402: "Security aspects of non-3GPP accesses".

[24] 3GPP TS 23.003: "Numbering, addressing and identification".

[25] 3GPP TS 29.273: "3GPP EPS AAA interfaces".

[26] Broadband Forum TR-059: "Architecture Requirements for the Support of QoS-Enabled IP Service", September 2003.

[27] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[28] 3GPP TS 25.413: "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling.".

[29] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[30] Broadband Forum TR-291: "Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access", March 2014.

[31] IETF RFC 4186 (January 2006): "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3GPP Femto: Refers to the HNB and HeNB NEs as defined by 3GPP. The HNB GW is always required for the HNB architecture while the HeNB GW is option for the HeNB.

UE local IP address is defined as: either the public IP address assigned to the UE connected to a BBF access network via a WLAN by the BBF domain in the no-NAT case, or the public IP address assigned by the BBF domain to the NATed RG that is used for this UE.

H(e)NB local IP address is defined as: either the public IP address assigned to the H(e)NB by the BBF domain in the no-NAT case, or the public IP address assigned by the BBF domain to the NATed RG that is used for this H(e)NB.

Non-seamless WLAN offload (NSWO) is a capability of a UE supporting routing specific IP flows over the WLAN access without traversing the EPC as defined in TS 23 402 [3], clause 4.1.5.

EPC-routed: User plane traffic that is routed via a PDN GW in EPC as part of a PDN Connection. EPC-routed applies to non-roaming, roaming with traffic home-routed and roaming with traffic local break-out cases.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ANDSF	Access Network Discovery and Selection Function
AF	Application Function
BBF	Broadband Forum
BRAS	Broadband Remote Access Server
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
DSCP	Differentiated Services (Diffserv) Code Point
DSMIPv6	Dual-Stack MIPv6
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
H-ANDSF	Home-ANDSF
MME	Mobility Management Entity
NSWO	Non-seamless WLAN offload
PCRF	Policy and Charging Rules Function
P-GW	PDN Gateway
PMIP/PMIPv6	Proxy Mobile IP version 6
RG	Residential Gateway
SeGW	Security Gateway
S-GW	Serving GW
TDF	Traffic Detection Function
V-ANDSF	Visited-ANDSF

4 Architecture model and requirements

4.1 Architectural requirements and assumptions

The interworking architecture is based on EPC reference architecture defined in TS 23.401 [2] and TS 23 402 [3] and on BBF access network defined by BBF TR-291 [30], BBF TR-058 [7], BBF TR-101 [8], BBF TR-134 [11], and BBF TR-203 [6] excluding EAP-SIM (RFC 4186 [31]) functionality.

The interworking architecture supports trusted and untrusted model for the host-based mobility (S2c) and the untrusted model for the network based mobility (S2b). The trusted/untrusted Non-3GPP access network detection is performed as defined in clause 4.1.4 of TS 23 402 [3].

The reference architecture defined in TS 23 402 Rel-11 clause 16 for Trusted WLAN using GTP s2a is applicable to the scenario where the Fixed Broadband / BBF Access network is considered as a trusted WLAN access. For such Fixed Broadband / BBF Access interworking deployments, in this version of the specification, the interactions between the EPC and the Fixed Broadband / BBF Access network consists only in S2a, STa interfaces and are not further detailed in this document. The detailed functional split within a Fixed Broadband / BBF Access network, the support of P2P link between the UE and the TWAG and the mapping between the S2a bearer QoS information received via S2a and Fixed Broadband Access specific parameters are outside 3GPP scope.

The architecture supports a UE simultaneously connected to the EPC via more than one access network for the same PDN connection as defined in TS 23.261 [9].

The architecture supports a UE that is capable of routing simultaneously active PDN connections to different APNs through different access networks as defined in TS 23.401 [2] and TS 23 402 [3].

The architecture supports the scenario of a single network operator deploying both the 3GPP EPC and the BBF access network and the scenario of two network operators one deploying the 3GPP EPC network and one deploying only the Broadband Forum Access network. Furthermore the architecture supports the roaming scenario between two PLMN operators.

The architecture supports local breakout of traffic in the EPC network whether a roaming subscriber is accessing the EPC via a 3GPP or a non-3GPP access network according to the design principles described in clause 4.1 of TS 23.401 [2].

The support of HeNB is based on reference architecture defined in TS 23.401 [2] and TS 36.300 [13], for the support of HNB in TS 23.060 [22] and TS 25.467 [12].

The architecture supports both offline and online charging in the 3GPP domain for the EPC routed traffic by means of accounting/charging information collected in 3GPP network elements.

The architecture supports STa/SWa reference points based accounting for the 3GPP UEs when traffic is NSWO in the Fixed Broadband Access network based on the assumption that the BBF network is able to collect per user accounting data for NSWO traffic of 3GPP UEs (i.e. BNG is able to recognize the traffic of individual 3GPP UEs), and periodically report this data via the STa/SWa reference points. If both EPC routed and NSWO are simultaneously provided to a UE, accounting information sent by BBF over SWa/STa shall allow distinguishing the accounting information for EPC routed traffic from that for NSWO traffic. This shall be supported based on Fixed Broadband Access accounting capabilities

NOTE 1: As defined in BBF TR-203 [6] the Fixed Aroadband Access may sent over SWa/STa accounting information for both EPC routed and NSWO.

NOTE 2: The online charging may be supported with limitation due to support of AAA RADIUS based accounting in the BBF network. It is assumed that the BBF does not need to be aware of whether online or offline charging is performed in the 3GPP domain

For S2b, the PCRF discovery function may select different PCRFs for PDN connection(s) for the UE in the PDN GW and for the IP session for NSWO traffic for the UE in the Fixed Broadband Access.

For S2c, the PCRF discovery function selects the same PCRF for all PDN connections for a certain IMSI and may select a different PCRF for IP-CAN session establishment over S9a for NSWO traffic.

There may be multiple TDFs deployed. If a TDF is used for traffic offloaded to the Fixed Broadband Access, the TDF selected for the NSWO traffic from the UE in the Fixed Broadband Access and that for the EPC routed traffic on SGi may or may not be the same.

In this Release, the policy interworking for user charging for NSWO traffic is only supported for scenarios without NAT in the Fixed Broadband Access domain.

4.2 Architecture for Fixed Broadband Access network interworking using WLAN access

4.2.1 General

The figure 4.2.2-1, 4.2.2-2 and 4.2.2-3 show the reference architecture for the non-roaming scenario and with the traffic routed to the mobile core network. The figure 4.2.3-1, 4.2.3-2 and 4.2.3-3 show the reference architecture for the roaming scenario with the traffic routed to the home network. The figure 4.2.3-5, 4.2.3-6 and 4.2.3-7 show the reference architecture for the roaming scenario with the local breakout in Visited PLMN.

The figure 4.2.4-1and 4.2.4-2 show the reference architecture for the NSWO with AF in 3GPP operator's network; the figure 4.2.4-3 and 4.2.4-4 show the reference architecture for the NSWO with AF ("BBF AF") in BBF domain; the figure 4.2.4-5 and 4.2.4-6 show the reference architecture for NSWO with TDF. The non-seamless traffic is routed to an external network directly from BBF network.

The following considerations apply to interfaces and reference points where they occur in figures in this clause:

- S5 and S8 can be GTP-based or PMIP-based.
- Gxc is used only in the case of PMIP variant of S5 or S8.
- S9 is used between the H-PCRF and V-PCRF in roaming scenario
- the reference points internal to the Fixed Broadband access network are defined or are under definition by Broadband Forum and are out of the scope of this specification.

NOTE 1: SWu shown in Figure 4.2.2-1, 4.2.3-1 and 4.2.3-4 also applies to architectural reference for untrusted scenario in Figures 4.2.2-3, 4.2.3-3 and 4.2.3-6 for the untrusted scenario with S2c but is not shown for simplicity.

The ANDSF is not shown in any of the following figures, but it may be used in all architectural variants, according to the principles defined in TS 23 402 [3].

4.2.2 Non-roaming architecture for EPC-routed traffic

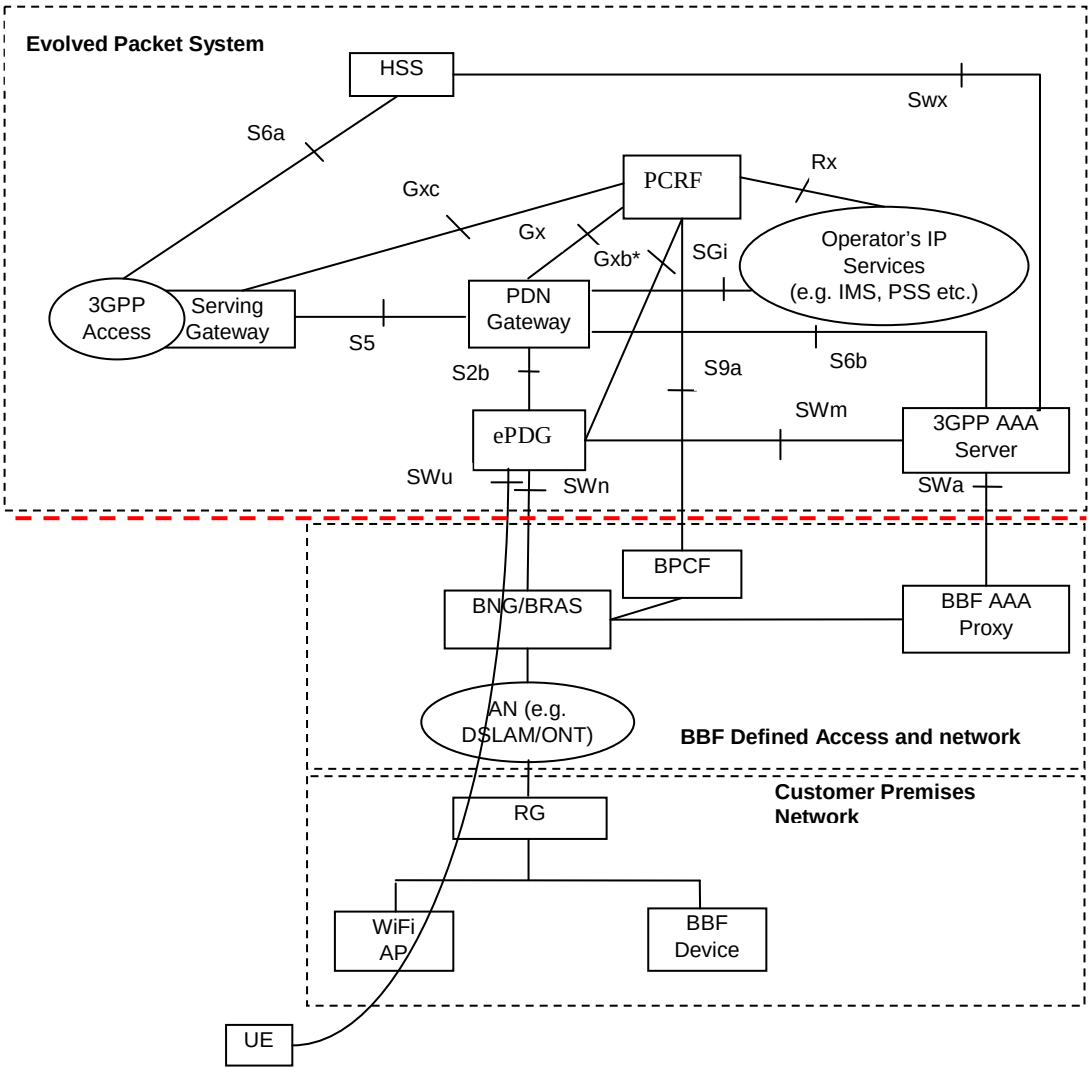

Figure 4.2.2-1: Non-Roaming Architecture for untrusted Fixed Broadband access network based on S2b

NOTE 1: The reference architecture is applicable when the 3GPP and Fixed Broadband access networks belongs to the same network operator or to different network operators.

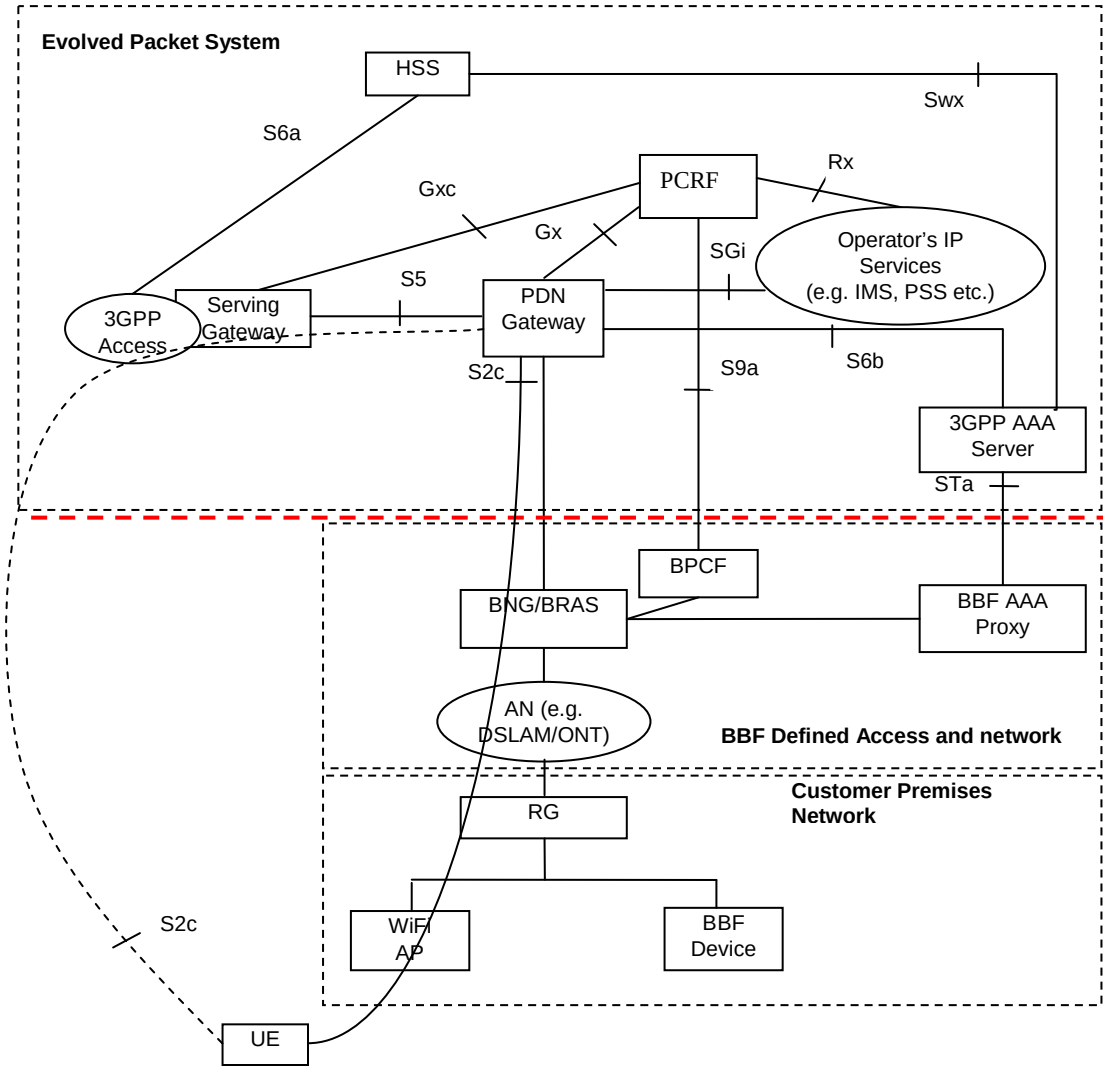

Figure 4.2.2-2: Non-Roaming Architecture for trusted Fixed Broadband access network based on S2c

NOTE 2: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same network operator or to different network operators.

NOTE 3: The connection between the BRAS/BNG and PDN Gateway is IP transport connection.

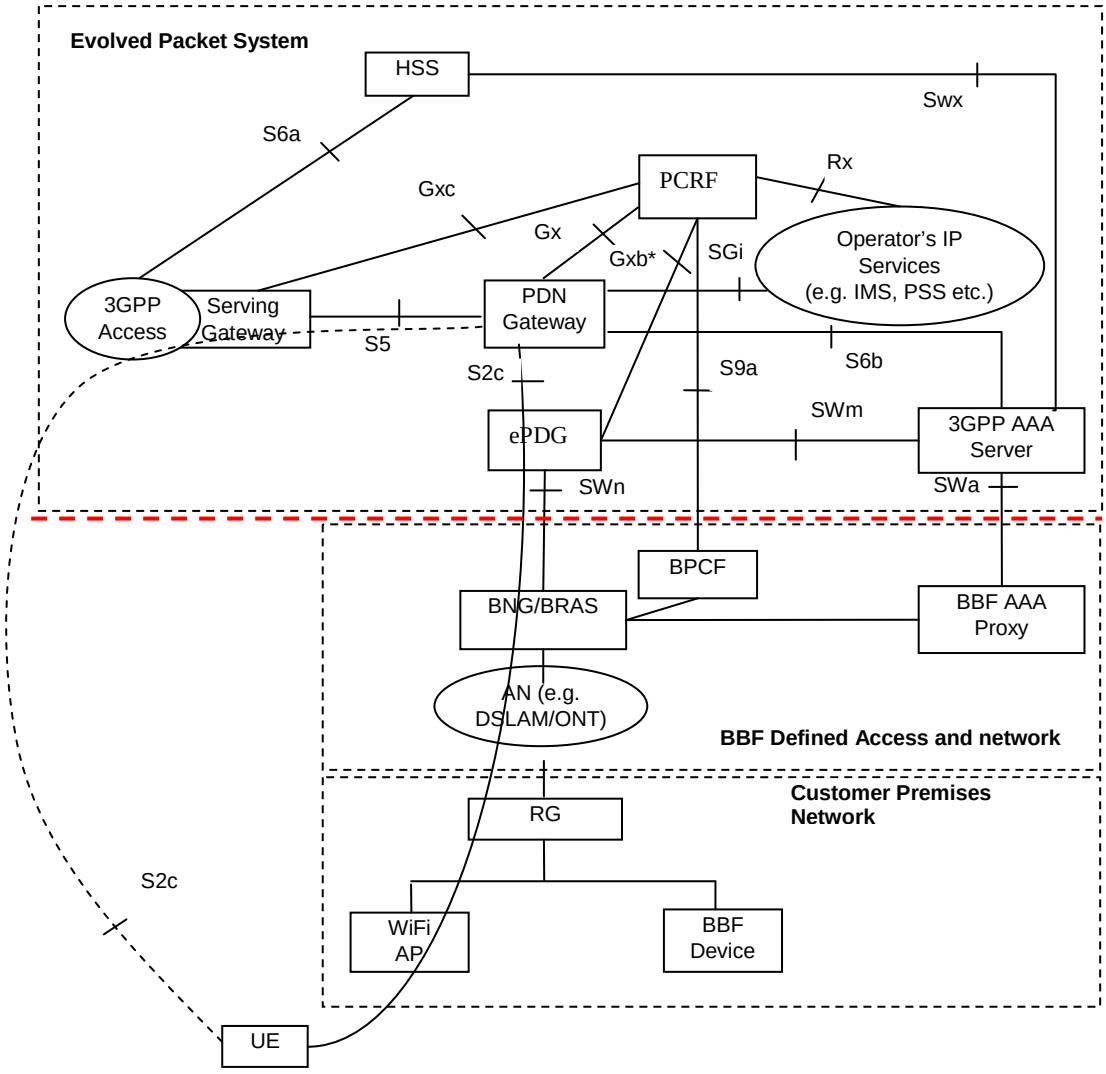

Figure 4.2.2-3: Non-Roaming Architecture for untrusted Fixed Broadband access network based on S2c

NOTE 4: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same network operator or to different network operators.

4.2.3 Roaming architecture for EPC-routed traffic

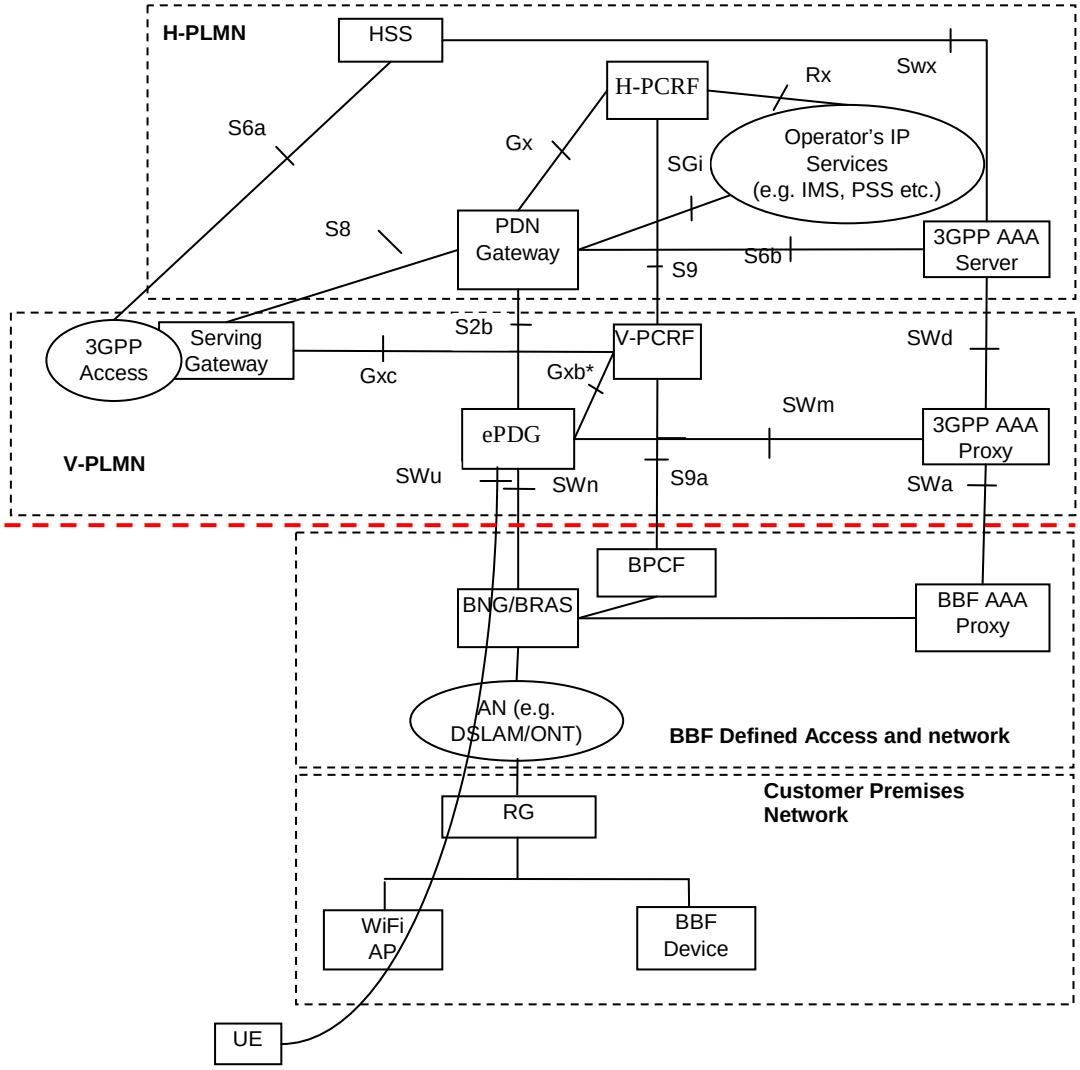

Figure 4.2.3-1: Roaming Architecture for untrusted Fixed Broadband access network based on S2b - Home routed traffic

NOTE 1: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

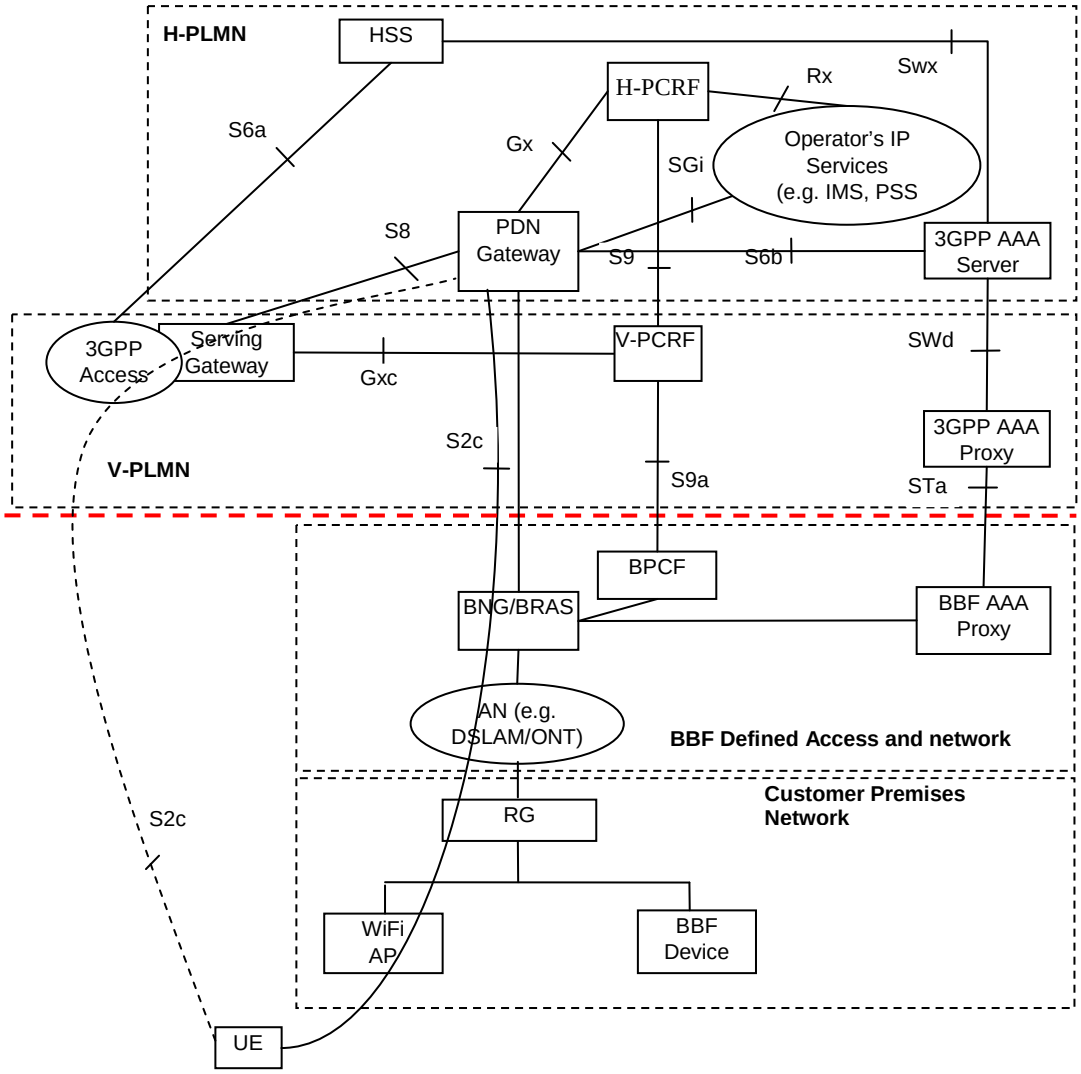

Figure 4.2.3-2: Roaming Architecture for trusted Fixed Broadband access network using S2c - Home Routed

NOTE 2: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

NOTE 3: The connection between the BRAS/BNG and PDN Gateway is an IP transport connection.

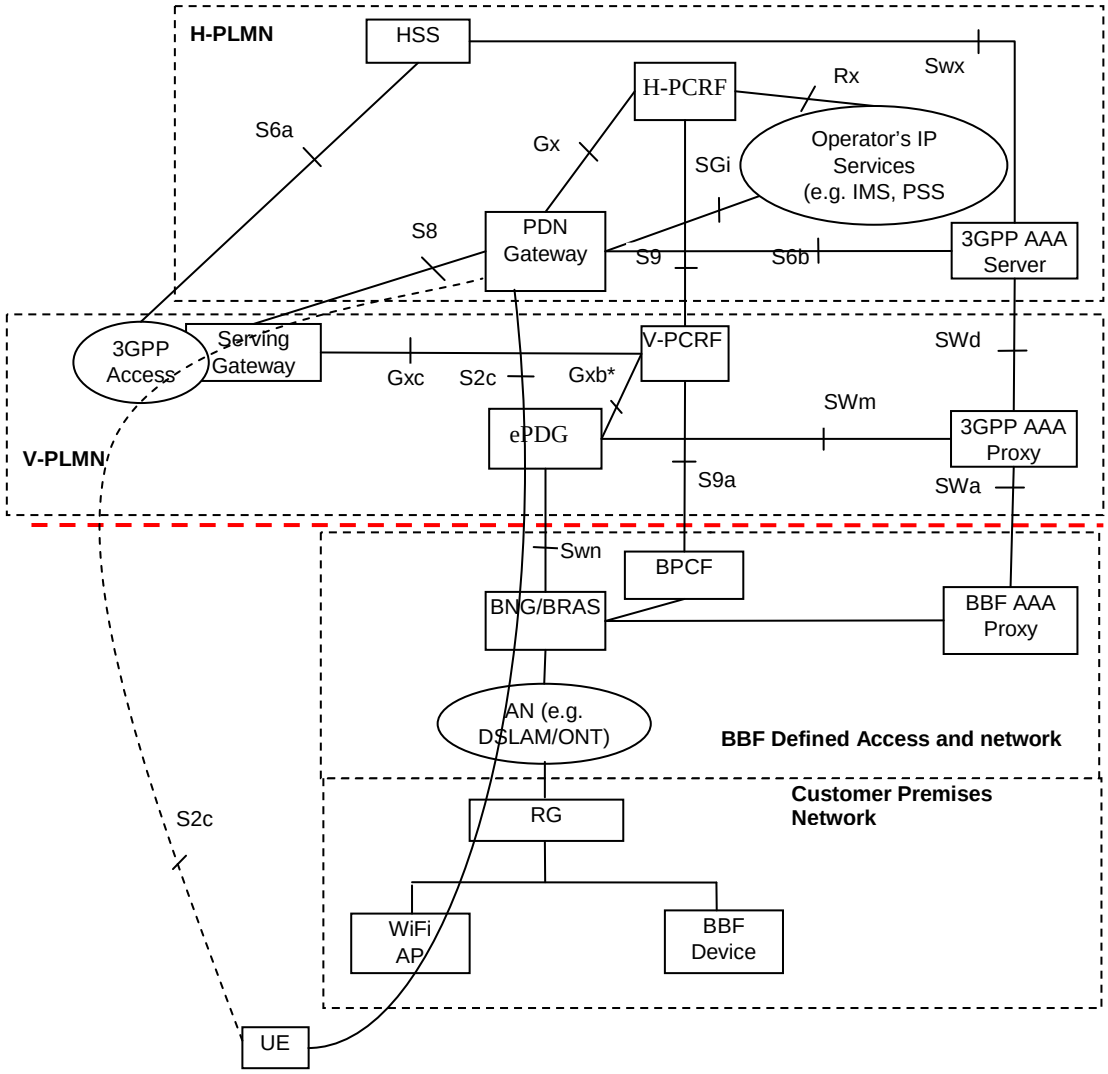

Figure 4.2.3-3: Roaming Architecture for untrusted Fixed Broadband access network using S2c - Home Routed

NOTE 4: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

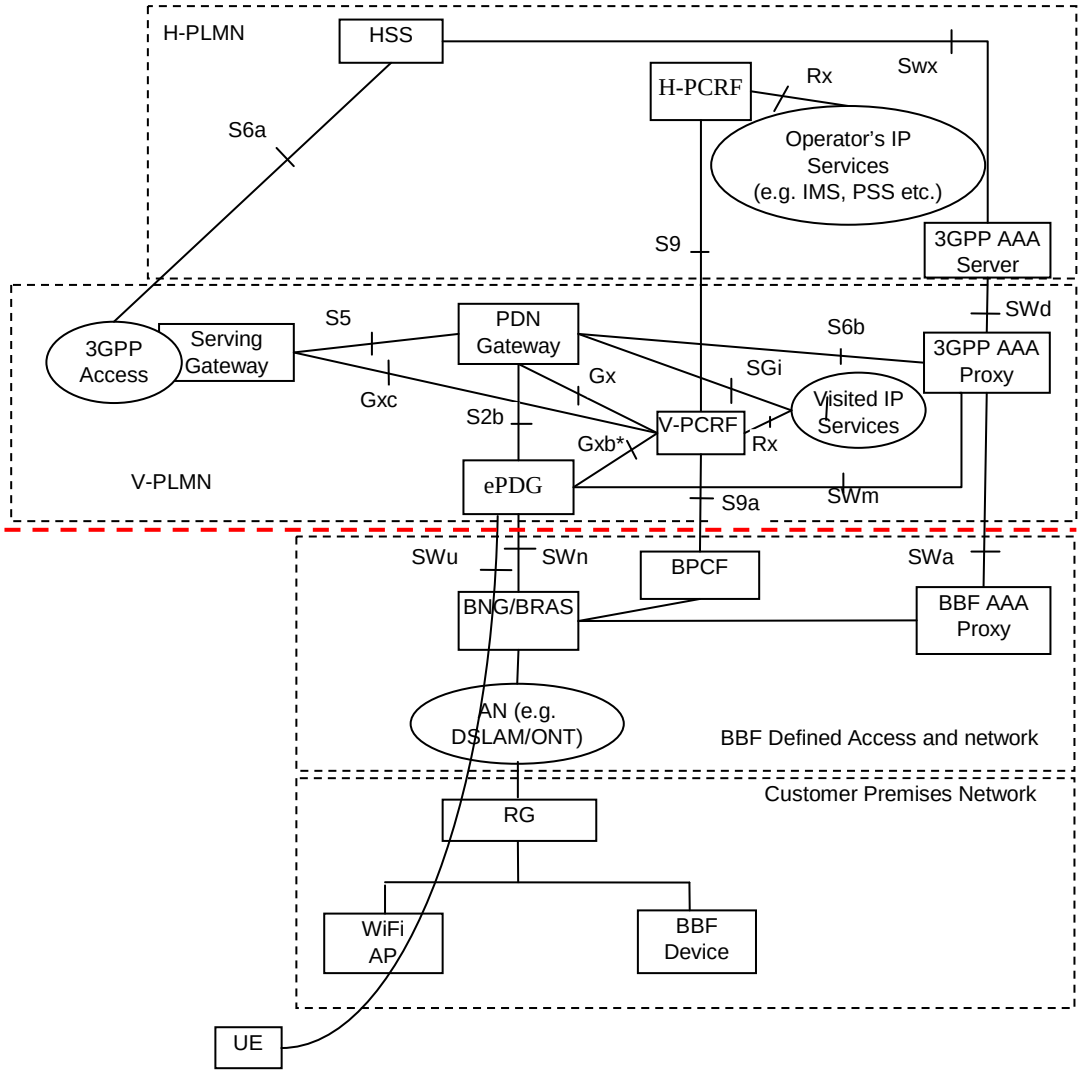

Figure 4.2.3-4: Roaming Architecture for untrusted Fixed Broadband access network using S2b – Local breakout in V-PLMN

NOTE 5: The two Rx instances in Figure 4.2.3-4 apply to different application functions in the HPLMN and VPLMN.

NOTE 6: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

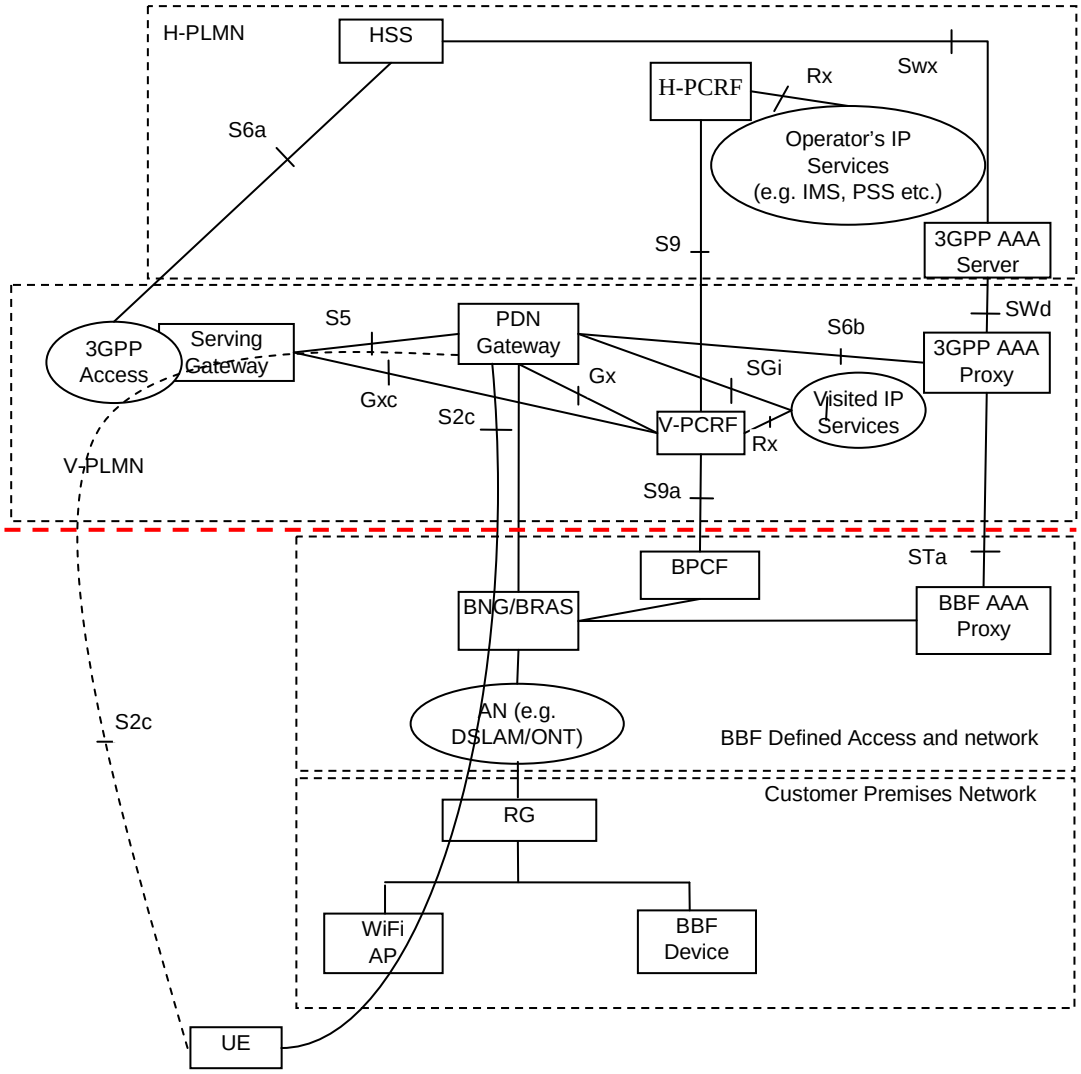

Figure 4.2.3-5: Roaming Architecture for trusted Fixed Broadband access network using S2c – Local breakout in V-PLMN

NOTE 7: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

NOTE 8: The two Rx instances in Figure 4.2.3-5 apply to different application functions in the HPLMN and VPLMN.

NOTE 9: The connection between the BRAS/BNG and PDN Gateway is a IP transport connection.

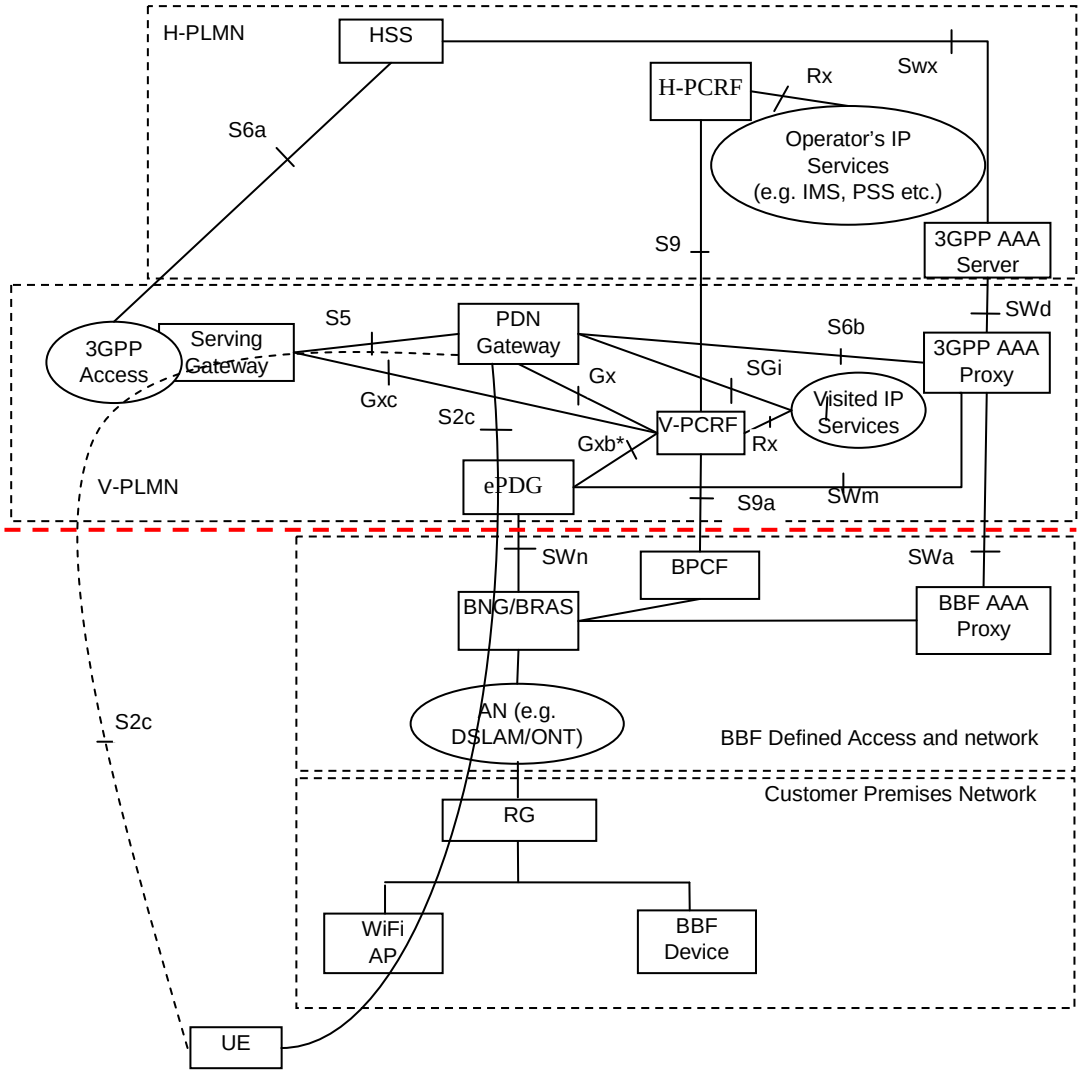

Figure 4.2.3-6: Roaming Architecture for untrusted Fixed Broadband access network using S2c – Local breakout in V-PLMN

NOTE 10: The reference architecture is applicable when both 3GPP and Fixed Broadband network belongs to the same VPLMN network operator or to different network operators.

NOTE 11: The two Rx instances in Figure 4.2.3-6 apply to different application functions in the HPLMN and VPLMN.

4.2.4 Architecture for non-seamless WLAN offload by the Fixed Broadband Access network

Figure 4.2.4-1, 4.2.4-2, 4.2.4-3, 4.2.4-4, 4.2.4-5, and 4.2.4-6 show the reference architectures for NSWO. The non-seamless traffic is routed to an external network directly from BBF network.

Although this clause describes only NSWO architecture scenarios, both NSWO and EPC-routed can co-exist during the network operation.

Architecture scenario A: AF in 3GPP operator's network

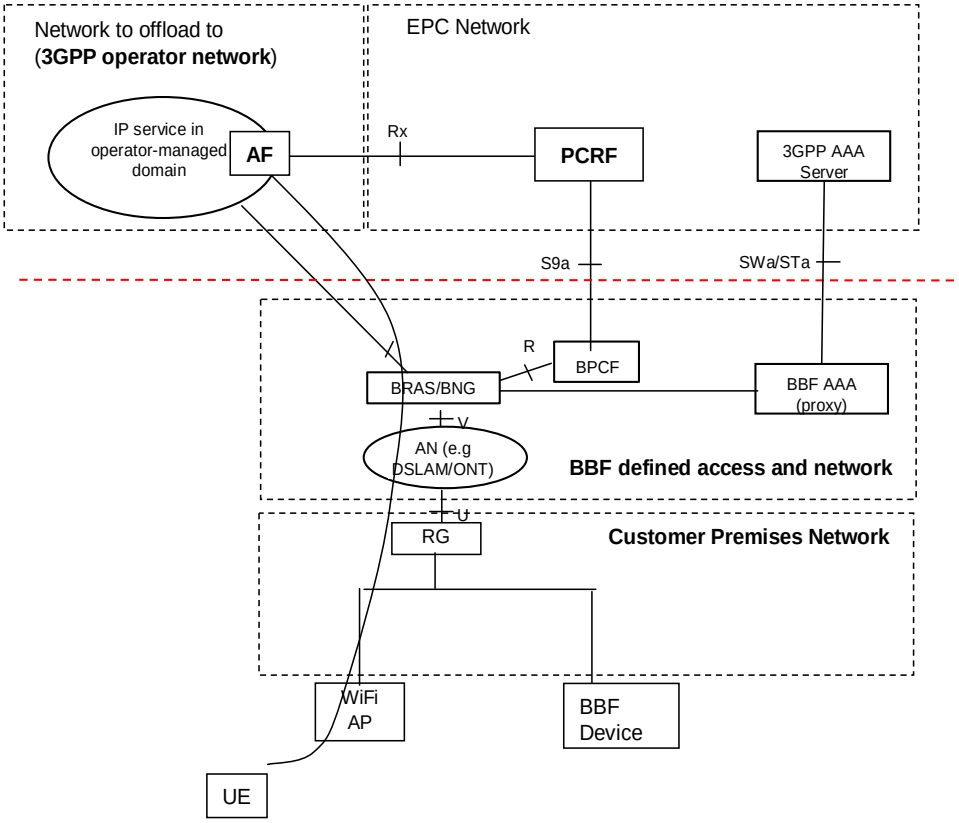

Figure 4.2.4-1: NSWO for 3GPP domain supporting the AF – non-roaming scenario

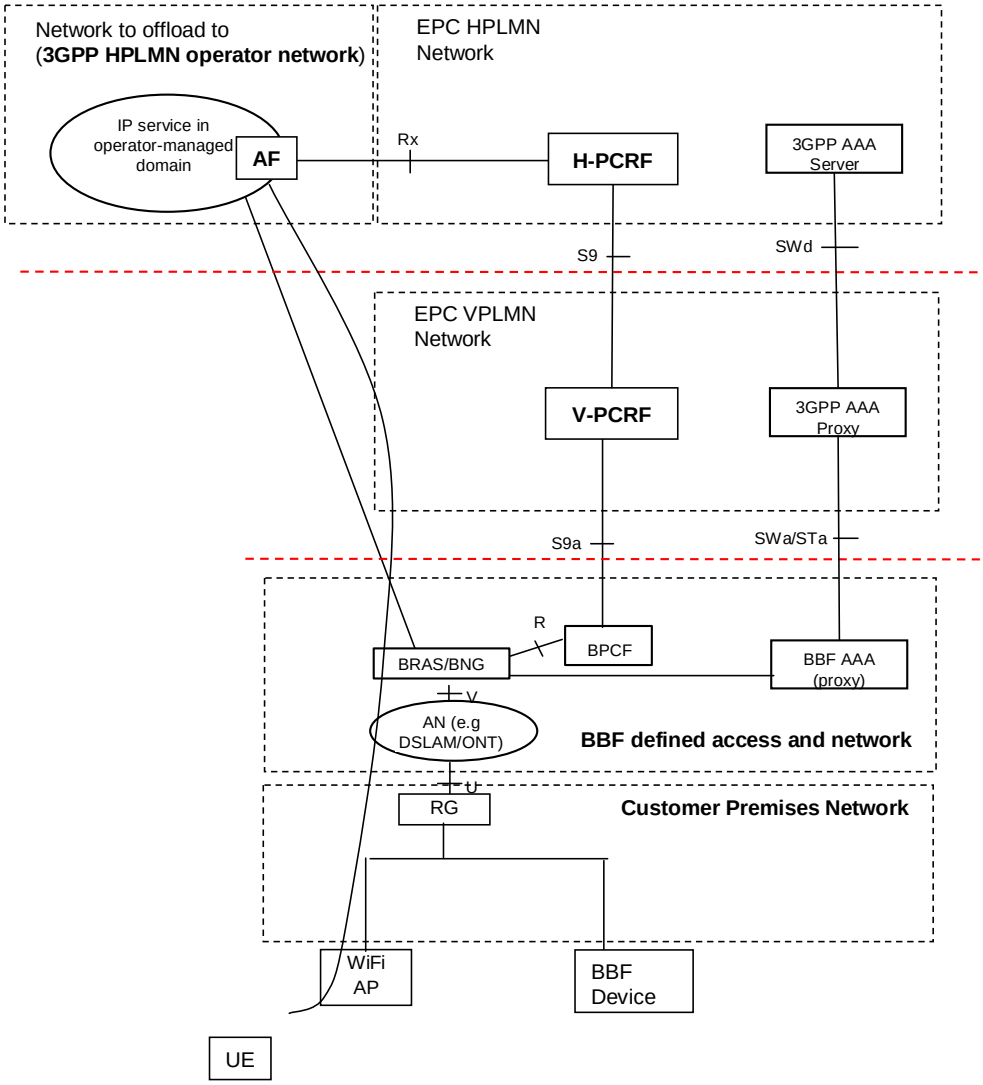

Figure 4.2.4-2: NSWO for 3GPP domain supporting the AF – roaming scenario

In this architecture scenario the AF is located in the 3GPP domain.

Architecture scenario B: AF ("BBF AF") in BBF domain

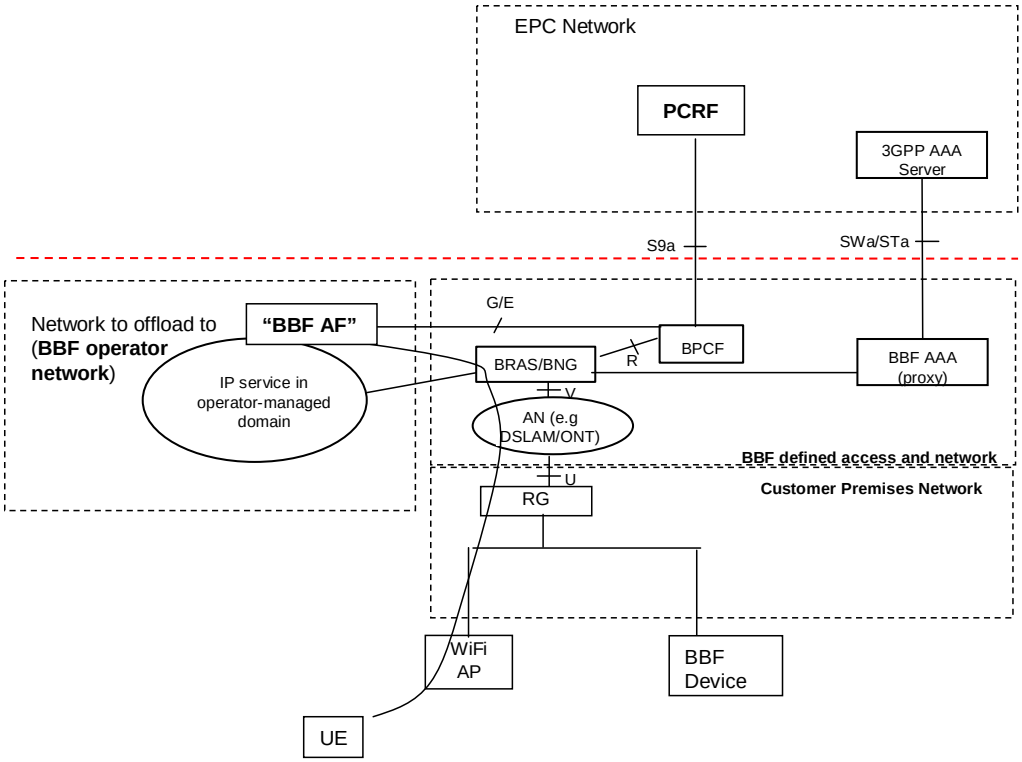

Figure 4.2.4-3: NSWO for 3GPP over BBF domain supporting the AF – non-roaming scenario

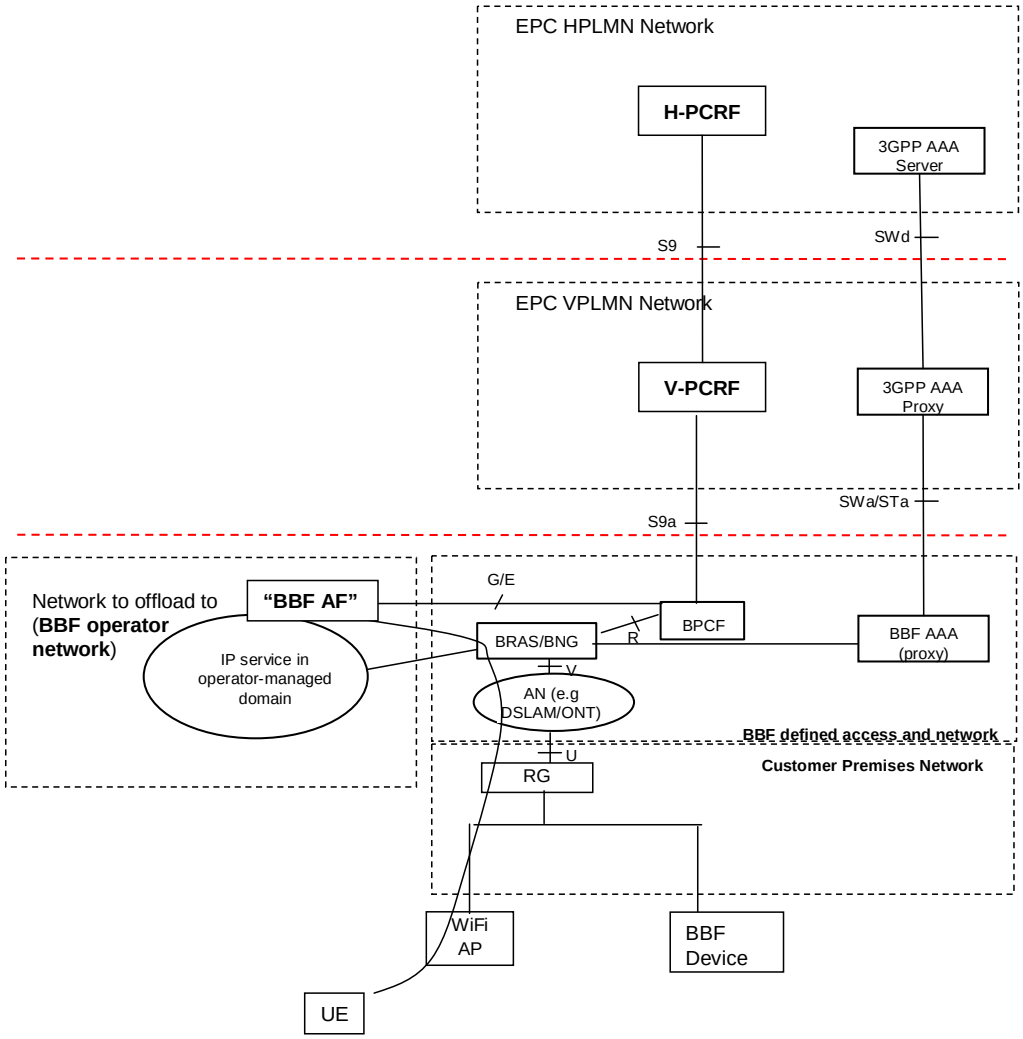

Figure 4.2.4-4: NSWO for 3GPP over BBF domain supporting the AF – roaming scenario

In this architecture scenario the AF ("BBF AF") is located in the BBF domain.

NOTE: The "BBF AF" and E/G reference point are out of 3GPP scope.

In this architecture scenario Rx signalling is supported over the S9a reference point.

The following assumptions are made about functionality in the BBF Access Network:

- The BPCF needs to map the request received over E/G (with UE local IP address) to the right IP-CAN session over S9a (i.e. session binding in BPCF) in order to find the right PCRF.
- The BPCF maps the signalling received from the BBF AF via G/E reference point in BBF domain to Rx signalling over S9a reference point.

Architecture scenario C: TDF

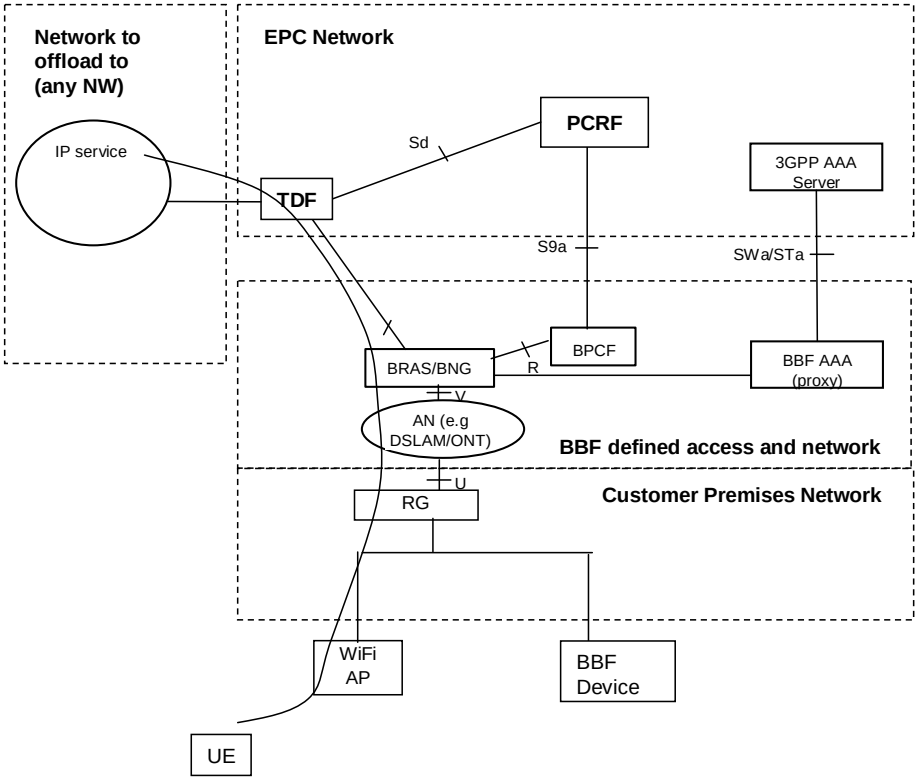

Figure 4.2.4-5: NSWO with TDF – non-roaming scenario

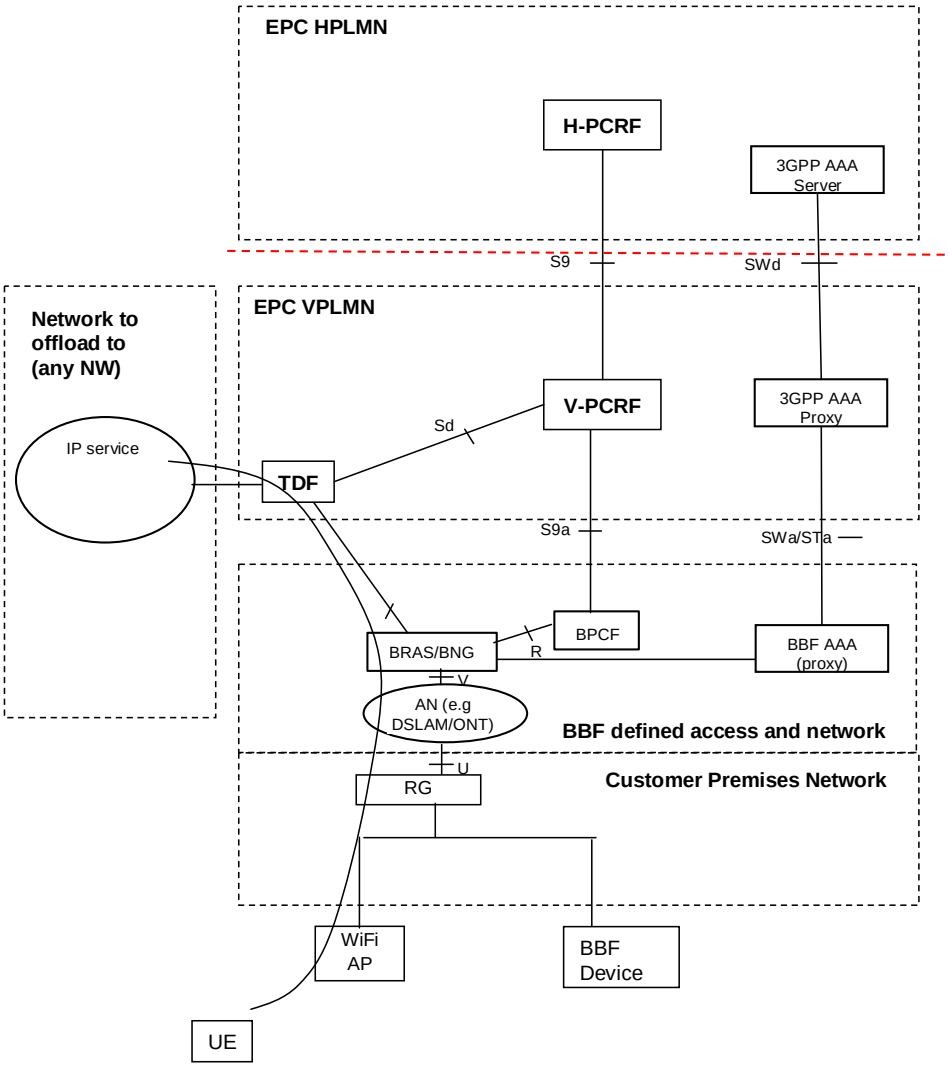

Figure 4.2.4-6: NSWO with TDF – roaming scenario

In this architecture alternative:

- Multiple TDFs may be deployed
- Sd is an intra-operator interface. This architecture variant is therefore limited to the case where the BBF domain and 3GPP domain are owned by the same operator.
- For roaming scenarios the TDF belongs to and is controlled by the VPLMN.
- For the solicited application reporting mode, the PCRF shall initiate the Sd interface triggered by S9a establishment, taking into account subscription data (verified by using e.g. IMSI, received from the BPCF).
- Home routed traffic (tunnelled using SWu, S2c) will not be subjected for packet inspection by the TDF.
- Policies for roaming users may be locally configured in the V-PCRF and/or TDF.

The following assumptions are made regarding functionality in the BBF Access Network:

- The BBF network routes the offloaded traffic subject to packet inspection and the offloaded traffic not subject to packet inspection via the same TDF, or
- The BBF network may be configured in such a way that the traffic determined to be subject to packet inspection is routed via the TDF. Traffic that is not subject to for packet inspection may physically bypass the TDF.

Editor's note: The support of differentiating routing handling for the traffic is subjected for packet inspection and the traffic not subjected for packet inspection by BBF access network requires further study in Broadband Forum.

4.3 Architecture for Fixed Broadband Access network interworking using H(e)NB

4.3.1 General

The architecture diagrams highlight the S9a interface between the PCRF and the BBF PCF (BPCF) for Femto access to support use cases and requirements per BBF TR-203 [6], TS 22.220 [14] and TS 22.278 [5].

The function of the S9a interface is to convey sufficient information to the BPCF to enable it to identify the BBF network elements the 3GPP Femto connects to, and perform admission control based on the bandwidth requirements and QoS attributes of a new or modified UE service data flow(s) (via the 3GPP Femto).

The reference architecture focuses on the policy management aspects of the 3GPP-BBF interworking.

NOTE 1: The assumption is that the BBF BNG may be enhanced to support new functionality such as provisioning of policies from the BPCF.

NOTE 2: The connection between the BRAS/BNG and the SeGW is IP transport connection.

NOTE 3: When the 3GPP and Fixed Broadband access networks belong to different Service Providers security arrangement are analogous to those between the H-PCRF and the V-PCRF, and can be based on TS 33.210 [16] or TS 33.310 [17].

4.3.2 Non Roaming Architecture

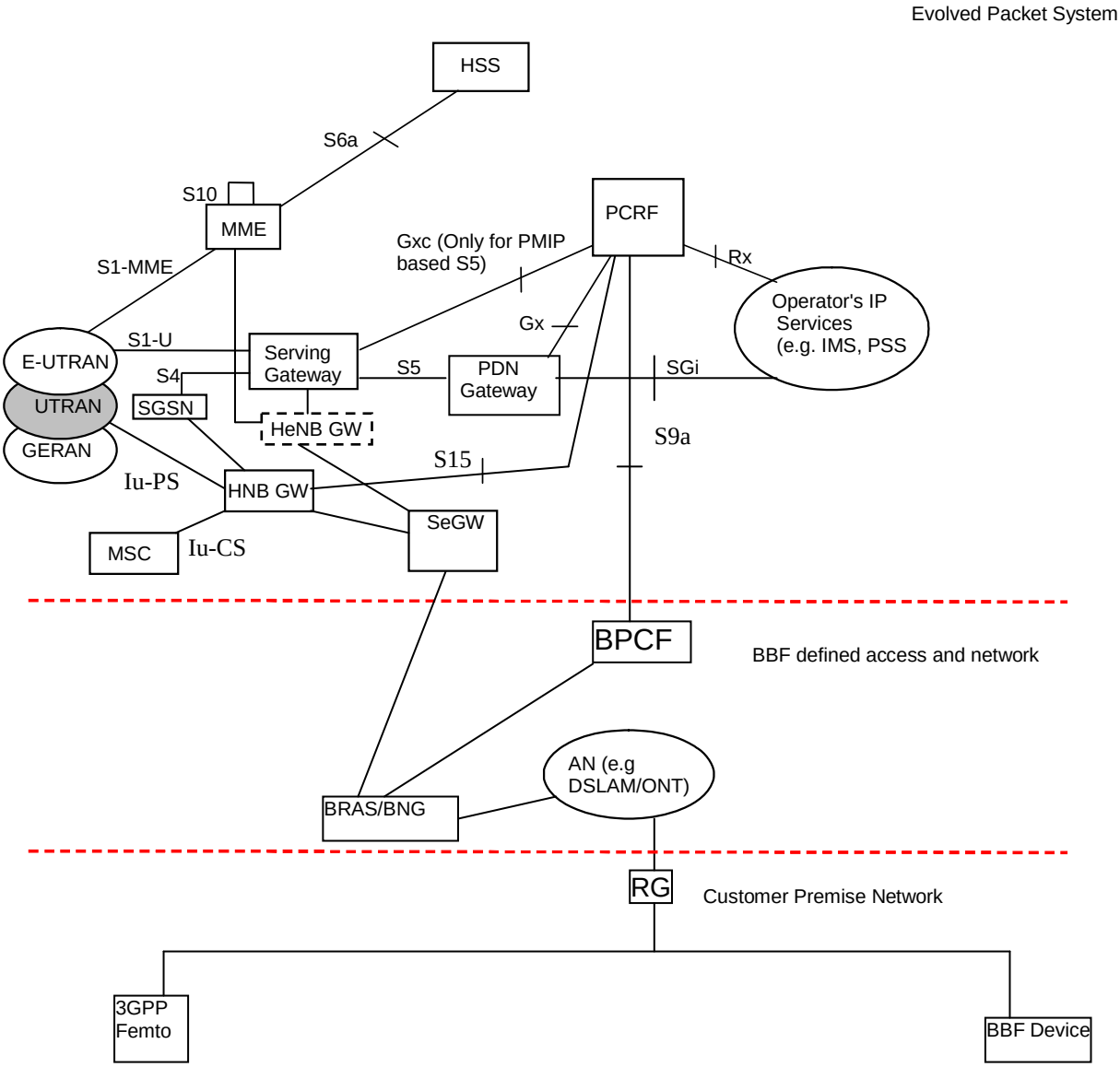

Figure 4.3.2-1: Non-Roaming Architecture

NOTE 1 The reference architecture is applicable when both 3GPP and Fixed Broadband network belong to the same network operator or to different network operators.

NOTE 2: There is only one S15 session for all UEs connected to a HNB.

4.3.3 Roaming Architecture - Home Routed

The GTP version of the architecture for the macro network does not require V-PCRF in the connection because the HPLMN does not provision QoS rules in the VPLMN. Since there is no V-PCRF in VPLMN the solution relies on the H-PCRF to initiate the Gateway Control Session over S9 to a selected V-PCRF that, in turn, initiates the Gateway Control Session over S9a with the BPCF. The HPLMN may provision policies in the VPLMN that take into account the fact that the UE connects to a 3GPP Femto.

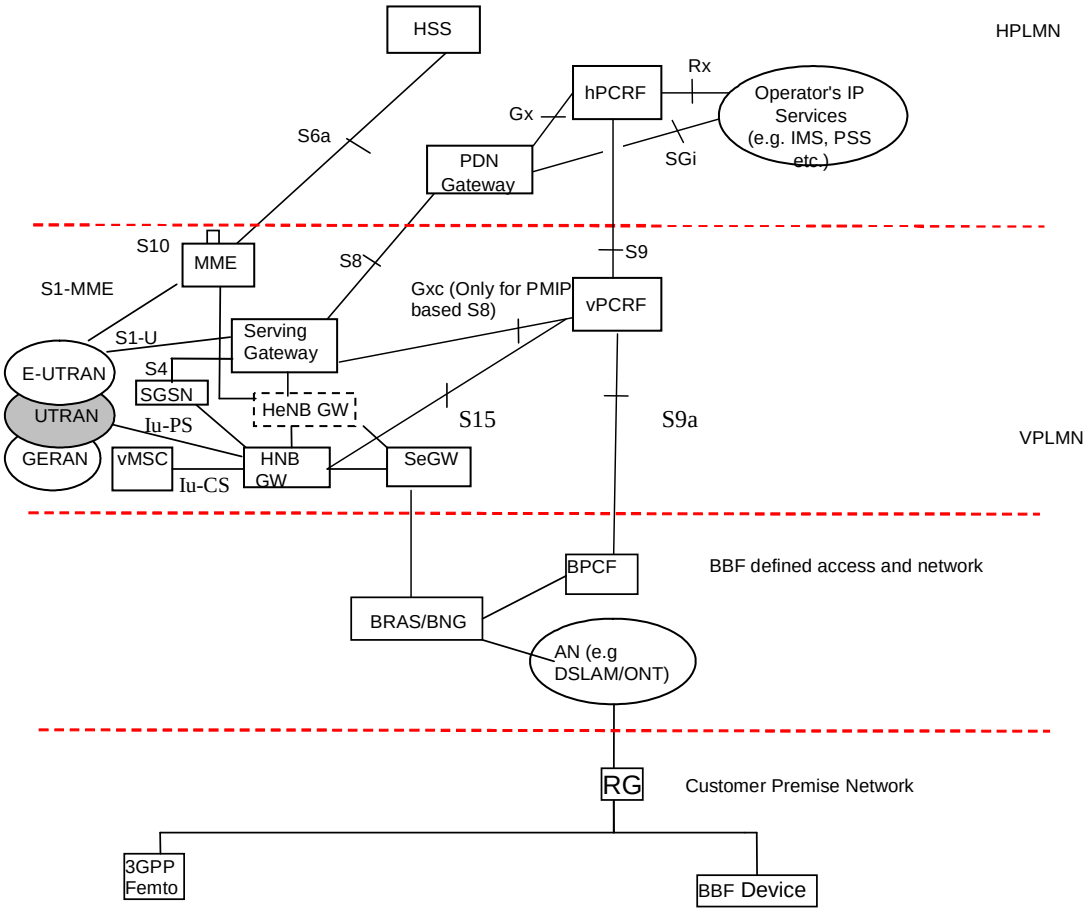

Figure 4.3.3-1: Roaming Architecture - Home Routed Traffic

NOTE 1: The reference architecture is applicable when both 3GPP VPLMN and Fixed Broadband network belong to the same network operator or to different network operators.

NOTE 2: There is only one S15 session for all UEs connected to a HNB.

4.3.4 Roaming Architecture - Visited Access/Local Breakout

The H-PCRF does need to be aware if the UE is connected via the 3GPP Femto in the VPLMN unless Home operators require provisioning of HPLMN policies in the VPLMN.

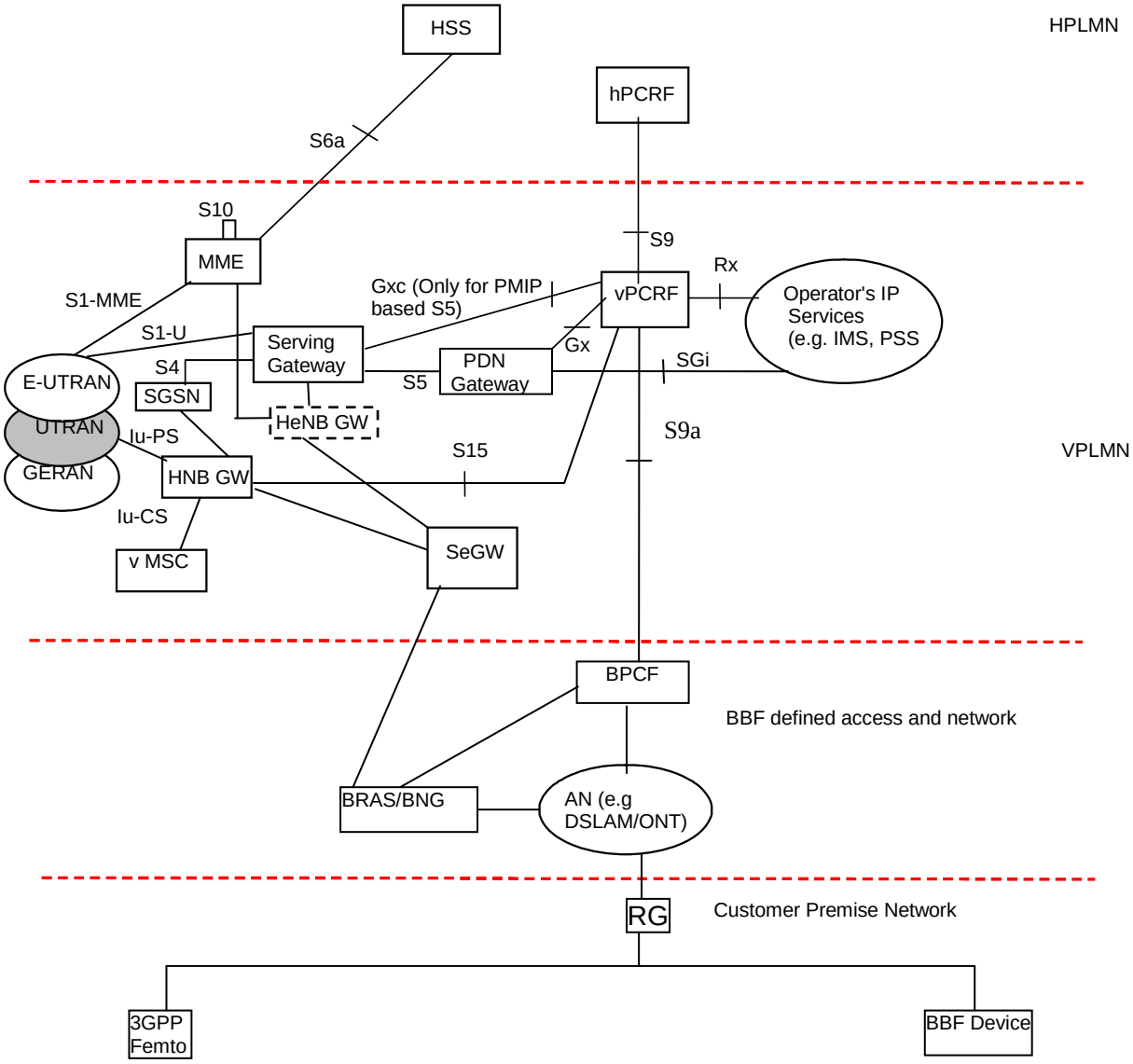

Figure 4.3.4-1: Roaming Architecture - Visited Access/ Local Breakout

NOTE 1: The reference architecture is applicable when both 3GPP VPLMN and Fixed Broadband network belong to the same network operator or to different network operators.

NOTE 2: There is only one S15 session for all UEs connected to a HNB.

5 Network Element, and Reference point

5.1 Network Elements

5.1.1 3GPP network elements

The 3GPP network elements are defined in details in TS 23.401 [2], TS 23 402 [3] and TS 23.203 [4].

5.1.1.1 ePDG

The details of functionality of ePDG are described TS 23 402 [3].

The following enhancements are applicable: To support initiation of a Gateway Control Session over S9a from the PCRF when using untrusted access procedures, the ePDG is enhanced to transport UE Local IP address, UDP port number(s) for the UE connected to WLAN to the PCRF via the Gxb* in untrusted S2c and S2b PMIP-based or via the S2b reference points in case of S2b GTP-based.

5.1.1.2 PCRF

The enhancement of PCRF for supporting interworking with BBF Policy Framework is described in TS 23.203 [4] Annex P.

5.1.1.3 3GPP AAA Server

The 3GPP AAA Server is within the 3GPP network. The 3GPP AAA Server is defined in TS 23 402 [3] and TS 29.273 [25].

In order to support offline and online charging for Non-seamless-WLAN offloaded traffic in Broadband Fixed Access network, the 3GPP AAA Server is enhanced to exchange accounting messages from 3GPP AAA proxy in roaming scenario or from BBF AAA proxy in non-roaming scenario. The 3GPP AAA Server reports per-user charging/accounting information about NS-WLAN offloaded traffic to the HPLMN Charging System.

5.1.1.4 3GPP AAA Proxy

The 3GPP AAA Proxy is within the 3GPP network. The 3GPP AAA Proxy is defined in TS 23 402 [3] and TS 29.273 [25].

In order to support offline and online charging for Non-Seamless WLAN offloaded traffic in Broadband Fixed Access network, the 3GPP AAA Proxy in VPLMN is enhanced to relay accounting data received from the BBF AAA Proxy in fixed domain to the 3GPP AAA Server in HPLMN. The 3GPP AAA Proxy is further enhanced to report per-user charging/accounting information to the VPLMN Charging System for inter-operator settlement for roaming users.

5.1.2 BBF network elements

The BBF network elements BRAS, BNG, RG, BBF AAA proxy, BPCF are defined in details in BBF TR-058 [7], BBF TR-101 [8], BBF TR-145 [10] and BBF TR-134 [11].The BBF device represents any devices defined by Broadband Forum or supported by Fixed Broadband Access, as a PC, Media centre, etc., and they are considered outside the scope of 3GPP.

The definition of enhancements for BBF AAA for 3GPP interworking and for BPCF to support Policy & QoS interworking with mobile networks is specified in BBF TR-134 [11] and BBF TR-203 [6]

5.2 Reference Points

The reference points S1-MME, S1-U, S3, S4, S5, S6a, S8, S10, S11 are defined in TS 23.401 [2]. The reference points S2c, S6b, SWx, SWd, SWm, SWn, SWu, SGi, Gxc are defined in TS 23 402 [3]. The reference point Rx and Sd are defined in TS 23.203 [4].

Gx For purpose of BBF interworking it transfers the UE/H(e)NB Local IP address and the UDP port number if NAT/NAPT is detected in the BBF access network at which the H(e)NB is connected to.

Gxb* It connects the ePDG with the PCRF and transports UE Local IP address, UDP port number(s) for the UE connected to WLAN. It is used in untrusted S2c and S2b-PMIP case .This information triggers the PCRF to initiate the Gateway Control Session over S9a.

S2b For purpose of BBF interworking it transfers UE Local IP address and UDP port number(s) in cases of S2b-GTP. This information triggers the PCRF to initiate the Gateway Control Session establishment over S9a towards the BPCF.

S15 It supports the initiation, modification and termination of sessions between the HNB GW and PCRF to support CS sessions. This interface triggers the PCRF to request allocation of resources in the Fixed Broadband access network for CS sessions.

S9 For BBF interworking for WLAN UE roaming with home routed access and S2b/Gx being used to trigger the PCRF to initiate the Gateway Control Session establishment over S9a, or for BBF interworking using GTP Home Routed Traffic for H(e)NB, the S9 interface is enhanced to carry from the H-PCRF to the V-PCRF the UE/H(e)NB Local IP address and the UDP port number if NAT/NAPT is detected in the Fixed Broadband access network at which the H(e)NB is connected to.

S9a For purpose of BBF interworking it provides transfer of dynamic QoS control policies (QoS) from the Home PCRF to the BBF Policy Control function (BPCF) and in roaming scenario from the Visited PCRF and to the BBF Policy Control function (BPCF). Furthermore the S9a carry from the H-PCRF/V-PCRF the UE/H(e)NB local IP address, UDP port number(s) and/or FQDN of Fixed Broadband access network at which the H(e)NB is connected to. The S9a is based on enhancement of S9 reference point for supporting interworking with BBF Policy Framework.

SWa For purpose of BBF interworking it connects the BBF AAA proxy with the 3GPP AAA Server/Proxy and transports access authentication, authorization and accounting information in a secure manner. The transport of accounting information is applicable only to non-seamless WLAN offloaded traffic.

STa For purpose of BBF interworking it connects the BBF AAA proxy with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and accounting information in a secure manner. The transport of accounting information is applicable only to non-seamless WLAN offloaded traffic.

The Reference points within the BBF access network are defined in BBF TR 058 [7], BBF TR-101 [8], BBF TR-145 [10] and BBF TR-134 [11] and they are considered out of the scope of 3GPP.

6 Policy and QoS interworking

6.1 General

6.1.1 Principles for EPC-routed traffic

Policy control for EPC routed traffic is provided when either 3GPP access authentication or tunnel based authentication is performed.

Multi Access PDN Connectivity for WLAN access located in a Fixed Broadband Access Network implies that a 3GPP UE with multi access PDN connectivity capabilities can connect to WLAN access located in a Fixed Broadband Access Network as described in TS 23.401 [2] and TS 23 402 [3].

Integrity and confidentiality protection for S2c trusted scenarios can be optionally activated by the UE or the PDN GW as defined in TS 23 402 [3]. In the case of confidentiality protection the Fixed Broadband Access Network does not have visibility of the inner header, similarly to what happens to the untrusted S2c case. However, given that DSCP of the outer header is used for packet differentiation, the procedures to support interworking with Fixed Broadband Access Network do not need to change due to the activation of confidentiality protection.

If the H(e)NB is located behind a NATed RG the H(e)NB local IP address is provided to the H(e)NB by the SeGW as part of the set up of the security tunnel with the SeGW using IKEv2 signalling.

A new HNB local IP address is provided by the SeGW to the HNB then included in Iu signalling (refer to the definition of INITIAL UE MESSAGE message, RELOCATION COMPLETE message and ENHANCED RELOCATION COMPLETE REQUEST message in TS 25.413 [28]) to the SGSN.

A new HeNB local IP address is provided by the SeGW to the H(e)NB then included in S1 signalling (refer to the definition of INITIAL UE MESSAGE message, HANDOVER NOTIFY message and PATH SWITCH REQUEST message in TS 36.413 [29]) to the MME.

6.1.2 Principles for Non-seamless WLAN-offload traffic

Policy control for NS-WLAN offloaded traffic is provided only if 3GPP access authentication is performed.

Policies for a UE's NS-WLAN offloaded traffic are sent from the EPC Network to the Fixed Broadband access network via S9a.

Policy interworking via S9a for NS-WLAN offloaded traffic in this release is supported for scenarios without NAT in the BBF domain,

For architecture scenario A in clause 4.2.4, the PCRF shall bind the request from AF with an existing IP-CAN session established over S9a using the UE local IP address received from AF and if available the subscriber ID (e.g. IMSI).

For architecture variant B in clause 4.2.4, it is assumed that BPCF binds the request from AF with an existing IP-CAN Session established over S9a using the UE local IP address received from AF and if available the subscriber ID (e.g. IMSI).

For architecture variant C in clause 4.2.4, in solicited application reporting mode, the PCRF shall start the Sd session with the TDF when an indication of IP-CAN session establishment is received over S9a for the UE local IP address. In unsolicited application reporting mode, the TDF notifies the PCRF of the detected service using the Sd interface.

The UE may simultaneously have one or more connection(s) to the EPC and a connection to NS-WLAN using the same local IP address. In order to allow the BNG to distinguish and to enforce separated QoS control for EPC routed traffic (tunnelled using SWu, S2c) and for NSWO traffic, the PCRF shall send the destination IP address of the IPSec outer IP header, i.e. the ePDG IP address (for S2b and untrusted S2c access), and PDN GW IP address(es) (for trusted S2c) and the UDP source port number (for used by IPSec tunnel traffic) to the BPCF.

6.2 Application of PCC to Fixed Broadband Access interworking

Fixed Broadband Access networks that support BBF Policy Framework and EPC network that supports the PCC interworked via procedures specified in TS 23.203 [4], Annex P.

6.3 QoS solution for 3GPP and Fixed Broadband Access Interworking

6.3.1 Generic

This clause describes how to detect and classify IP packets for the purpose of QoS treatment in the Fixed Broadband Access network. The solution is based on DSCP marking of packets traversing the Fixed Broadband Access network. The Fixed Broadband Access network (e.g. BNG) makes packet classification based on the DSCP of the incoming packets. The solution assumes functionality in the BBF domain, all these functions are out-of-scope for 3GPP; also, these functions may or may not be implemented depending on the agreement between 3GPP and Fixed Broadband Access operator, these functions are described for information only.

Fixed Broadband Access network currently supports the DSCP marking as specified in BBF TR-092 [20] for BRAS, in BBF TR-101 [8] for Access Nodes and Aggregation Nodes and in BBF TR-124 Issues 2 [21] for the RG.

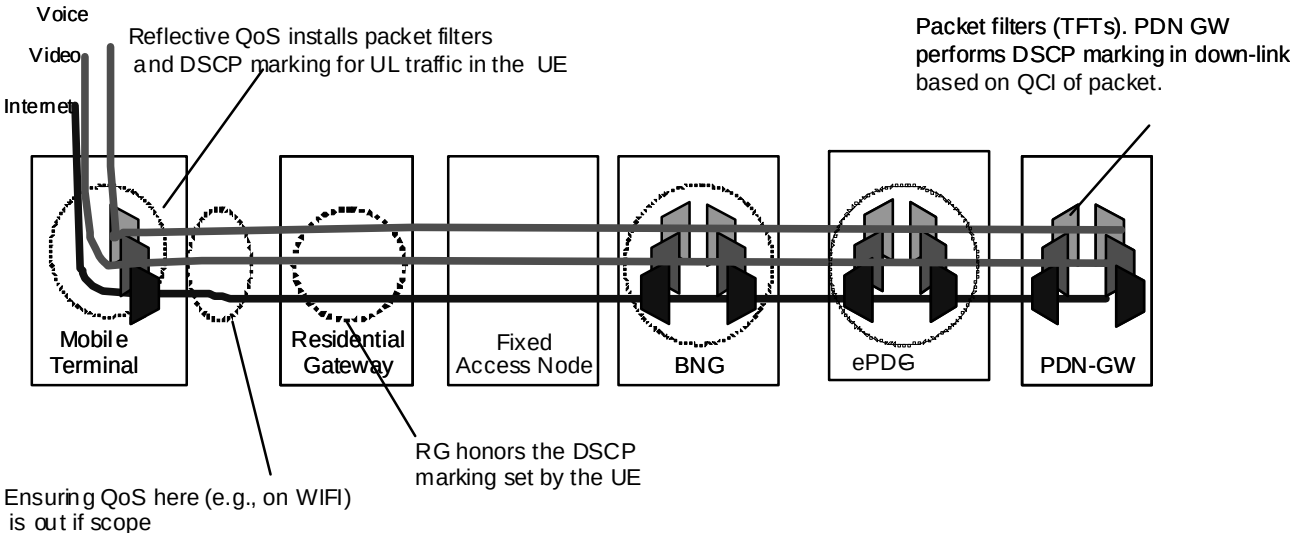

Figure 6.3.1-1: Packet classification and packet forwarding treatment in a 3GPP-Fixed Broadband Access interworking scenario for traffic routed to EPC

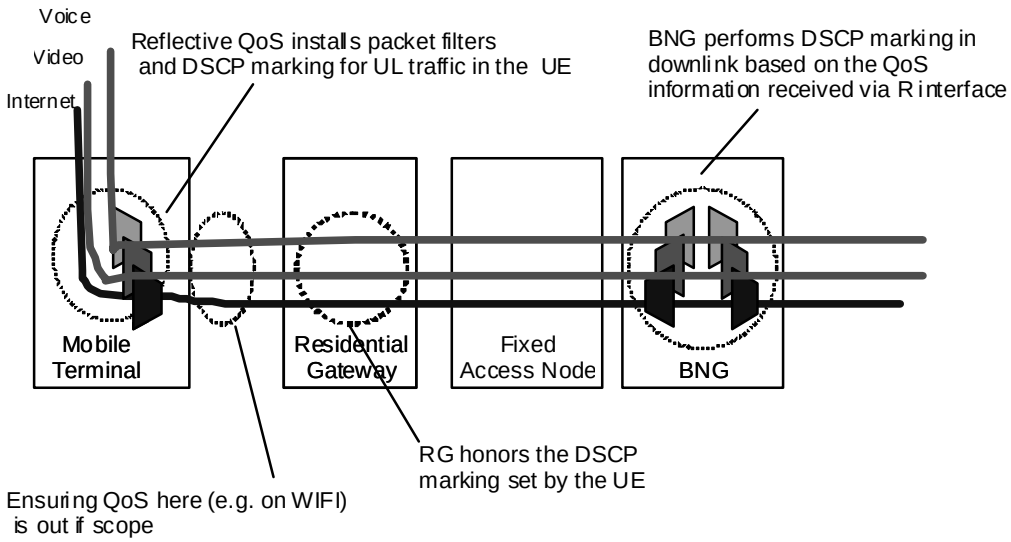

Figure 6.3.1-2: Packet classification and packet forwarding treatment in a 3GPP-Fixed Broadband Access interworking scenario for NS-WLAN offload traffic

The figure 6.3.1-1 and the figure 6.3.1-2 are simplified and the intermediate transport network entities in both figures are not shown. The details of traffic handling in the Fixed Broadband Access domain are out of 3GPP scope.

In order to support QoS in Fixed Broadband Access:

- The BPCF needs to map the QoS information (QCI, bit rates, ARP) received over S9a to access-specific parameters applicable in the Fixed Broadband Access network as specified in TR-203 [6].
- The BRAS/BNG can perform QoS treatment and QoS remapping based on DSCP value of the outer IP header as specified in BBF TR-059 [26]. For NS-WLAN offload traffic, the BRAS/BNG can support per-flow DSCP marking on each packet based on the QoS information received via R interface.
- The RG can perform QoS treatment and QoS remapping based on DSCP value of the outer IP header based on pre-provisioned rules in the RG as specified in BBF TR-059 [26].
- For both EPC routed traffic and NS-WLAN offload traffic cases, if the UE implements reflective QoS and the Fixed Broadband Access network needs to be protected from a misbehaving UE, Fixed Broadband Access needs to implement protective measures (e.g. per-UE bandwidth limitation in the RG or in the BNG).

- The decision to apply Reflective QoS is performed as part of the AAA signalling for UE authentication. The 3GPP AAA takes the decision to apply Reflective QoS based on the capabilities of the UE, the type of access and local policies then informs the UE.

- If the UE supports Reflective QoS then the UE shall indicate support of reflective QoS to the 3GPP AAA server during the authentication procedure using EAP-AKA signalling.

- In response to the UE indication, the 3GPP AAA may provide an indication to the UE on whether Reflective QoS shall be applied during the UE authentication procedure using EAP-AKA signalling.

    - When access authentication is performed the BBF AAA informs the 3GPP AAA that the UE is attached via BBF-defined Fixed Broadband access network in over STa/SWa and the UE shall perform UE reflective QoS on all traffic of the attached network. The UE shall disable the reflective QoS if the UE is detached or moves away from the attached Fixed Broadband access network.

    - When authentication is performed as part of IKEv2 signalling the 3GPP AAA determines if the UE is connected via a BBF-defined WLAN access based on UE Local IP address received in EAP-AKA signalling over SWm or S6b and the UE shall perform UE reflective QoS on the tunnelled traffic of the attached network. The UE shall disable the reflective QoS if the tunnel established by using the IKEv2 signalling is released.

NOTE: In this Release there is no procedure defined to support activation and deactivation of Reflective QoS towards the UE when moving from one BBF defined Fixed Broadband Access network into another BBF defined Fixed Broadband Access network.

6.3.2 Downlink

6.3.2.1 EPC routed traffic

For the WLAN case, the P-GW in the 3GPP domain sets a per-flow DSCP marking on each packet outer header, as defined in TS 23 402 [3]. In un-trusted scenarios where traffic is sent in an IPSec tunnel from ePDG to the UE, the ePDG shall copy that marking to the new outer header unless DSCP remapping is performed as defined in clause 6.3.4.

For the H(e)NB case, the P-GW in the 3GPP domain sets a per-flow DSCP marking on each packet outer header, as defined in TS 23.401 [2]. The SeGW shall copy that marking to the new outer header.

NOTE 1: DSCP remapping performed as defined in clause 6.3.4 may apply.

The BRAS/BNG located in between the H(e)NB and the SeGW/H(e)NB GW and between the UE and ePDG/PDN GW, may perform QoS treatment and QoS remapping based on DSCP value of the outer IP header.

For the control plane in the H(e)NB case, the QoS associated with control plane traffic (e.g. H(e)NB management traffic, Iu/S1 messages) could be preconfigured in the relevant network entity (e.g. H(e)MS, MME/SGSN) for downlink. The relevant message traffic thus may be marked with the appropriate DSCP according to the preconfigured QoS. The SeGW shall copy this DSCP if it exists from the inner header to the outer header.

NOTE 2: It is assumed that the MME/SGSN set the DSCP value of signalling traffic independently whether there is H(e)NB or not.

6.3.2.2 NS-WLAN offloaded traffic

The BNG/BRAS in the BBF domain may set a per-flow DSCP marking on each packet header. Alternatively, for operator deployments when the BNG is not at the network edge, the BNG may perform QoS treatment based on the DSCP value of the packet IP header.

6.3.3 Uplink

For the WLAN case, including EPC-routed traffic and NS-WLAN offload traffic, DSCP marking may be performed by the UE by means of reflective QoS. The UE creates a 5-tuple rule from the corresponding downlink 5-tuple derived from the downlink IP traffic. It associates that uplink rule with the DSCP received in corresponding downlink 5-tuple. Each uplink packet matching that uplink rule is marked with the associated DSCP.

For IP flows initiated from the UE, uplink packets will not be marked until a marked downlink packet is received with the downlink n-tuple that matches the received uplink n-tuple.

Some clarifications to the function of reflective QoS in the UE (this describes only the logical function for the reflective QoS marking, the implementation might be differently):

- For each incoming downlink IP packet the UE checks if a DSCP marking rule for the n-tuple of this IP packet exists. If the rule does not exist, then a new marking rule is added. Otherwise, the DSCP value and the time stamp for this marking rule are set.
- The uplink n-tuple in each marking rule is made from the downlink n-tuple of that rule by swapping address (and port) destination and source.
- For each outgoing IP packet the UE checks if a marking rule for this IP packet exists. If the n-tuple of the packet matches the uplink n-tuple of a marking rule, then the DSCP value of the packet is set to the DSCP value of that marking rule. The time stamp for that rule is set.
- For tunnelled scenarios, the n-tuples correspond to the n-tuples of the inner header of the packet. In all scenarios, the DSCP value of the marking rule is the DSCP value of the outer header of the packet. This in both downlink and uplink direction.
- A marking rule is removed when a certain period of time has passed since the time stamp.
- The function of reflective QoS will overwrite DSCP markings set by the UE application.

The Fixed Broadband Access implements bandwidth limitation on a per-line granularity. However, at this point in time, Fixed Broadband Access does not implement per-device bandwidth limitation in the RG. Therefore, the UE may take more uplink resources between RG and PDN GW then it was entitled to by S9a admission control (e.g. the UE might set the DSCP incorrectly). Fixed Broadband Access might implement a number of mechanisms to protect the Fixed Broadband Access network from a misbehaving UE :

- The RG might have pre-configured rules to allow only 3GPP UEs to set DSCP. Distinguishing 3GPP UE from other devices might for example be based on authentication (always EAP-AKA for 3GPP UEs) or from packet destination address (always ePDG/P-GW for S2b/S2c).
- The BNG may enforce UE bandwidth limitation based on the information (including QoS rules) received over S9a via the BPCF. These rules may have a different granularity as determined suitable for the Fixed Broadband Access network (e.g. in a scenario with user place confidentiality protection). The granularity may be on a per UE and DSCP or per UE and IP flow basis.

For the H(e)NB case, DSCP marking is performed by the H(e)NB according to the QoS information of the EPS bearer/PDP context. The H(e)NB shall copy the marking to the outer header. Based on H(e)NB configuration either the QCI mapping or the Reflective QoS may be used.

The RG and BNG located in between the H(e)NB and the SeGW/H(e)NB GW and between the UE and ePDG/PDN GW may perform QoS treatment and QoS remapping based on DSCP value of the outer IP header.

For the control plane in the H(e)NB case, the QoS associated with control plane traffic (e.g. H(e)NB management traffic, Iu/S1 messages) could be preconfigured in the H(e)NB for uplink. The H(e)NB marks the relevant message traffic with the appropriate DSCP according to the preconfigured QoS. It then copies the DSCP from the inner header to the outer header to ensure the correct QoS treatment in the tunnel before it gets into it.

6.3.4 DSCP remapping

This clause is only applied to EPC routed traffic case.

Since different domains and operators might use different DSCP values, the scheme above only works if there are agreed re-mappings of the DSCP values. E.g., there might be an edge router in inter-operator domain boundaries that re-maps the DSCPs.

It is assumed that there are appropriate inter-operator agreements (e.g. SLAs) in place to ensure that such re-mapping is consistent and predictable. If there is no such inter-operator agreement, the DSCP re-mapping may not be consistent and predictable.

6.3.5 Correlating admission control with DSCP marking

NOTE: This clause is applied to both EPC routed case and NS WLAN-offload traffic case.

In Fixed Broadband Access the admission control decision may be performed by the BPCF or be delegated by the BPCF to another Fixed Broadband Access node. Based on the admission control decision, the BPCF accepts or rejects the request received over S9a. The Fixed Broadband Access operator may also want to ensure that the traffic for a specific UE is not exceeding the traffic agreed by admission control and communicated over S9a. In order to do so, the BPCF may provide policies to the BNG. These policies are based on the QoS Rules received over S9a but may have a different granularity as determined suitable for the Fixed Broadband Access network.

Regardless of the access method used, the BPCF shall be able to translate QCI received in QoS Rules on S9a into the DSCP that the BNG will see. To do this, the BPCF shall know the relation between QCIs and DSCPs for the traffic that enters the Fixed Broadband Access domain. The QCI to DSCP mapping used in BBF access network in under BBF responsibility.

The correlation function mentioned above is Fixed Broadband Access-internal and therefore out-of-scope for 3GPP.

6.3.6 Multiple IPSec Child SAs support

This clause is only applied to EPC-routed case.

RFC 4301 [27] clarifies that if different classes of traffic (distinguished by DSCP bits) are sent on the same IPSec Security Association (SA) and if the receiver is employing the optional anti-replay feature available in both AH and ESP; this could result in inappropriate discarding of lower priority packets due to the windowing mechanism used by this feature. If this anti-replay feature is implemented then the ePDG/SeGW (downlink) and UE/H(e)NB (uplink) should map IP flows of different DSCP to different child SA to avoid this problem.

When the UE initial access through S2b, or s2c with extended security enabled or when H(e)NB power on, depending on the operator's policy, multiple IPSec child SAs with or without different DSCP are established between UE and ePDG or between H(e)NB and the SeGW. Both the uplink and downlink IP flows should be encapsulated and transferred within the appropriate child SA identified by the DSCP, if security association for different DSCP values are established, as described in RFC 4301 [27].

When a right child SA is not found a new child SA shall be created by the ePDG/SeGW (downlink) and UE/H(e)NB (uplink).

The increase of the anti-replay window size can also be used but it does not guarantee that packets will not be discarded.

6.4 Authentication and Security procedures for 3GPP and Fixed Broadband access interworking

The following procedures are defined for authentication of a 3GPP UE via a Fixed Broadband Access network as specified in TS 33.402 [23]:

- 3GPP-based access authentication. This assumes that the Fixed Broadband Access network supports 3GPP EAP-based access authentication and forwards EAP signalling messages between the UE and EPC.
- Tunnel authentication procedures for SWu. This authentication is transparent to the Fixed Broadband Access network.
- Authentication for S2c (DSMIPv6). This authentication is transparent to the Fixed Broadband Access network.

In procedure 1, the permanent user identity (i.e. an IMSI in EPC root NAI format as defined by TS 23.003 [24]) shall be provided upon successful authentication in the reply from 3GPP AAA to Fixed Broadband Access AAA, for both STa and SWa. The BPCF shall initiate an IP-CAN Session over S9a towards the PCRF for the UE as defined in clauses 7 and 8 and in TS 23.203 [4].

In procedure 2 and 3, a Gateway Control Session over S9a for this UE shall be triggered by the PCRF as defined in clauses 7 and 8 and in TS 23.203 [4].

Translation between RADIUS and Diameter is performed in the Fixed Broadband Access as described in TR-203 [6].

7 Functional Description and Procedures for Fixed Broadband Access network over S2b

7.1 General

The call flow figures in the subsequent clauses are based on TS 23 402 [3]. The home routed roaming, LBO and non-roaming scenarios are depicted. In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

The optional PCRF interaction steps between the gateways/BPCF and the PCRF in all the procedures only occur if dynamic policy provisioning is deployed. Otherwise the gateways may employ the policies statically configured in the gateways and Fixed Broadband Access may employ Fixed Broadband Access local policies.

7.2 Initial Attach

This clause specifies the additional procedures at the UE's initial attachment to a Fixed Broadband access network via PMIPv6 or GTPv2 based S2b interface, for the UE to establish the first PDN connection over the Fixed Broadband Access with S2b, and/or for the UE to have offloaded traffic via Fixed Broadband Access.

NOTE 1: It is up to stage 3 to optimize S9a procedures for Non-Seamless WLAN offloaded traffic and EPC routed traffic handled by the same PCRF.

This procedure establishes a session between the BPCF and the PCRF to provision policy decisions for NS-WLAN offloaded traffic and/or to provision policy decisions for EPC routed traffic.

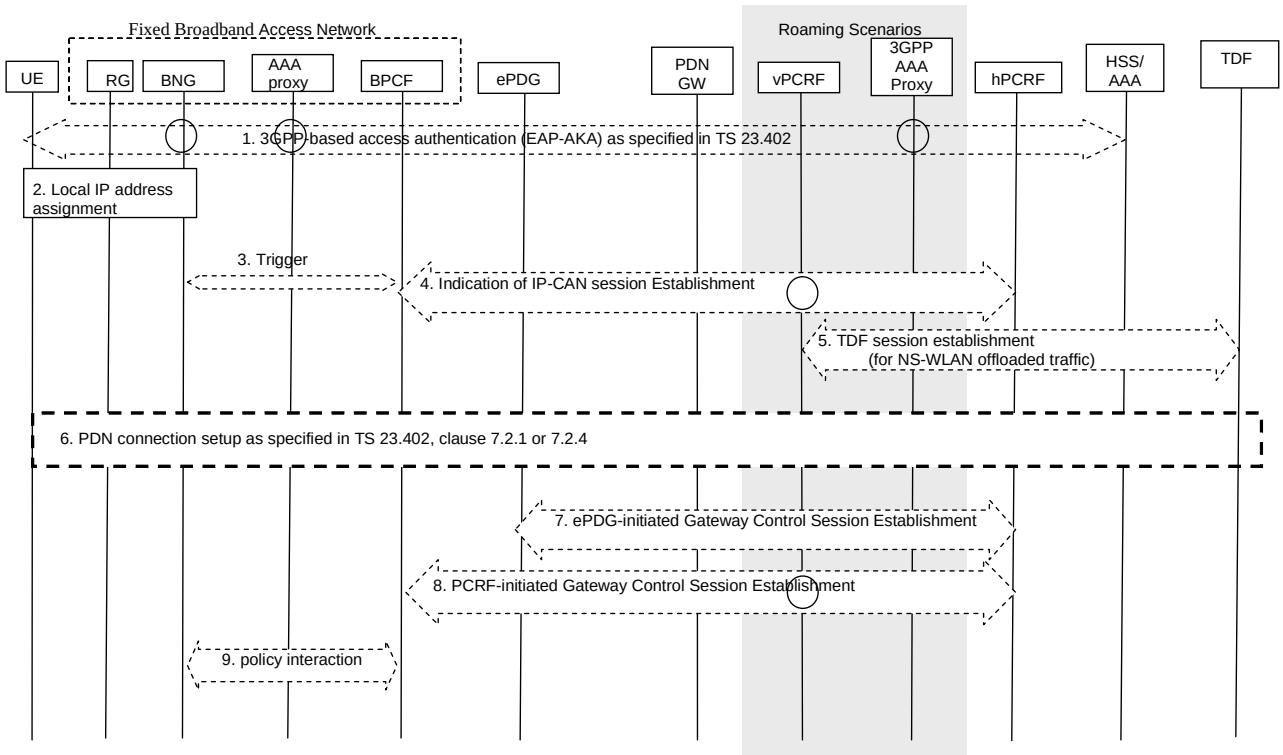

Figure 7.2-1: Initial attachment

NOTE 2 In the roaming case, step 7 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 3, 4, 5, 7 and 8 do not occur. Instead, the Fixed Broadband Access Network may employ local policies.

For NS-WLAN offloaded traffic, the local IP session for the UE in Fixed Broadband Access is handled as an IP-CAN session by the PCRF. For EPC-routed traffic, the IP-CAN session for the PDN Connection in the PDN GW is created via Gx procedures. In addition, a Gateway Control Session is established between the BPCF and the PCRF corresponding to the EPC-routed IP-CAN session in the PCRF.

The Fixed Broadband Access domain has local policies that indicate as part of the inter-operator agreements, both if policy control for NSWO is provided and the NSWO-APN for subscribers for a given HPLMN.

NOTE 3: Dynamic provisioning from the HPLMN of either an indication of policy control for NS-WLAN traffic and what the NSWO-APN is for the subscriber of a certain PLMN is out of the scope of this Release.

1. The UE may perform the 3GPP based (EAP) access authentication procedure involving the Fixed Broadband Access network as specified in TS 23 402 [3] clause 7.2.1 step 1. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the Fixed Broadband Access network and an indication to apply Reflective QoS is provided to the UE..

2. The UE receives a local IP address from the Fixed Broadband Access Network. How this is done is out of 3GPP scope, but it may involve IP address assignment by an RG or a BNG.

The steps in 3, 4 and 5 describe PCC signalling to provision policies for NS-WLAN offloaded traffic and are only triggered when 3GPP access authentication is performed and the BPCF receives the IMSI and the Fixed Broadband Access allocated UE local IP address.

3. Triggered by steps 1 and 2, the BPCF is informed about the UE accessing over Fixed Broadband Access. How this is done is out of 3GPP scope.

4. When the BPCF receives the trigger and policy interworking with PCRF is supported, if local policies indicate that policy control for NS-WLAN offloaded traffic is provided for subscribers from that PLMN, the BPCF sends an indication of IP-CAN session establishment for NS-WLAN offloaded traffic as specified in TS 23.203 [4]. The BPCF includes the IMSI, IP-CAN type, UE local IP address and the NSWO-APN in the message to the PCRF. The PCRF acknowledges the IP-CAN session establishment if HPLMN operator policies enable policy control for NS-WLAN offloaded traffic for this user as specified in TS 23.203 [4]..

5. Triggered by the successful establishment of the IP-CAN session for the UE local IP address in step A2, the V-PCRF (roaming) and the PCRF (non-roaming) may establish a session with the TDF to provision ADC Rules for that UE local IP address (if applicable and when solicited application reporting mode applies).

The steps in 6, 7 and 8 describe PCC signalling to provision policies for EPC routed traffic. Step 7 is only applicable when S2b PMIPv6 is used.

6. The description of the PDN connection setup procedure is the same as for steps 2-9 in TS 23 402 [3], clause 7.2.1 or for steps A.1-E.1 in TS 23 402 [3] clause 7.2.4, with the following additions when S2b-GTP is used: The UE local IP address and optionally UDP source port number (if NAT is detected) are also included in the Create Session Request message. The UE local IP address and optionally UDP source port number (if NAT is detected) are forwarded to the PCRF in IP-CAN Session Establishment procedure, an indication to apply Reflective QoS is provided to the UE as part of the IKEv2 tunnel establishment.

7. Triggered by the IKEv2 tunnel establishment in step 3 and by the indication that the UE is connected via a WLAN connected to fixed broadband access from 3GPP AAA, the ePDG initiates Gxb* session establishment with the PCRF by using Gateway Control Session establishment procedure as specified in TS 23.203 [4]. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC, the UE local IP address and optionally UDP source port number (if NAT is detected).

NOTE 4: The 3GPP AAA determines if the UE is connected via a WLAN connected to a fixed broadband access on UE Local IP address received in EAP-AKA signalling over SWm.

8. This step may be triggered by step 6 or step 7.

   When triggered by step 6, the PCRF (for non-roaming case), the V-PCRF (for visited access) or the H-PCRF (for home routed) initiates Gateway Control Session establishment with the BPCF. The V-PCRF (for home routed) proxies the Gateway Control Session Establishment request to the BPCF: IMSI and UE local IP address and port needs to be included in the Gateway Control Session Establishment request message.

When triggered by step 7, the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case) initiates Gateway Control Session establishment request over S9a with the BPCF. IMSI and UE local IP address and port needs to be included in the Gateway Control Session Establishment request message over S9a.

9. The BPCF may interact with the BNG, e.g. to download policies, as defined by Fixed Broadband Access Policy Framework specifications BBF TR-134 [11] and BBF TR-203 [6]. This step is out of 3GPP scope.

7.3 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection

This clause is related to the case when the UE has one or more PDN connection(s) established via a Fixed Broadband access network via PMIPv6 or GTPv2 based S2b interface and the Detach Procedures is initiated by UE or ePDG, or the UE-requested PDN disconnection procedure is triggered. It is also related to the case when the UE has no PDN connection(s) established via a Fixed Broadband access network.

The UE can initiate the Detach procedure, e.g. when the UE is power off. The ePDG may initiate the Detach procedure due to administration reason or the IKEv2 tunnel releasing.

As part of the Detach procedure for multiple PDN connectivity, steps 1 to 3 of this procedure shall be repeated for each PDN connected.

This procedure terminates both the IP-CAN session and the Gateway Control Session(s) over S9a between the BPCF and the PCRF.

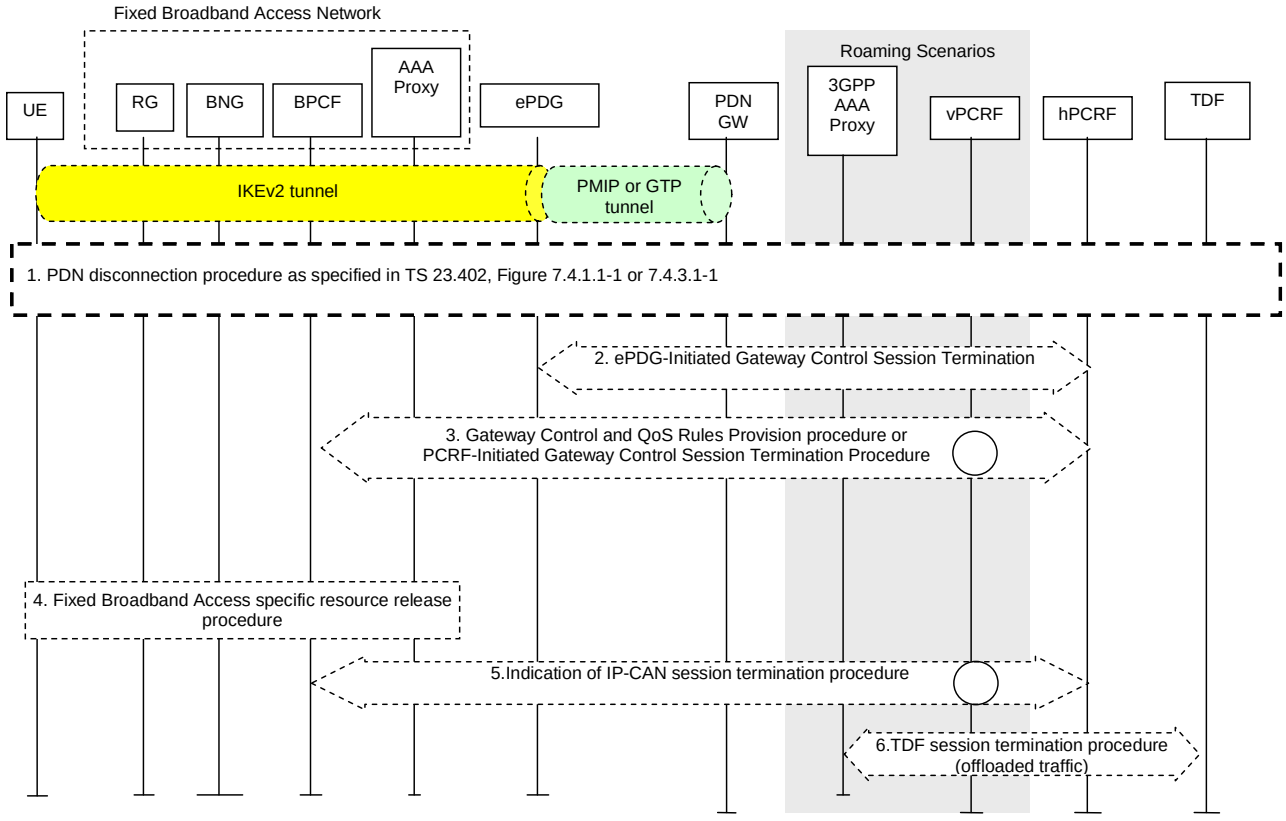

Figure 7.3-1: UE/ePDG-initiated detach procedure or UE-requested PDN disconnection procedure

NOTE 1: In the roaming case, the Step 2 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 2, 3, 5 and 6 do not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

1. The description of the IKEv2 tunnel and the PMIPv6 or GTPv2 tunnel releasing procedure is same as TS 23 402 [3], clause 7.4.1.1 or 7.4.3.1.

The steps in 2 and 3 describe PCC signalling to remove policies for EPC routed traffic.

2. Triggered by the IKEv2 tunnel releasing in step 1, the ePDG executes Gateway Control Session termination procedure with the PCRF as specified in TS 23.203 [4]. This step is only applicable when S2b PMIPv6 is used.

3. Triggered by the Gateway Control Session termination received from ePDG or by the IP-CAN session termination over Gx, the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case for S2b-PMIP) and the H-PCRF (for home routed and visited access roaming case for S2b-GTPv2) executes a Gateway Control and QoS Rules Provision procedure with the BPCF or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF would be performed as specified in TS 23.203 [4]. This step is applicable when either S2b based PMIPv6 or GTPv2 are used.

4 Fixed Broadband Access specific resource release procedure may be executed, as defined by Fixed Broadband Access Policy Framework specifications BBF TR-134 [11] and BBF TR-203 [6]. This step is out of the scope of 3GPP.

The steps in 5 and 6 describe PCC signalling to remove policies for NS-WLAN offloaded traffic. Step 5 may be triggered by the notification to the BPCF that the IMSI is not authenticated any longer (e.g. re-authentication time out) and/or the UE local IP address was released using Fixed Broadband Access procedures.

5. The BPCF sends an indication of IP-CAN session termination to the PCRF as described in TS 23.203 [4].

6. Triggered by previous step, the PCRF (for non-roaming case) and the V-PCRF (for roaming cases) terminates the TDF session for the UE local IP address (if applicable).

7.4 HSS/AAA-initiated Detach Procedure

This procedure is applicable if the UE accesses a Fixed Broadband Access network with GTPv2 or PMIPv6 based S2b interface. And the HSS initiates the detach procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

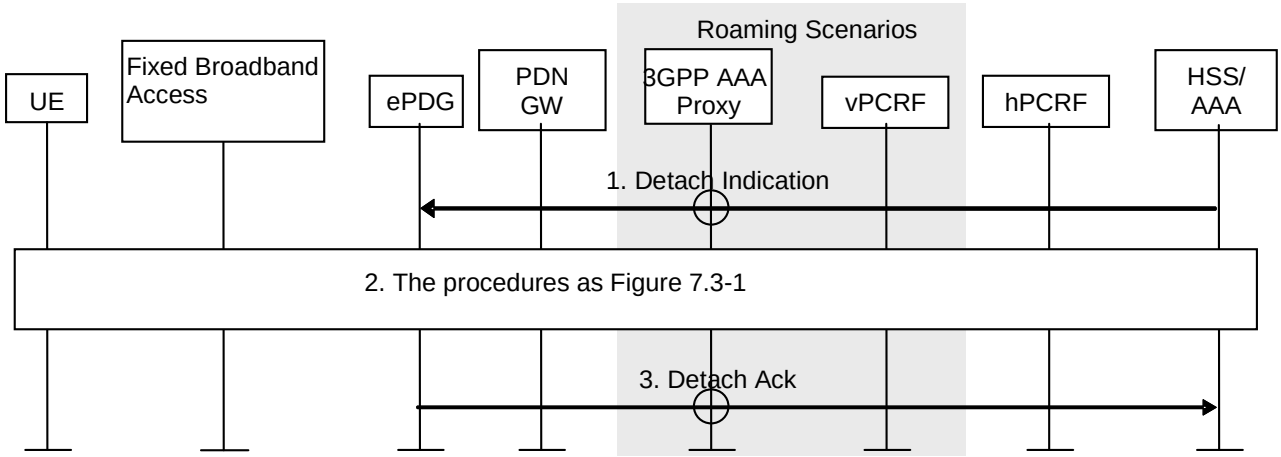

Figure 7.4-1: HSS/AAA-initiated detach procedure

For connectivity to multiple PDNs, Step 2 shall be repeated for each PDN the UE is connected to. Step 2 can occur in parallel for each PDN.

1. The description of this step is the same as for step 1 in TS 23 402 [3], clause 7.4.2.1.

2. This description of the detach procedure is same as clause 7.3.

3. The description of this step is the same as for step 3 in TS 23 402 [3], clause 7.4.2.1.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIPv6 or GTPv2 tunnels on S2b, since the ePDG is responsible for removing the PMIPv6 or GTPv2 tunnels on S2b. The PDN GW acknowledges the receipt of the detach indication message to the HSS/AAA.

7.5 UE-initiated Connectivity to Additional PDN

This clause is related to the case when the UE has an established PDN connection via a Fixed Broadband Access Network using GTPv2 or PMIPv6 based S2b and wishes to establish one or more additional PDN connections over the same access. Since GTPv2 or PMIPv6 is used to establish connectivity with the additional PDN, the UE shall establish a separate SWu instance (i.e. a separate IPSec tunnel) for each additional PDN.

The description of supporting additional PDN connections with PMIPv6 based S2b is same as it is specified in TS 23 402 [3], clause 7.6.1. The description of supporting additional PDN connections with GTPv2 based S2b is same as it is specified in TS 23 402 [3], clause 7.6.3.

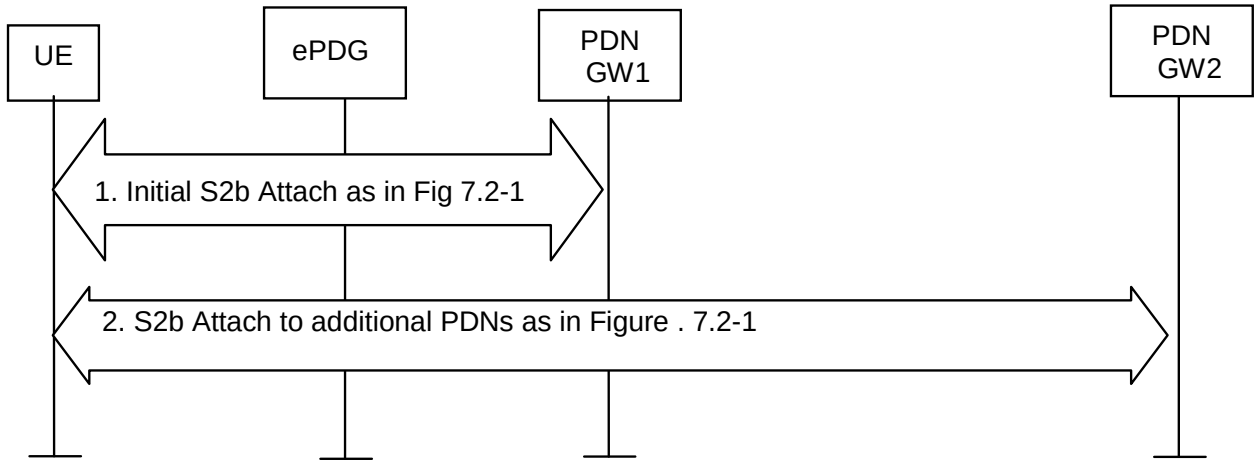

Figure 7.5-1: UE-initiated connectivity to additional PDN over a Fixed Broadband Access Network

1. The UE has performed the Initial S2b Attach procedure as defined in clause 7.2 and has an established PDN connection.
2. The UE repeats the procedure of clause 7.2, steps 6-9 for each additional PDN the UE wants to connect to, with the following exceptions:
   - The IKEv2 tunnel establishment procedure for each additional PDN connection is initiated with the ePDG that was selected in step 1 in clause 7.2.
   - For network supporting multiple mobility protocols, if there was any dynamic IPMS decision in step 1 in clause 7.2, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.
   - In Step 8, if no Gateway Control session over S9a for this UE, then the PCRF initiates the Gateway Control Session Establishment procedure with the BPCF. Otherwise, the PCRF provide new QoS rules corresponding to the new PDN connection to the BPCF using the Gateway Control and QoS Rules Provisioning procedure.

7.6 Network-Initiated Dynamic PCC for EPC-routed Traffic

This procedure is applicable if the UE accesses via a Fixed Broadband Access network with GTPv2 or PMIPv6 based S2b interface for the EPC-routed traffic. And if dynamic PCC is deployed, the procedure given in Figure 7.6-1 is used by the PCRF to provision rules to the Fixed Broadband Access and for the Fixed Broadband Access to enforce the policy by controlling the resources and configuration in the access. This procedure is applicable only when the UE is already attached the Fixed Broadband Access network access and the PCRF is capable to discover the BPCF for the Fixed Broadband Access serving the UE. The access specific procedure executed in the Fixed Broadband Access is out of scope of this specification. In case 2b, defined in clause 7.1 of TS 23.203 [4] when UE connecting via Fixed Broadband Access access no QoS Rules should be provisioned to the ePDG.

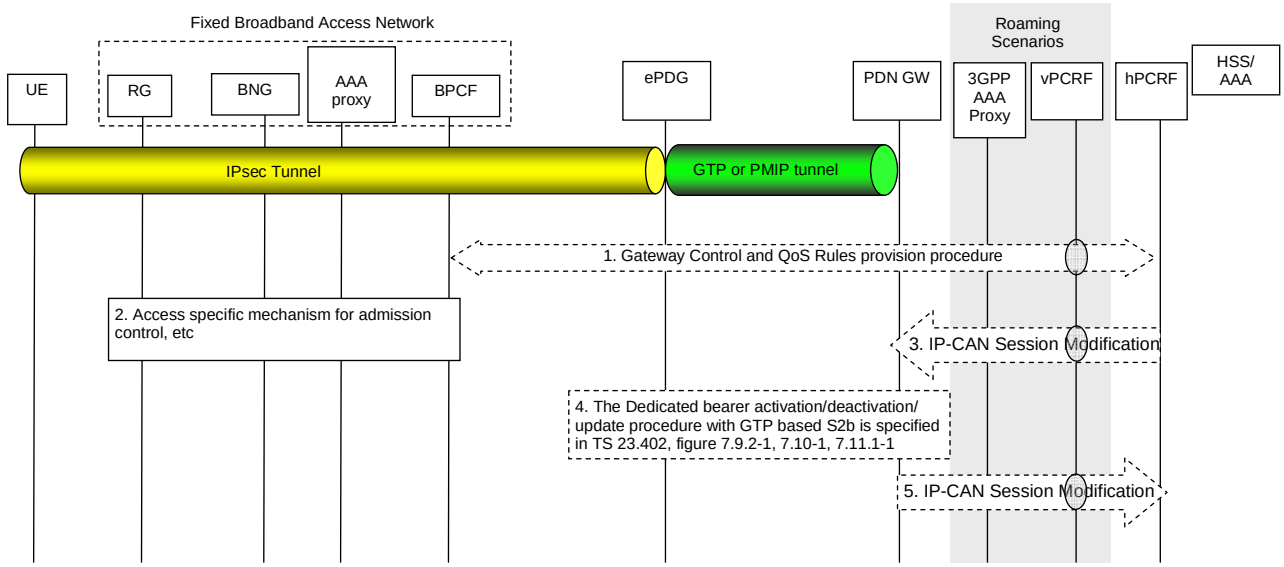

Figure 7.6-1: Network-initiated dynamic policy control procedure

If dynamic policy provisioning over S9a is not deployed, the optional step 1 does not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

1. The PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case) initiates the Gateway Control and QoS Rules Provision Procedure with the BPCF over S9a as specified in TS 23.203 [4]. In roaming scenario, the H-PCRF will initiate the procedure over S9 towards the V-PCRF and the V-PCRF in turns initiates the procedure over S9a towards the BPCF.

2. The Fixed Broadband Access Network performs admission control based on the QoS rules provisioned to it, and establishes all necessary resources and configuration in the Fixed Broadband Access network. The details of this step are out of the scope of this specification.

3. The PCRF sends PCC Rules to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4].

4. The step only available when GTP S2b is used. P-GW initiates GTP bearer activation/deactivation/update procedure as defined in TS 23 402, figure 7.9.2-1, 7.10-1, 7.11.1-1.

5. If the dynamic policy control procedure was triggered by a PCC Rules Provision message from the PCRF, the PDN GW replies with a provisioning acknowledgement message to the PCRF and later informs the PCRF whether the requested PCC Rules could be enforced after the completion of IP CAN bearer signalling.

7.7 Network-Initiated Dynamic PCC for NS-WLAN offloaded traffic

This procedure is applicable if the UE accesses via a Fixed Broadband Access network, traffic is offloaded by the BNG where dynamic PCC is deployed. The purpose of the procedures is to provision PCC Rules over S9a for offloaded traffic in the Fixed Broadband Access. The Fixed Broadband Access is able to perform admission control and to provision policy rules in the BNG for the purpose to identify traffic based on the UE's local IP address in order to enforce QoS.

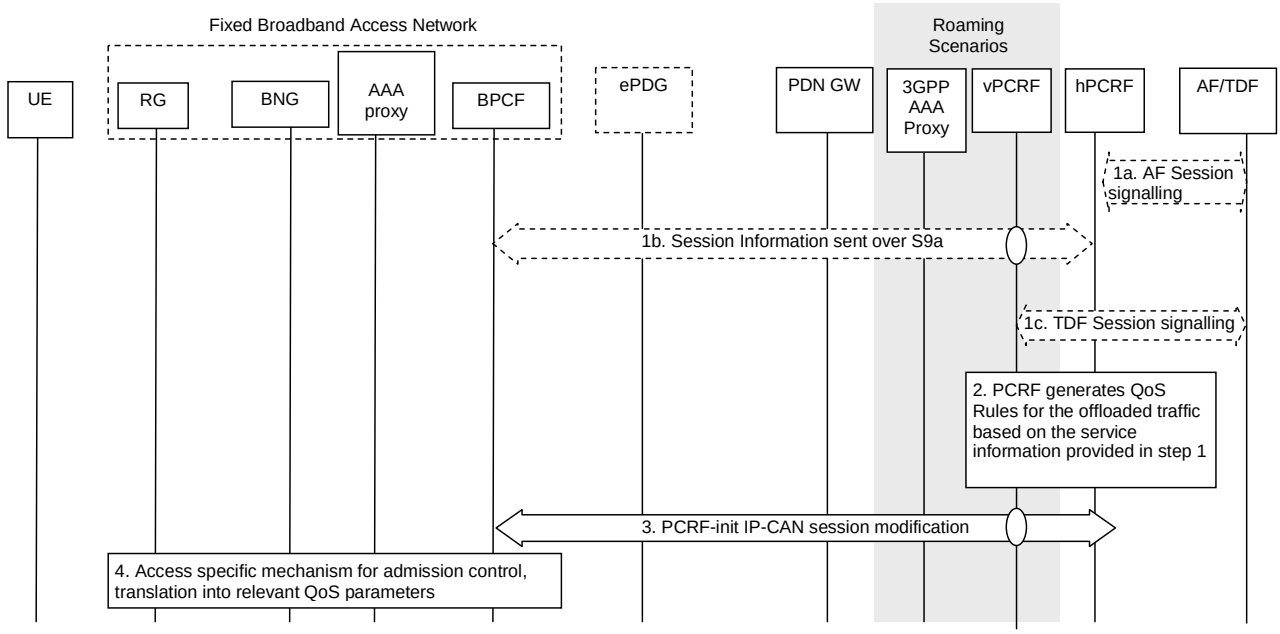

Figure 7.7-1: Network-initiated dynamic policy control procedure for offloaded traffic

1. This procedure only applies if dynamic policy provisioning over S9a is deployed. Steps 1a, 1b and 1c are corresponding to architecture scenarios A, B and C and all of them are optional.

   1a. For variant A, the service information is received by PCRF (non-roaming case) or H-PCRF(roaming case) over Rx interface.

   1b. For variant B ,service information for a 3GPP UE identified by the UE's local IP address or the IMSI is received by BPCF which will then sent it over S9a to the PCRF (non-roaming case), or to V-PCRF and the V-PCRF in turns forward them to the H-PCRF(roaming case).

   1c. For variant C, the service information is received by the PCRF (non-roaming case) or V-PCRF (roaming case) over Sd interface.

2. PCRF generates PCC Rules for the offloaded traffic based on the service information provided in step 1.

3. Triggered by step 2. The PCRF (for non-roaming case) and the V-PCRF (for roaming case) initiates the PCRF-initiated IP-CAN session modification procedure with the BPCF over S9a to provision PCC Rules for the UE's local IP address. In roaming scenario, the H-PCRF will initiate the procedure over S9 towards the V-PCRF which in turns initiates the procedure over S9a towards the BPCF.

4. The Fixed Broadband Access Network performs admission control based on the provisioned PCC Rules, and establishes all necessary resources and configuration in the Fixed Broadband Access network. The details of this step are out of the scope of this specification.

7.8 PDN GW initiated Resource Allocation Deactivation

This procedure is applicable if the UE accesses a Fixed Broadband Access network with GTPv2 or PMIPv6 based S2b interface. And the PDN GW initiated the resource releasing procedure, for example, due to IP-CAN session modification requests from the PCRF or due to handover from Fixed Broadband Access network to 3GPP. When it is performed due to a handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

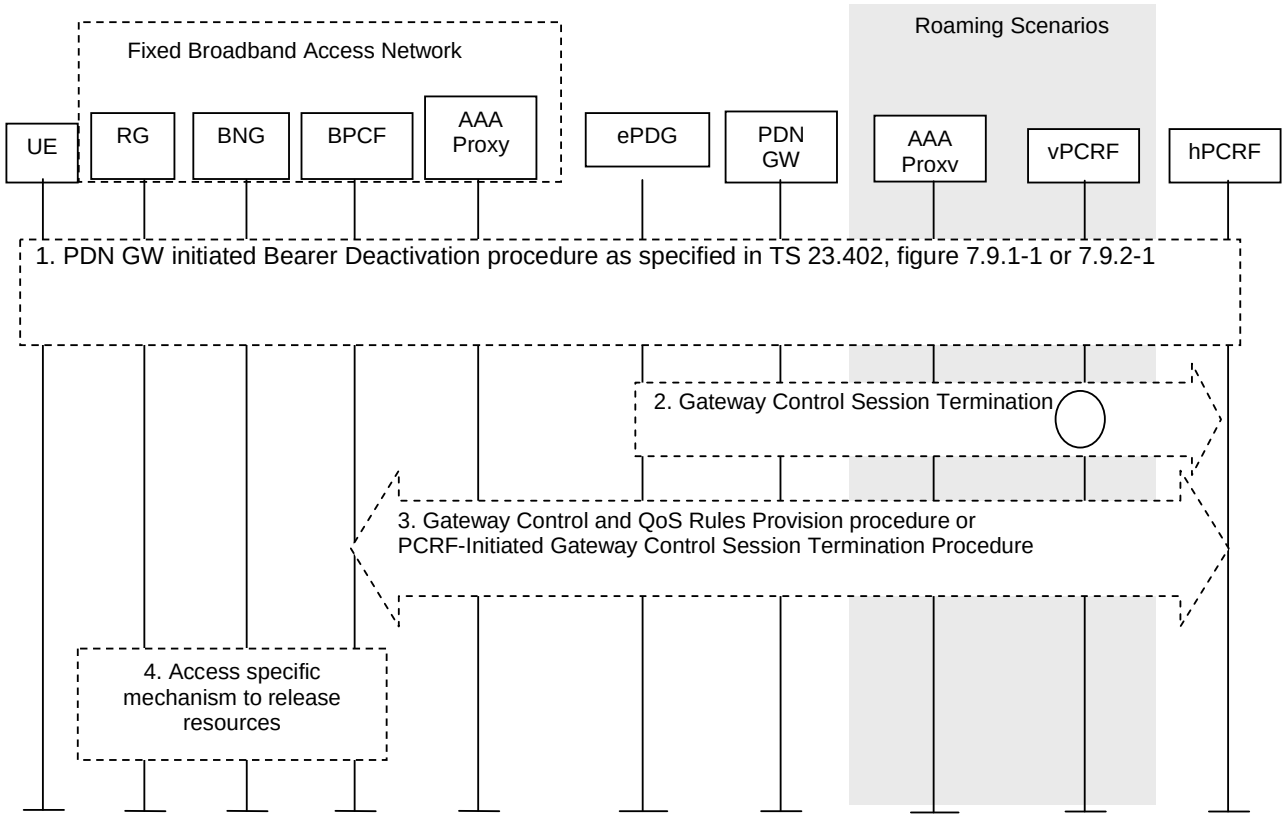

Figure 7.8-1: PDN GW Initiated Bearer Deactivation

NOTE 1: In the roaming case, the Step 2 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 2 and 3 do not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

Step 2 is only applicable when S2b PMIPv6 is used.

1. The description of the step is the same as it is in TS 23 402 [3], clause 7.9.1 or 7.9.2 with following exceptions:

   - The step 4 in clause 7.9.1 or step 3b in clause 7.9.2 is not executed.

2. Triggered by the IPSec tunnel termination, the ePDG terminates the Gxb* session. This step is only applicable when S2b PMIPv6 is used and Gxb* was used to trigger initiation of the S9a session from PCRF. This step may occur at any time.

NOTE 2: Step 2 may occur before or after steps 3-5. Step 2 does not trigger step 3.

3. Triggered by step 1, the PCRF (for non-roaming case) and the V-PCRF (for the home routed and visited access roaming case) executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE over Fixed Broadband Access, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF. In roaming scenario, for the case when GTP is used on S2b, the H-PCRF will initiate the procedure over S9 towards the V-PCRF and the V-PCRF in turns initiates the procedure over S9a towards the BPCF.

4. The resources may be released in the Fixed Broadband Access, according to an access specific release mechanism. The details of this step are out of the scope of this specification.

7.9 Handover from 3GPP Access to Fixed Broadband Access with GTP or PMIPv6 on S2b

This clause shows the combined call flow for a handover from 3GPP Access with GTPv2 or PMIPv6 based S5/S8 interface to a Fixed Broadband Access network via GTPv2 or PMIPv6 based S2b interface. In addition, the procedures

for the IP session establishment for NS-WLAN offload using the Fixed Broadband Access network are also integrated into the combined procedures.

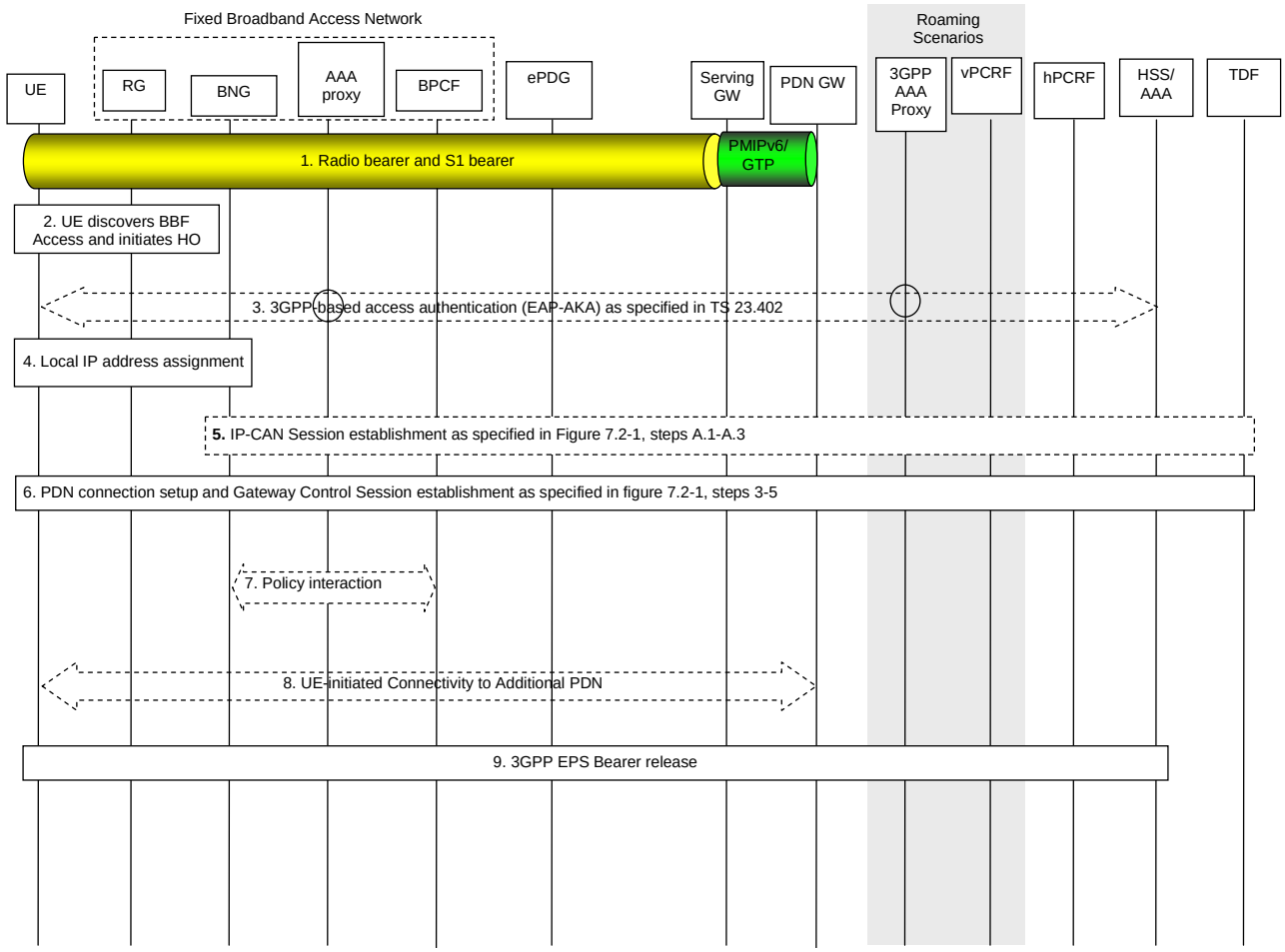

Figure 7.9-1: Handover from 3GPP Access to Fixed Broadband Access

If dynamic policy provisioning over S9a is not deployed, the optional steps 5, 7 and 8 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

For connectivity to multiple PDNs, step 8 shall be repeated for each PDN the UE is connected to. Step 8 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in TS 23 402 [3] clause 8.1.

Handover is only applicable to the EPC-routed PDN connections. For the NS-WLAN offloaded traffic, a new IP session in fixed broadband access network will be established.

1-2. The description of these steps are is same as for steps 1-2 in TS 23 402 [3], clause 8.2.3.

3-4. The description of these steps is the same as for steps 1-2 in Figure 7.2-1.

5. This step describes PCC signalling to provision policies for offloaded traffic and are only triggered when the BPCF receives the IMSI and the allocated UE local IP address using Fixed Broadband Access procedures. The description of this step is the same as for steps 3-5 in Figure 7.2-1.

6. The description of PDN Connection setup and Gateway Control Session setup is the same as for steps 3-5 in Figure 7.2-1 with following additions:

   - Step 3 in Figure 7.2-1 is mandatory when performing handover from E-UTRAN to Fixed Broadband Access.

   - If the UE supports IP address preservation during the handover, the UE shall include its address (IPv4 address or IPv6 prefix /address or both) allocated when it's attached to 3GPP Access into the CFG_Request sent to the ePDG during IKEv2 message exchange. The ePDG shall include the received UE address in the

Create Session Request message or Proxy Binding Request message, and set the HO flag when sending to the PDN GW.

7. The description of this step is the same as for step 6 in Figure 7.2-1.

8. For connectivity to multiple PDNs, the UE establishes connectivity to each PDN that is being transferred from 3GPP access, besides the PDN connection that was established in the steps 5-6, by executing the UE-initiated Connectivity to Additional PDN procedure specified in clause 7.5.

9. The description of this step is the same as for steps 11 in TS 23 402 [3], clause 8.2.3.

7.10 Handover from Fixed broadband Access with GTP or PMIPv6 on S2b to 3GPP Access

This clause shows the combined call flows for a handover from Fixed Broadband Access network via GTPv2 or PMIPv6 based S2b interface to a 3GPP Access (GERAN, UTRAN, E-UTRAN) with GTPv2 or PMIPv6 based S5/S8 interface.

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the TAU with MME and Serving GW change procedure defined in TS 23.401 [2], clause 5.3.3.1 as well as Inter-eNodeB Handover with CN Node Relocation described in TS 23.401 [2], clause 5.5.1.2.

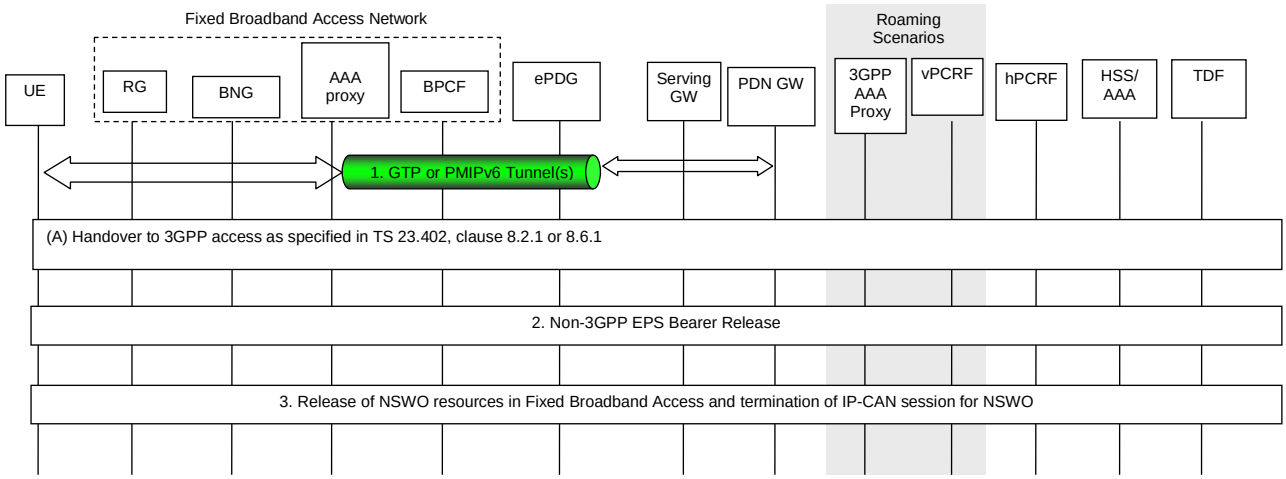

Figure 7.10-1: Handover from Fixed Broadband Access to 3GPP Access

For connectivity to multiple PDNs the same behaviour as described in clause 8.2.1.1 also applies to this procedure.

1. The UE uses Fixed broadband Access and is being served by PDN GW.

A. This step is the same as defined in TS 23 402, clause:

- 8.2.1.1, step 2 to 17 for HO from PMIPv6 on S2b to E-UTRAN with GTP on S5/S8
- 8.2.1.2, step 2 to 18 for HO from PMIPv6 on S2b to E-UTRAN with PMIPv6 on S5/S8
- 8.2.1.3, step 2 to 16 for HO from PMIPv6 on S2b to UTRAN/GERAN with GTP-based S5/S8
- 8.2.1.4, step 2 to 18 for HO from PMIPv6 on S2b to UTRAN/GERAN with PMIPv6 on S5/S8
- 8.6.1.1, steps in (C) for HO from GTP on S2b to E-UTRAN with GTP on S5/S8
- 8.6.1.2, steps in (D) for HO from GTP on S2b to UTRAN/GERAN with GTP on S5/S8

2. The PDN GW shall initiate resource allocation deactivation procedure in the Fixed Broadband Access as defined in clause 7.7

3. If the NS-WLAN offloaded connection is released (e.g. if the UE moves out of WLAN coverage), the Fixed Broadband Access executes the access specific resource release procedure and initiates termination of the IP-CAN session for NS-WLAN offloaded traffic as described in steps 4-6 in clause 7.3

7.11 IPSec tunnel modified

This clause is related to the case where the IPSec tunnel between the UE and the ePDG has been modified due to the UE initiated IPSec tunnel update procedure, or the UE local IP address updating. The IPSec tunnel modification procedure is assumed that GTP based or PMIPv6 based S2b is used. This procedure is only applicable if MOBIKE is supported by the UE.

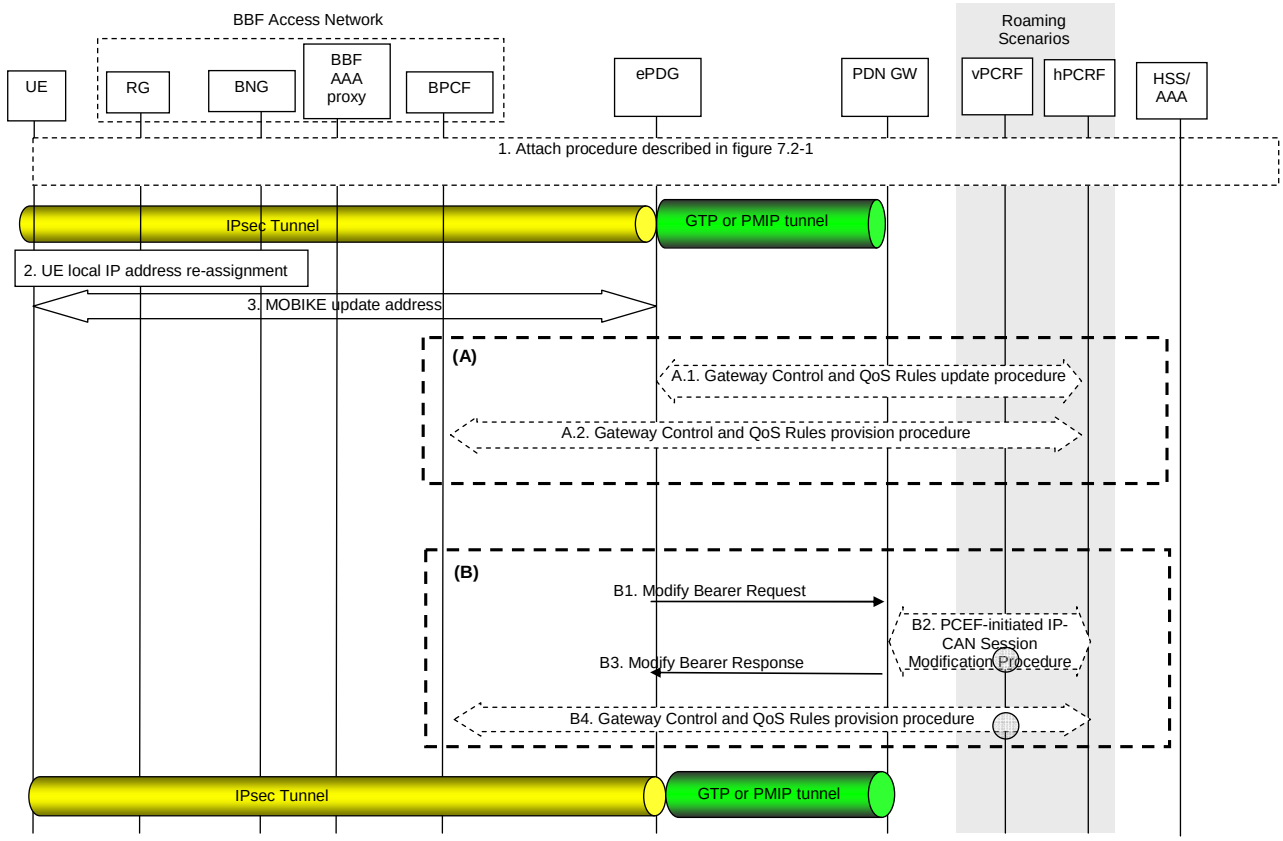

Figure 7.11-1: IPSec tunnel modified

If dynamic policy provisioning over S9a is not deployed, the optional step A2 and B4 do not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

1. UE attaches to EPC from BBF access network via ePDG, as described in figure 7.2-1. The IPSec tunnel is established between ePDG and UE; the PMIPv6 or GTP tunnel is established between the PDN GW and ePDG

2. The BBF Access Network may assign a new local IP address to the UE.

3. UE initiated IPSec tunnel update procedure, which may be as a result of UE IP address for IPSec tunnel expired or released. MOBIKE update address message exchanges. And optionally, MOBIKE address verification, initiated by ePDG, is send to UE as described in MOBIKE [18].

A. These steps are only applicable when S2b PMIPv6 is used.

   A.1. The ePDG initiates Gxb* session modification with the PCRF. The ePDG includes the UE local IP address and optionally the UDP source port number (if NAT is detected) in the message to the PCRF.

   A2. Triggered by step A2, the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case) initiates the Gateway Control and QoS Rules Provision Procedure with the BPCF over S9a as specified in TS 23.203 [4].

B. These steps are only applicable when S2b GTP is used.

B1. The ePDG sends Modify bearer request message with the UE local IP address and optionally the UDP source port number (if NAT is detected) to P-GW.

B2. The PCEF initiated IP-CAN session modification procedure is triggered.

B3. The P-GW responses with Modify Bearer Response message to the ePDG.

B4. Triggered by the PCC Rule provisioning to the PCEF, the PCRF (for non-roaming case) and the V-PCRF (for the home routed and visited access roaming case) initiates the Gateway Control and QoS Rules Provision Procedure with the BPCF over S9a as specified in TS 23.203 [4]. In roaming scenario, the H-PCRF will initiate the procedure over S9 towards the V-PCRF and the V-PCRF in turns initiates the procedure over S9a towards the BPCF.

8 Functional Description and Procedures for Fixed Broadband Access network over S2c

8.1 Introduction

The description for the PCC procedures applicable for S2c untrusted and trusted scenarios including the NS-WLAN offloaded traffic. The IP session for the UE in Fixed Broadband Access is handled as an IP-CAN session by the PCRF. For EPC-routed traffic, the IP-CAN session for the PDN Connection in the PDN GW is created via Gx procedures. In addition a Gateway Control Session is established between the BPCF and the PCRF corresponding to the EPC-routed IP-CAN session in the PCRF.

NOTE: It is up to stage 3 to optimize S9a procedures for Non-Seamless WLAN offloaded traffic and EPC routed traffic handled by the same PCRF.

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure.

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.
- In the non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

8.2 Procedures for trusted Fixed Broadband Access network over S2c

8.2.1 Initial Attach with DSMIPv6 on S2c to trusted Fixed Broadband Access

This clause specifies the additional procedures at the UE's initial attachment to a Fixed Broadband Access which is considered a trusted access to EPC, for the UE to establish the first PDN connection over the Fixed Broadband Access with S2c, and/or for the UE to have offloaded traffic via Fixed Broadband Access.

This procedure establishes a session between the BPCF and the PCRF to provision policy decisions for NS-WLAN offloaded traffic and/or to provision policy decisions for EPC routed traffic.

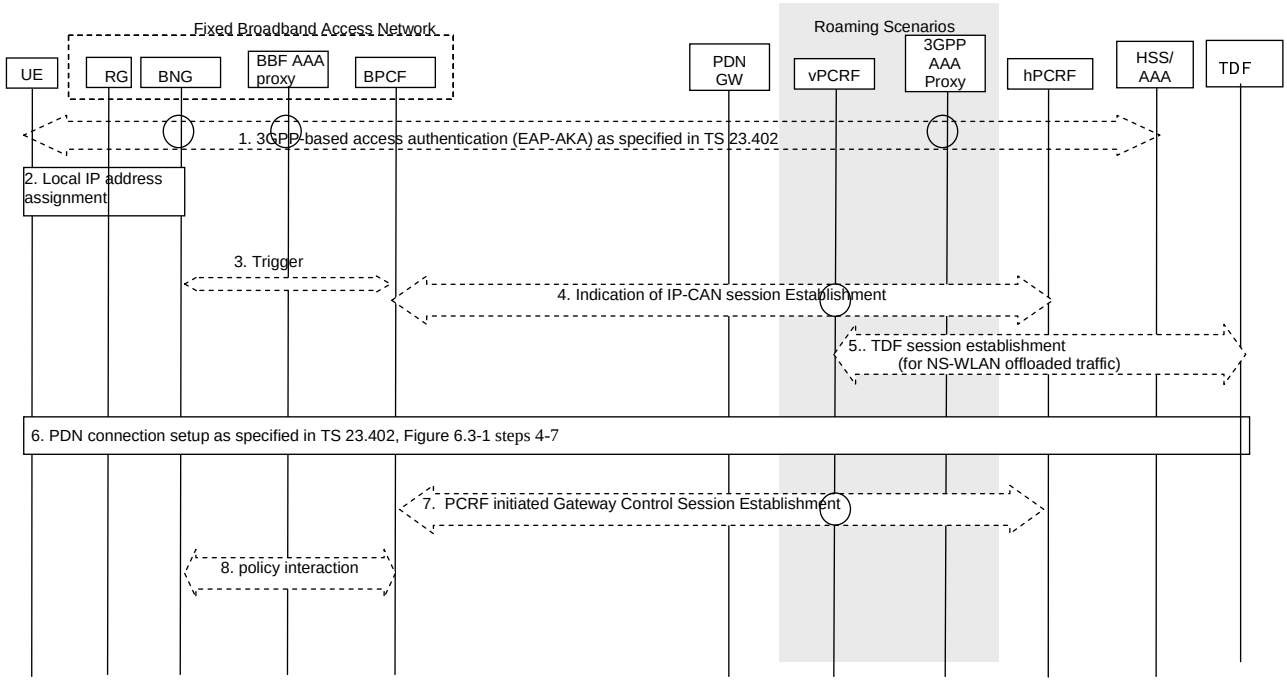

Figure 8.2.1-1: Initial attachment with DSMIPv6 when S2c is used for roaming, non-roaming and LBO

If dynamic policy provisioning over S9a is not deployed, the optional steps 3,4, 5, 7 and 8 do not occur. Instead, the Fixed Broadband Access Network may employ local policies.

1. The description of this step is the same as clause 7.2, step 1.
2. The description of this step is the same as clause 7.2 step 2. The UE local IP address is used as CoA in S2c signalling.

The steps in 3, 4 and 5 describe PCC Signalling for NS-WLAN offloaded traffic, the triggered is described in clause 7.2.

3. The description of this step is the same as step 3 in clause 7.2.
4. This description of this step is the same as step 4 in clause 7.2.
5. This description of this step is the same as step 5 in clause 7.2.
6. The description of this step is the same as for steps 4-7 in TS 23 402 [3], clause 6.3, with the following information: The UE local IP address (i.e. CoA) and optionally UDP source port number of the DSMIPv6 binding update signalling (if NAT is detected) are forwarded to the PCRF in step 6 of TS 23 402 [3], clause 6.3 (i.e. IP-CAN session establishment procedure).

The step in 7 PCC signalling to provision policies for EPC routed traffic.

7. The description of this step is the same as step 8 in clause 7.2 for GTP case. The UE local IP address is used as CoA in S2c signalling.
8. The description of this step is the same as step 9 in clause 7.2.

8.2.2 UE-initiated Detach Procedure and UE-Requested PDN Disconnection with DSMIPv6 on S2c in trusted Fixed Broadband Access

The procedure in this clause applies to UE-initiated detach procedures (e.g. triggered by power-off), and to the UE-requested PDN disconnection procedure.

In the case when UE has multiple PDN connections, this detach procedure shall be repeated for each PDN connection.

This clause also covers the termination of the IP-CAN session for UE's offloaded traffic initiated by the Fixed Broadband Access network.

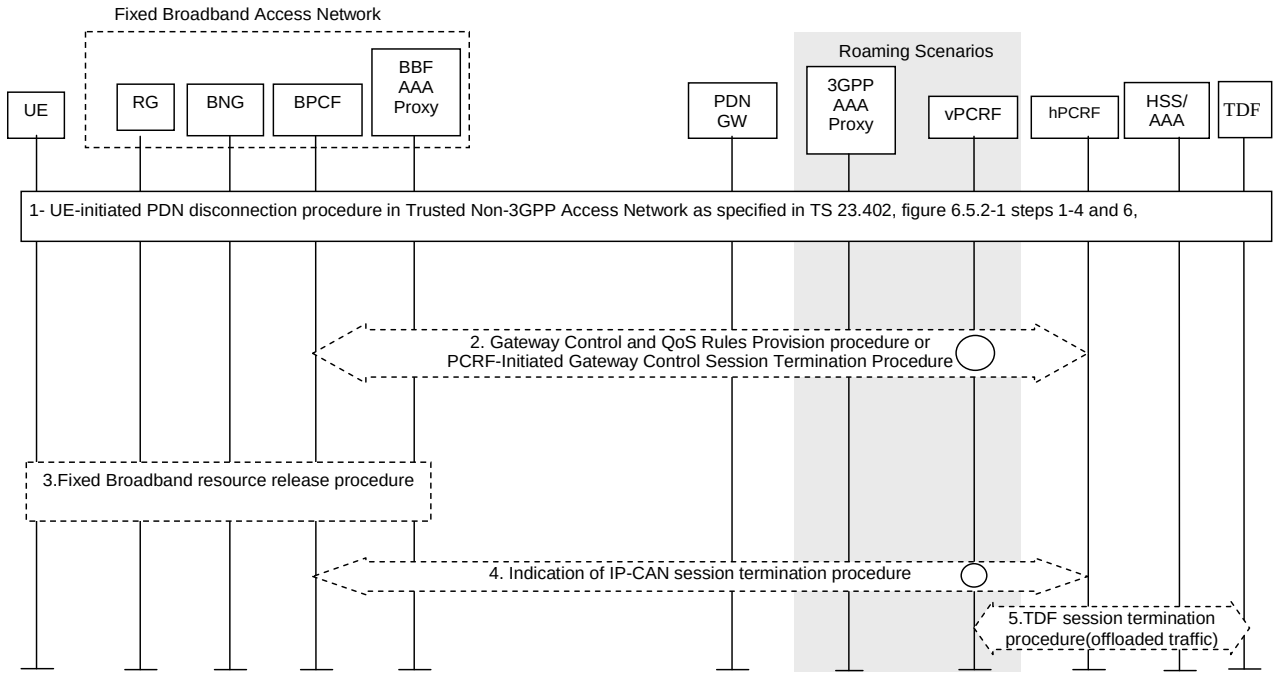

Figure 8.2.2-1: UE-initiated detach procedure with DSMIPv6 on trusted s2c

If dynamic policy provisioning is not deployed, the optional steps 2, 4 and 5 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The descriptions of these steps are the same as UE-initiated PDN disconnection procedure in trusted non-3GPP access network as specified in TS 23 402 [3], figure 6.5.2-1 steps 1-4 and 6.
2. Triggered by the IP-CAN session termination, if this is not the last PDN connection for the UE, the PCRF executes a Gateway Control and QoS Rules Provision procedure; otherwise, if this is the last PDN connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF over S9a.
3. The description of this step is the same as clause 7.3 step 4.
4. The description of this step is the same as clause 7.3 step 5.
5. The description of this step is the same as clause 7.3 step 6.

8.2.3 HSS-initiated Detach Procedure with DSMIPv6 on S2c in trusted Fixed Broadband Access

The procedure in this clause applies to Detach Procedures, initiated by HSS.

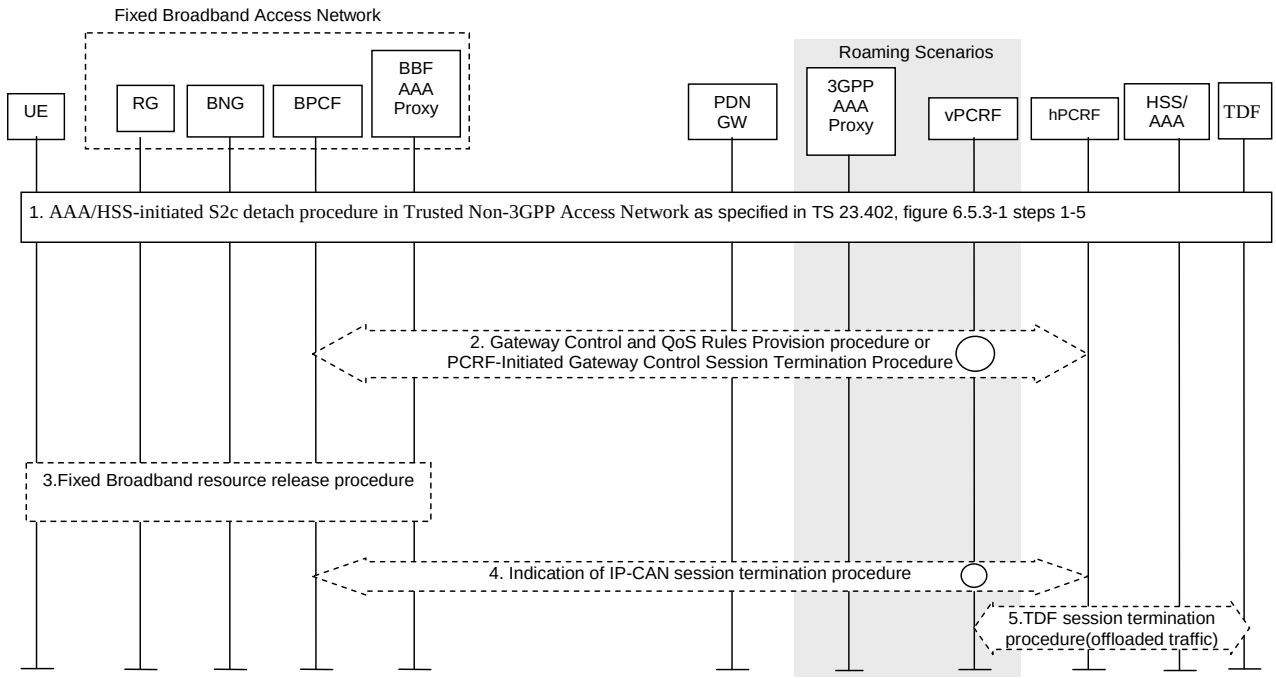

Figure 8.2.3-1: HSS-initiated detach procedure with DSMIPv6 on trusted s2c

If dynamic policy provisioning over S9a is not deployed, the optional step 2, 4 and 5 do not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

1. The description of these steps are the same as for steps 1-5 in TS 23 402 [3], clause 6.5.3.
2. Triggered by the IP-CAN session termination, the PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF over S9a.
3. The description of this step is the same as clause 7.3 step 4.
4. The description of this step is the same as clause 7.3 step 5.
5. The description of this step is the same as clause 7.3 step 6.

8.2.4 PDN GW-initiated PDN disconnection Procedure with DSMIPv6 on S2c in trusted Fixed Broadband Access

The procedure in this clause applies to PDN disconnection procedure initiated by PDN GW.

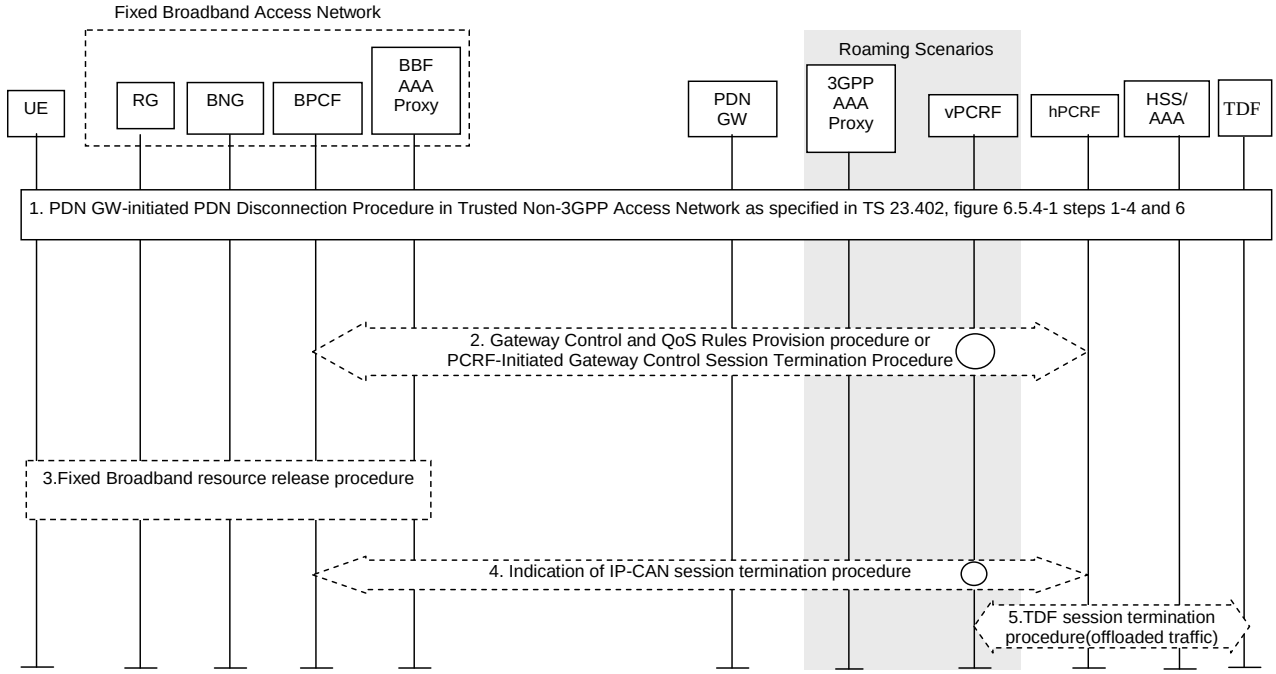

Figure 8.2.4-1: PDN GW-initiated PDN disconnection procedure with DSMIPv6 on trusted S2c

If dynamic policy provisioning over S9a is not deployed, the optional step 2, 4 and 5 do not occur. Instead, the Fixed Broadband Access network may employ Fixed Broadband Access local policies.

1. The description of these steps are the same as for steps 1-4 in TS 23 402 [3], clause 6.5.4.
2. Triggered by the IP-CAN session termination, the PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF over S9a.
3. The description of this step is the same as clause 7.3 step 4.
4. The description of this step is the same as clause 7.3 step 5.
5. The description of this step is the same as clause 7.3 step 6.

8.2.5 E-UTRAN to Trusted Fixed Broadband Access Handover with DSMIPv6 on S2c

This clause shows the combined call flow for a handover when a UE moves from an E-UTRAN to a trusted Fixed Broadband Access network. In addition, the procedures for the IP session establishment for NS-WLAN offload using the Fixed Broadband Access network are also integrated into the combined procedures.

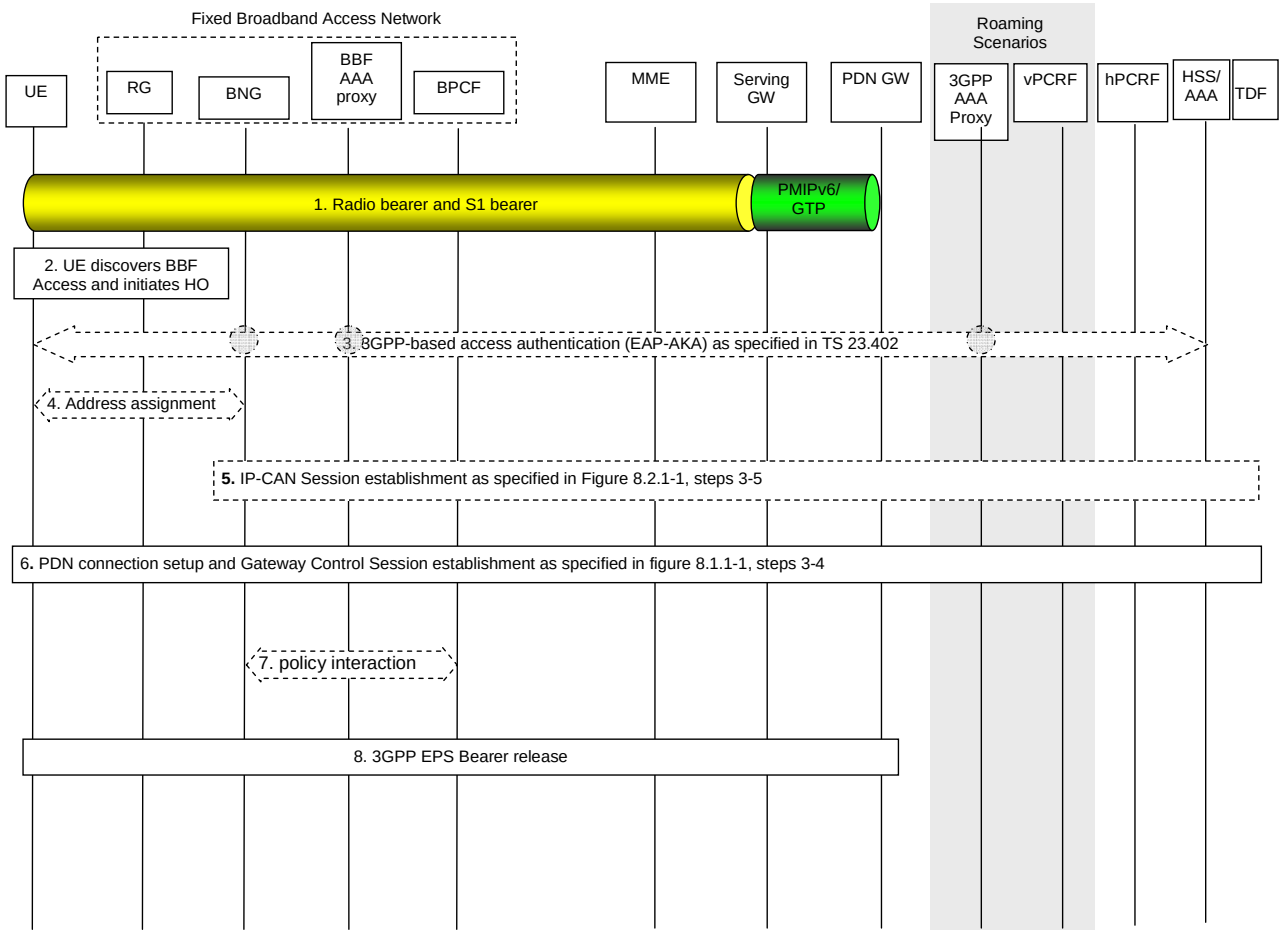

Figure 8.2.5-1: E-UTRAN to Trusted Fixed Broadband Access Handover with DSMIPv6 on s2c

Both the roaming and non-roaming scenarios are depicted in the figure.

If dynamic policy provisioning over S9a is not deployed, the optional steps 5 and 7 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

Handover is only applicable to the EPC-routed PDN connections. For the NS-WLAN offloaded traffic, a new IP session in fixed broadband access network will be established.

For connectivity to multiple PDNs, steps B.1 to 6 shall be repeated for each PDN.

1-2. The description of these steps is the same as for steps 1-2 in TS 23 402 [3], clause 8.4.2.1.

3-4. The description of these steps is the same as for steps 1-2 in Figure 8.2.1-1.

5. This steps describe PCC signalling to provision policies for offloaded traffic and are only triggered when the BPCF receives the IMSI and the allocated UE local IP address using Fixed Broadband Access procedures. The description of this step is the same as for steps 3-5 in Figure 8.2.1-1.

6. The description of PDN Connection setup and Gateway Control Session setup are the same as for step 3-4 in Figure 8.2.1-1 with following addition:

   - Step 4 in Figure 8.2.1-1 is mandatory when performing handover from E-UTRAN to Fixed Broadband Access.

7. The description of this step is the same as for step 5 in Figure 8.2.1-1.

8. The description of this step is the same as for step 12 in TS 23 402 [3], clause 8.4.2.

8.2.6 Handover from Trusted Fixed Broadband Access with DSMIPv6 over S2c to 3GPP Access

In this scenario, the session starts in a trusted Fixed Broadband Access system using DSMIPv6 over S2c and subsequently, the session hands over to a 3GPP access system.

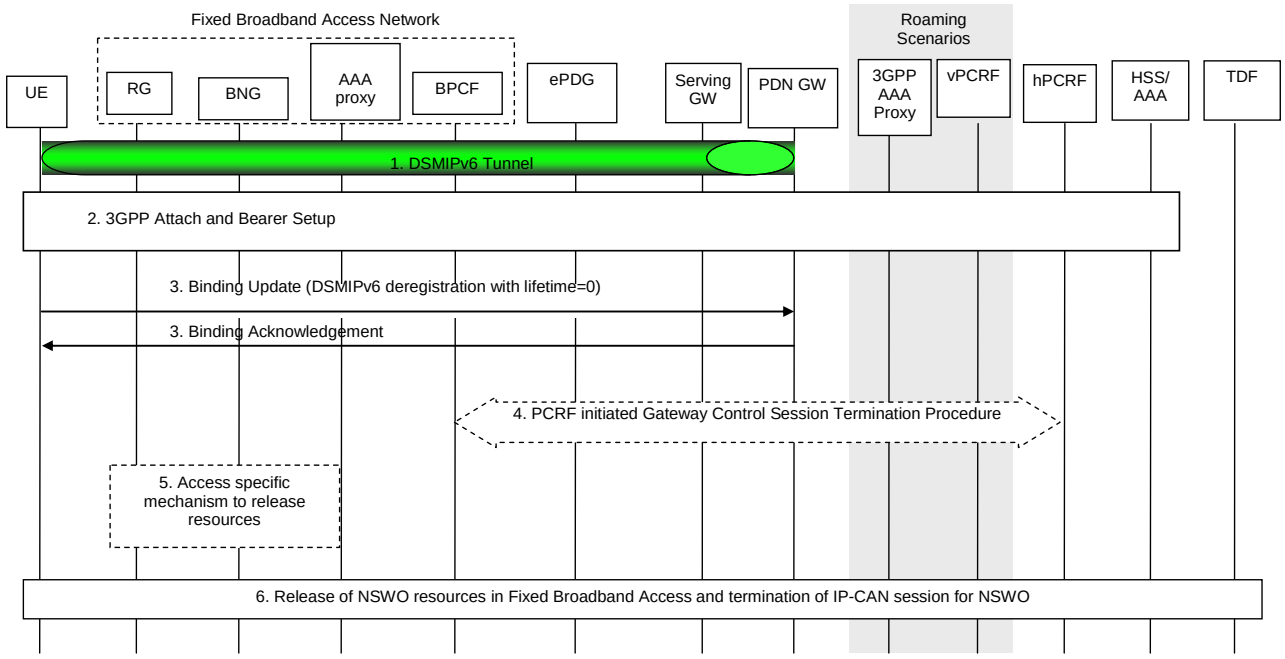

Figure 8.2.6-1: Fixed Broadband Access with S2c (DSMIPv6) to 3GPP access handover

If dynamic policy provisioning over S9a is not deployed, the optional step 4 does not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The UE uses a Fixed Broadband Access system. It has a DSMIPv6 session with the PDN GW.

2-3. The description of these steps is the same as for step 2-3 in TS 23 402, clause 8.4.1.

4. The PCRF (for non-roaming case) and the V-PCRF (for the home routed and visited access roaming case) executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE over Fixed Broadband Access, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF. In roaming scenario, for the case when GTP is used on S2b, the H-PCRF will initiate the procedure over S9 towards the V-PCRF and the V-PCRF in turns initiates the procedure over S9a towards the BPCF. This procedure is triggered by the PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF, occurring as a result of step 2.

5. The resources may be released in the Fixed Broadband Access, according to an access specific release mechanism. The details of this step are out of the scope of this specification.

6. If the NS-WLAN offloaded connection is released (e.g. if the UE moves out of WLAN coverage), the Fixed Broadband Access executes the access specific resource release procedure and initiates termination of the IP-CAN session for NS-WLAN offloaded traffic as described in steps 3-5 in clause 8.1.2.

8.2.7 Network-Initiated Dynamic PCC for DSMIPV6 on S2c when accessing trusted Fixed Broadband Access for EPC-routed Traffic

This procedure is applicable if the UE accesses over a Fixed Broadband Access network which is considered trusted.

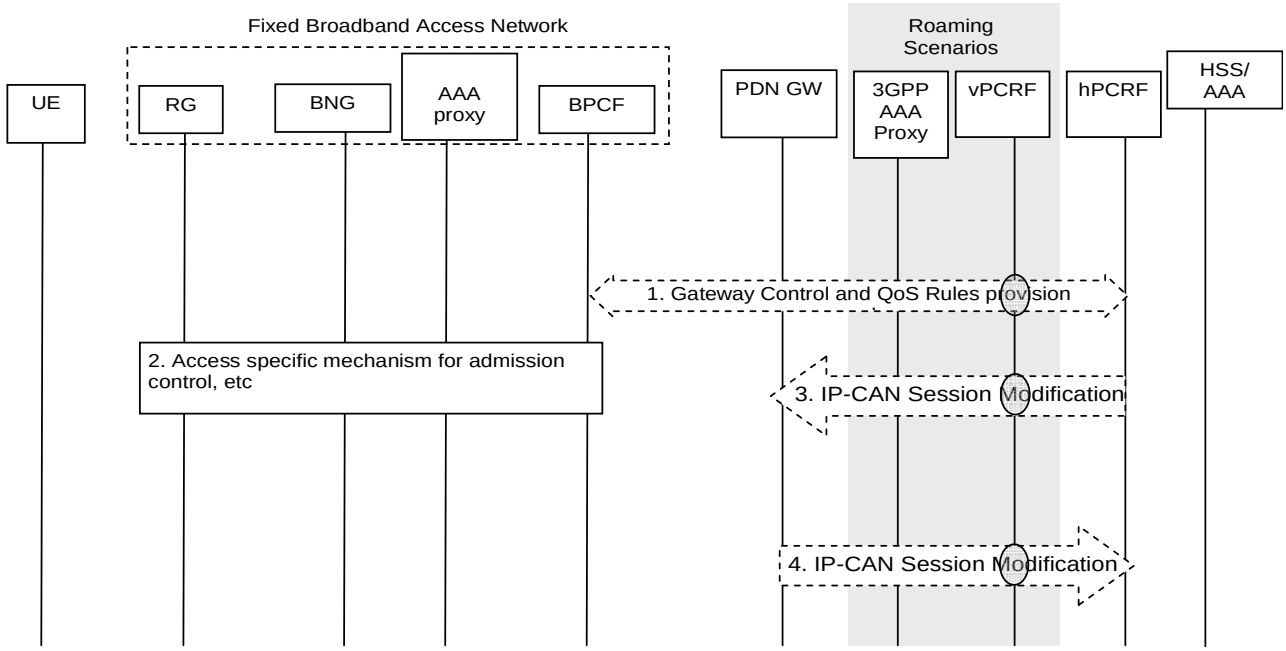

Figure 8.2.7-1: Network-initiated dynamic policy control procedure in Trusted BBF IP Access for DSMIPv6 on S2c

This procedure concerns both the non-roaming (as Figure 4.2.2-3) and roaming case (as Figure 4.2.3-3). In the roaming case, the vPCRF in the VPLMN forwards messages between the BPCF and the hPCRF in the HPLMN. In the case of Local Breakout (as Figure 4.2.3-6), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures, step 1 and 3, only occur if dynamic policy provisioning is deployed. Otherwise Fixed Broadband Access network may employ BBF local policies.

1-3. The description of these steps is the same as for steps 1-3 in clause 7.6.

4. The PCEF acknowledges the provisioning of PCC Rules in the PCEF. For details please refer to TS 23.203 [4].

8.2.8 Network-Initiated Dynamic PCC for DSMIPV6 on S2c when accessing trusted Fixed Broadband Access for NS-WLAN offloaded Traffic

The information flow of "Network-Initiated Dynamic PCC for DSMIPV6 on S2c when accessing trusted Fixed Broadband Access for offloaded Traffic" is same as S2b case, which is defined in clause 7.7.

8.2.9 UE-Initiated Connectivity to Additional PDN with DSMIPv6 on S2c over trusted Fixed Broadband Access

This clause is related to the case when the UE has an established PDN connection and wishes to establish one or more additional PDN connections.

There can be more than one PDN connection per APN if the PDN GW supports that feature.

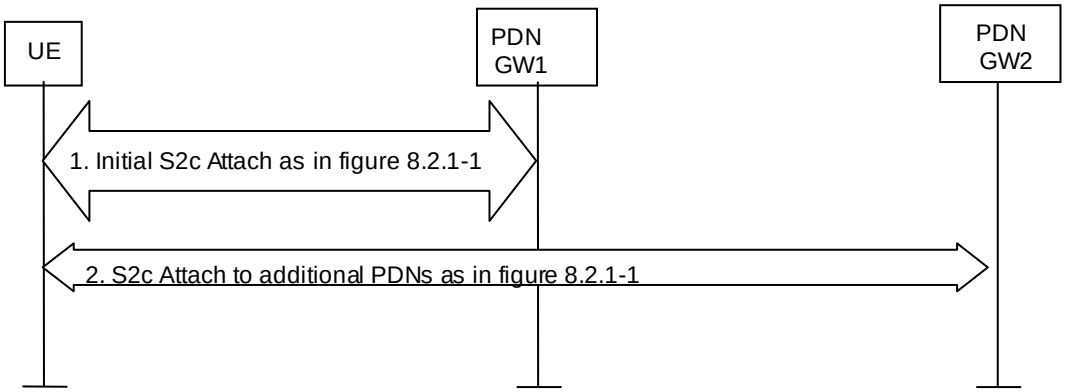

Figure 8.2.9-1: UE-Initiated connectivity to additional PDN from Trusted Non-3GPP IP Access with DSMIPv6 on S2c

1. The UE has performed the Initial S2c attach procedure as defined in clause 8.2.1 and has an established PDN connection.

2. The UE repeats the procedure steps 3-5 of clause 8.2.1, Figure 8.2.1-1 for each additional PDN the UE wants to connect to.

- In Step 7, if no Gateway Control session over S9a for this UE, then the PCRF initiates the Gateway Control Session Establishment procedure with the BPCF. Otherwise, the PCRF provide new QoS rules corresponding to the new PDN connection to the BPCF using the Gateway Control and QoS Rules Provisioning procedure.

8.2.10 Activation of enhanced security for S2c

This clause is related to the case that UE creates the child SA to protect the user plane traffic exchanged over the S2c tunnel when the UE is in a trusted Fixed Broadband access.

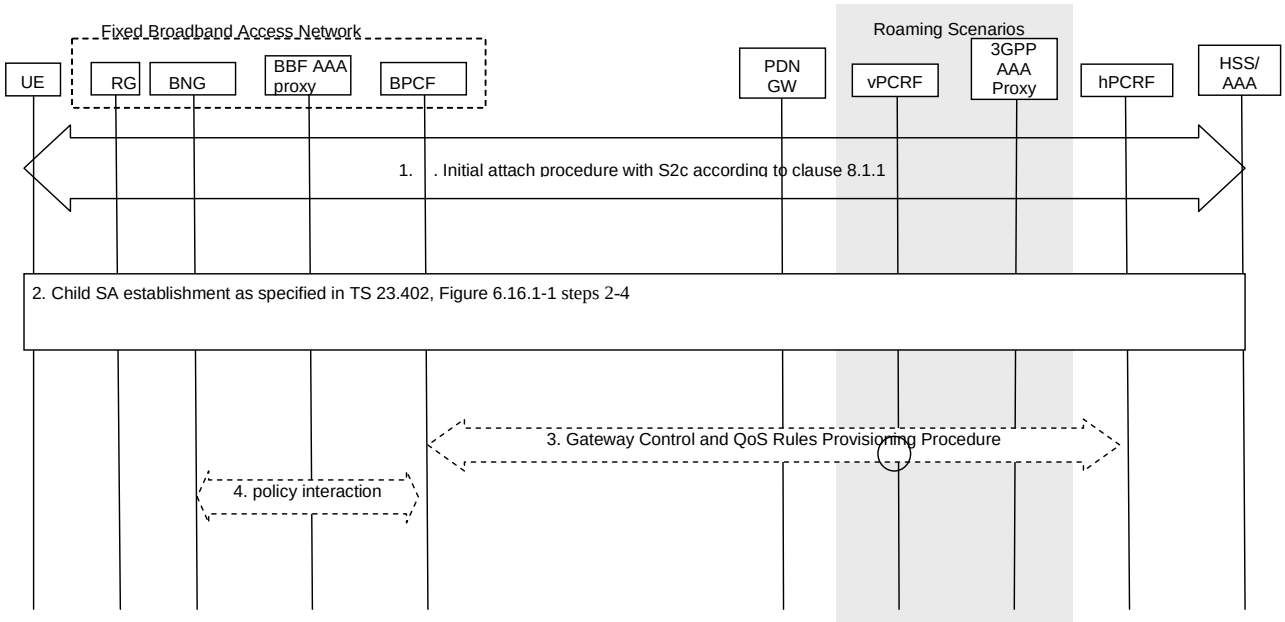

Figure 8.2.10-1 Activation of enhanced security for S2c

1. The UE has performed the Initial S2c attach procedure as defined in clause 8.2.1 and has an established PDN connection.

2. The UE repeats the procedure steps 2-4 of clause 6.16.1, Figure 6.16.1-1 to establish the child SA with the following additions: UDP source port number of IPSec tunnel as according to RFC 5996 is included in IP-CAN session modification.

3. The Gateway Control and QoS Rules provision procedure is initiated by the PCRF towards the BPCF as specified in TS 23.203 [4] Annex P, with the following additions: UDP source port number of IPSec tunnel as according to RFC 5996.

4. The BPCF may interact with the BNG, e.g. to download policies, as defined by Fixed Broadband Access Policy Framework specifications BBF TR-134 [11] and BBF TR-203 [6]. This step is out of 3GPP scope.

8.2.11 UE local IP address update on S2c over trusted Fixed Broadband Access

This clause is related to the case where the UE local IP address, e.g. the CoA in the DSMIP procedure, is updated.

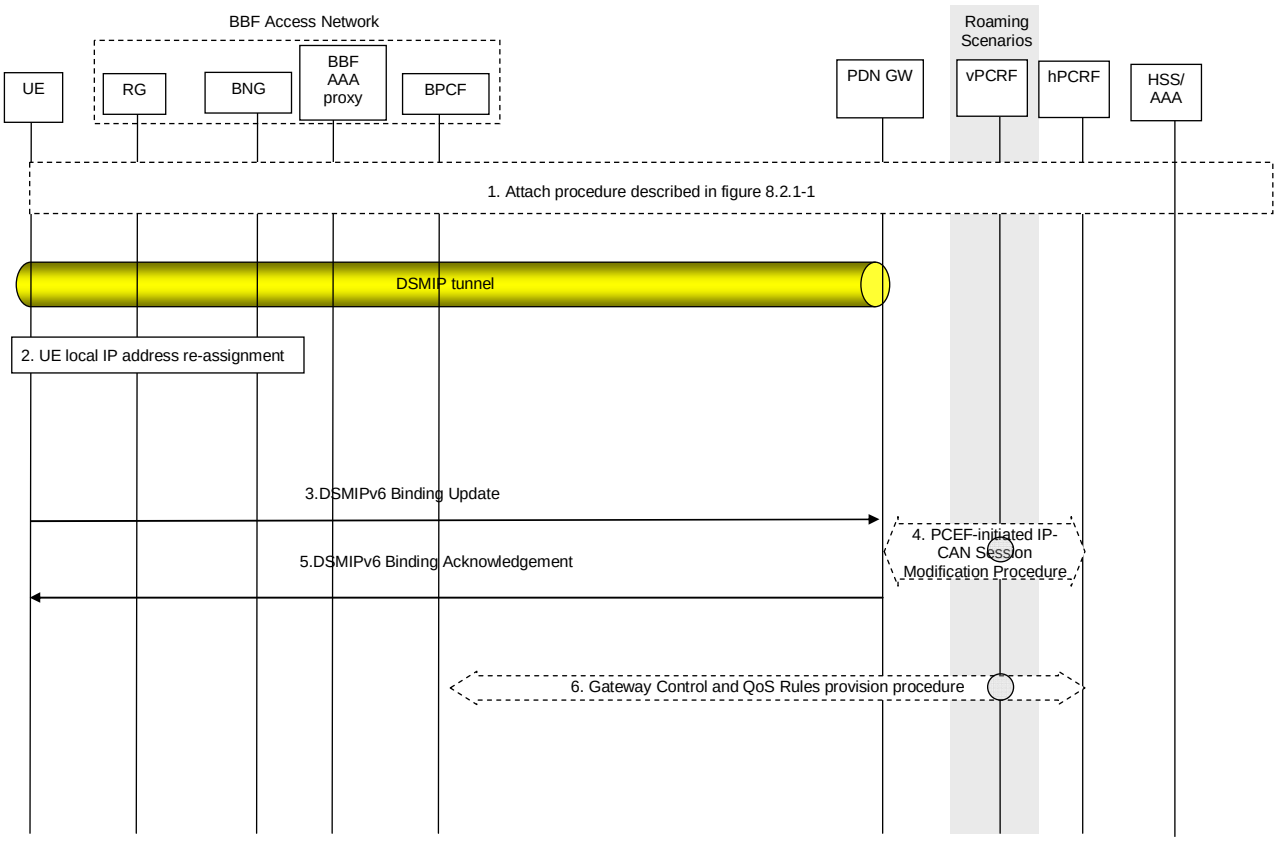

Figure 8.2.11-1: UE local IP address changes on S2c over trusted Fixed Broadband Access

If dynamic policy provisioning over S9a is not deployed, the optional step 4 and 6 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. UE attaches to EPC from BBF access network as described in clause 8.2.1. The IPSec tunnel and DSMIP tunnel are established between P-GW and UE.

2. The description of this step is the same as step 2 in clause 7.11.

3. Upon a change of the UE's CoA, the UE sends the DSMIPv6 Binding Update message to the P-GW. In this step the P-GW gets the updated UE local IP address (i.e. the UE's CoA if no NAT is deployed or the NATed CoA when NAT is deployed) and optionally the UDP source port number (if NAT is detected) of the DSMIPv6 binding update signalling.

4. The description of this step is the same as step B.2 in clause 7.11.

5. P-GW replies with the DSMIPv6 Binding Acknowledgement message to UE.

6. The description of this step is the same as step B.4 in clause 7.11.

8.3 Procedures for untrusted Fixed Broadband Access network over S2c

8.3.1 Initial Attach with DSMIPv6 on S2c to untrusted Fixed Broadband Access

This clause is related to the case when the UE attaches to a Fixed Broadband Access which is considered untrusted and S2c procedures are used when the UE establishes the first PDN connection over the Fixed Broadband Access with S2b, or when the UE has only the offloaded traffic via Fixed Broadband Access.

This procedure establishes a session between the BPCF and the PCRF to provision policy decisions for NS-WLAN offloaded traffic or to provision policy decisions for EPC routed traffic.

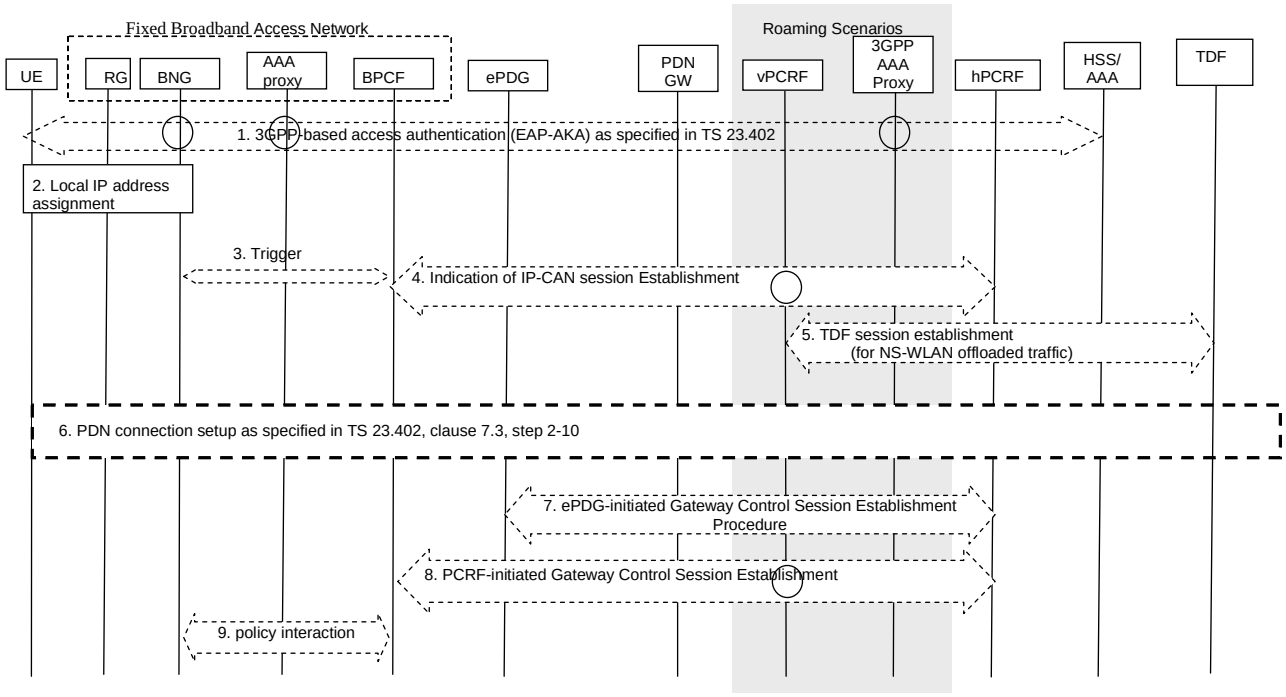

Figure 8.3.1-1: Initial attachment when S2c is used for roaming, non-roaming and LBO

NOTE: In the roaming case step 7 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 3, 4, 5, 7 and 8 do not occur.

1. The description of this step is the same as step 1 in clause 7.2.
2. The description of this step is the same as step 2 in clause 7.2.

The steps in 3, 4 and 5 describe PCC Signalling for NS-WLAN offloaded traffic, the trigger is described in clause 7.2.

3. The description of this step is the same as step 3 in clause 7.2.
4. This description of this step is the same as step 4 in clause 7.2.
5. This description of this step is the same as step 5 in clause 7.2.

Steps 6, 7 and 8 describe PCC signalling to provision policies for EPC routed traffic.

6. The description of the PDN connection setup procedure is the same as for steps 2-10 in TS 23 402 [3], clause 7.3
7. The description of this step is the same as step 7 in clause 7.2.
8. This description of this step is the same as step 8 in clause 7.2.

9. This description of this step is the same as step 9 in clause 7.2.

8.3.2 UE-initiated Detach Procedure and UE-Requested PDN Disconnection with DSMIPv6 on S2c in untrusted Fixed Broadband Access

The procedure in this clause applies to UE-initiated detach procedures (e.g. UE power-off), initiated by UE, and to the UE-requested PDN disconnection procedure. The UE can initiate the Detach procedure, e.g. when the UE is power off. For multiple PDN connectivity, this detach procedure shall be repeated for each PDN connected.

This clause covers also the termination of the IP-CAN session for UE's NS-WLAN offloaded traffic initiated by the Fixed Broadband Network.

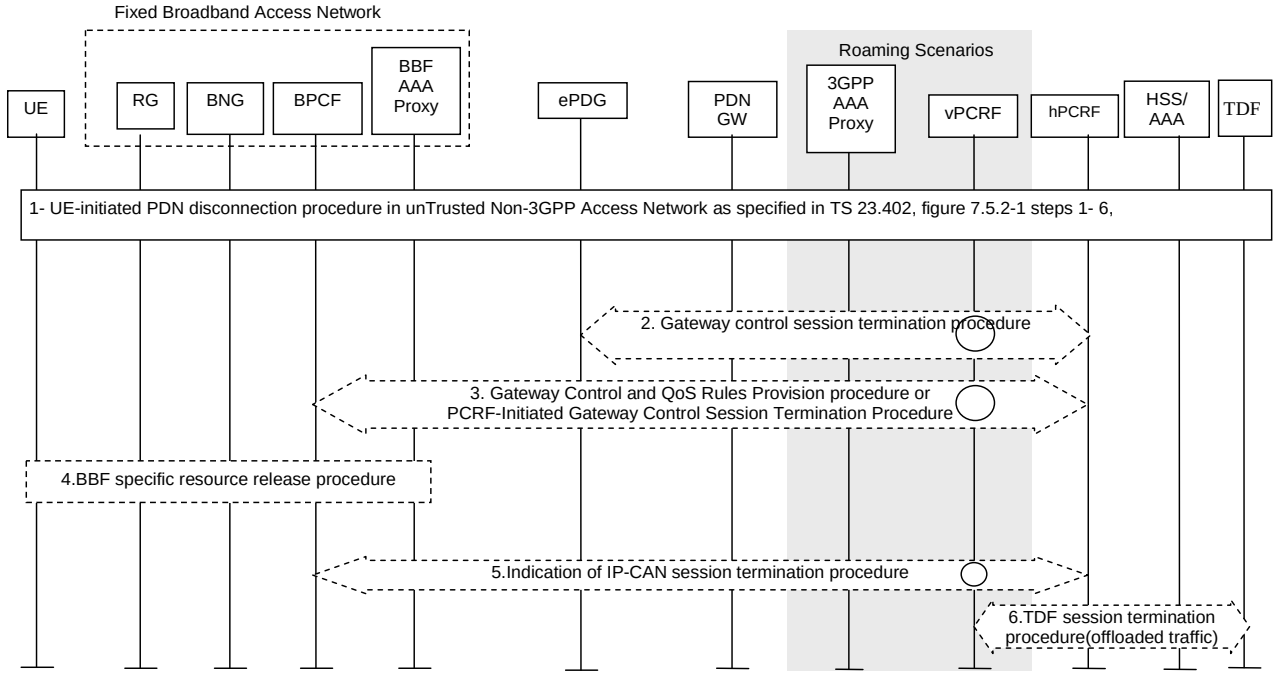

Figure 8.3.2-1: UE-initiated detach procedure with DSMIPv6 on untrusted S2c

NOTE: In the roaming case, the Step 2 terminates at the V-PCRF.

If dynamic policy provisioning is not deployed, the optional steps 2, 3, 5 and 6 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The description of this step is the same as UE-initiated PDN disconnection procedure in untrusted Non-3GPP Access Network as specified in TS 23 402, figure 7.5.2-1 steps 1-4 and 6;

2. The PCRF initiates Gateway Control Session termination procedure with the ePDG over Gxb*, if the last PDN connection is terminated for that UE.

3. Triggered by the IP-CAN session termination in step 1, the PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF.

4. The description of this step is the same as clause 7.3 step 4.

5. The description of this step is the same as clause 7.3 step 5.

6. The description of this step is the same as clause 7.3 step 6.

8.3.3 HSS-initiated Detach Procedure with DSMIPv6 on S2c in untrusted Fixed Broadband Access

The procedure in this clause applies to Detach Procedures, initiated by HSS.

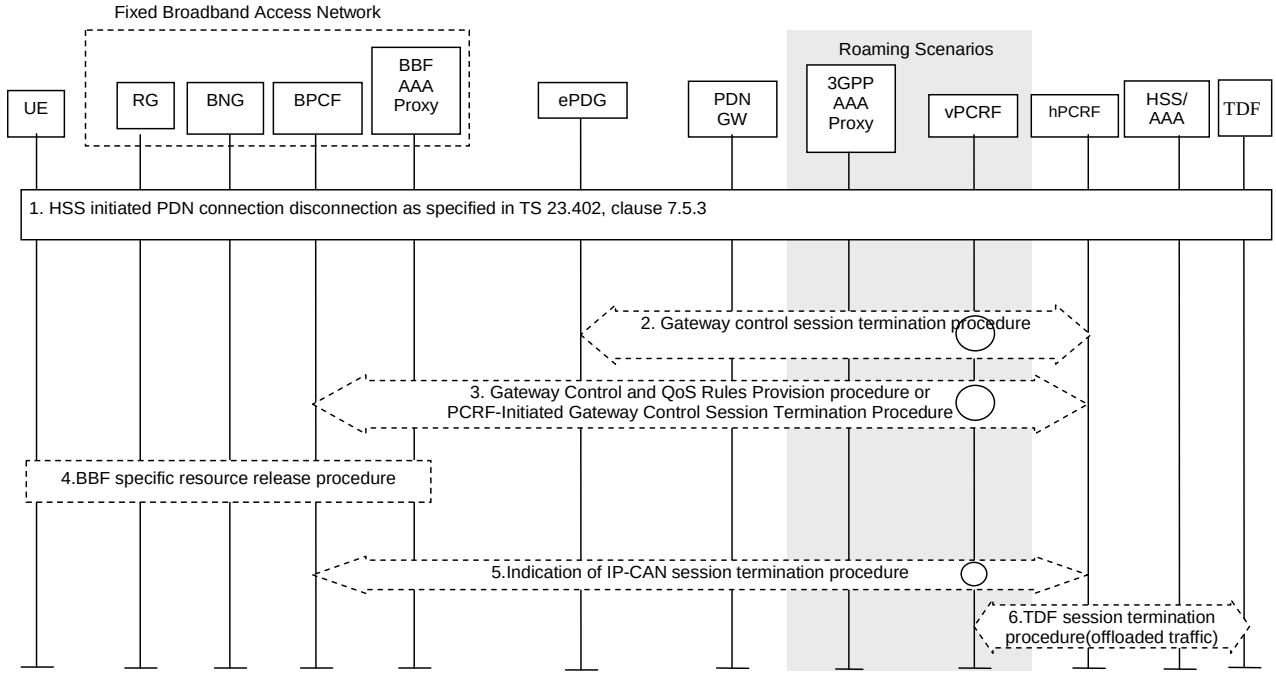

Figure 8.3.3-1: HSS-initiated detach procedure with DSMIPv6 on untrusted s2c

NOTE: In the roaming case, the Step 2 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 2, 3, 5 and 6 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The description of this step is the same as for steps 1-5 in TS 23 402 [3], clause 7.5.3.
2. If the last PDN connections is released, PCRF initiates Gxb* session termination procedure.
3. Triggered by the IP-CAN session termination in step 1, the PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF.
4. The description of this step is the same as clause 7.3 step 4.
5. The description of this step is the same as clause 7.3 step 5.
6. The description of this step is the same as clause 7.3 step 6.

8.3.4 PDN GW-initiated PDN disconnection Procedure with DSMIPv6 on S2c in untrusted Fixed Broadband Access

The procedure in this clause applies to PDN disconnection procedure initiated by PDN GW.

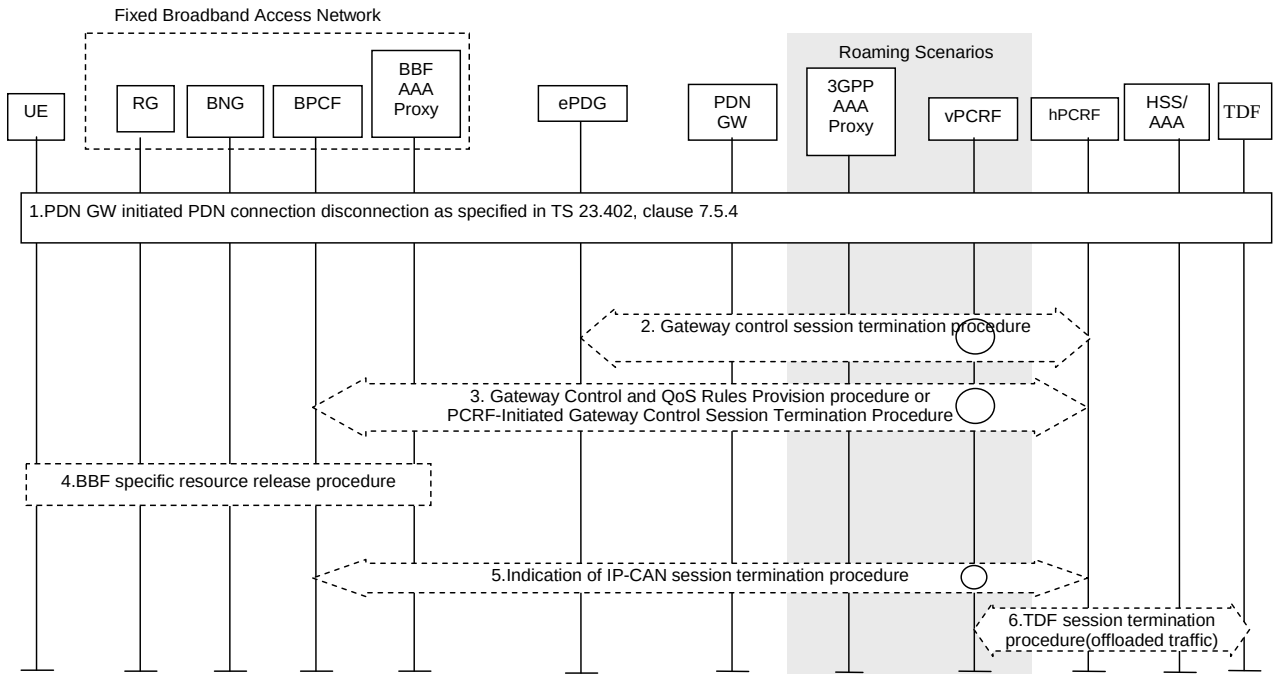

Figure 8.3.4-1: PDN GW-initiated PDN disconnection procedure with DSMIPv6 on untrusted s2c

NOTE: In the roaming case, the Step 2 terminates at the V-PCRF.

If dynamic policy provisioning over S9a is not deployed, the optional steps 2, 3, 5 and 6 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The description of this step is the same as for steps 1-4 in TS 23 402 [3], clause 7.5.4.

2. If the last PDN connections is released, PCRF initiates Gxb* session termination procedure.

3. Triggered by the IP-CAN session termination in step 1, the PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the BPCF.

4. The description of this step is the same as clause 7.3 step 4

5. The description of this step is the same as clause 7.3 step 5.

6. The description of this step is the same as clause 7.3 step 6.

8.3.5 E-UTRAN to untrusted Fixed Broadband Access Handover with DSMIPv6 on S2c

This clause shows the combined call flow for a handover when a UE moves from an E-UTRAN to an untrusted Fixed Broadband Access network. In addition, the procedures for the IP session establishment for NS-WLAN offload using the Fixed Broadband Access network are also integrated into the combined procedures.

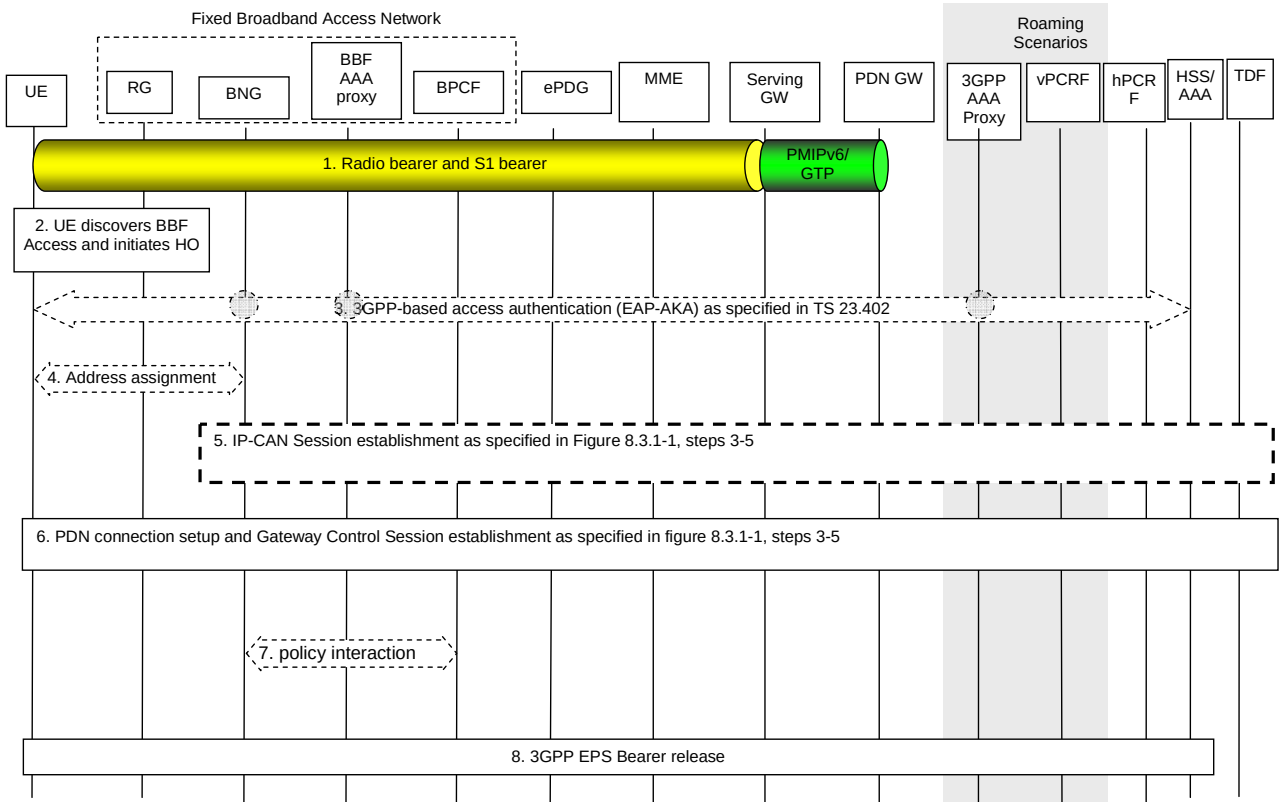

Figure 8.3.5-1: E-UTRAN to untrusted Fixed Broadband Access Handover with DSMIPv6 on s2c

Both the roaming and non-roaming scenarios are depicted in the figure.

If dynamic policy provisioning over S9a is not deployed, the optional steps 5 and 7 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

Handover is only applicable to the EPC-routed PDN connections. For the NS-WLAN offloaded traffic, a new IP session in fixed broadband access network is established.

For connectivity to multiple PDN steps 5 to 6 shall be repeated for each PDN connection.

1-2. This step is the same as steps 1-3 in TS 23 402 [3], clause 8.4.3, with the following addition: As part of the 3GPP-based authentication, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the Fixed Broadband Access network

3-4. The description of these steps is the same as for step 2 in Figure 8.3.1-1.

5. This step describes PCC signalling to provision policies for offloaded traffic and is only triggered when the BPCF receives the IMSI and the allocated UE local IP address using Fixed Broadband Access procedures. The description of this step is the same as for steps 3-5 in Figure 8.3.1-1.

6. The description of PDN Connection setup and Gateway Control Session setup are the same as for step 3-5 in Figure 8.3.1-1 with following addition:

   - Step 3 in Figure 8.3.1-1 is mandatory when performing handover from E-UTRAN to Fixed Broadband Access.

7. The description of this step is the same as for step 5 in Figure 8.2.1-1

8. The description of this step is the same as for step 11 in TS 23 402 [3], clause 8.4.3.

8.3.6 Handover from Untrusted Fixed Broadband Access with DSMIPv6 over S2c to 3GPP Access

In this scenario, the session starts in a untrusted Fixed Broadband Access system using DSMIPv6 over S2c and subsequently, the session hands over to a 3GPP access system.

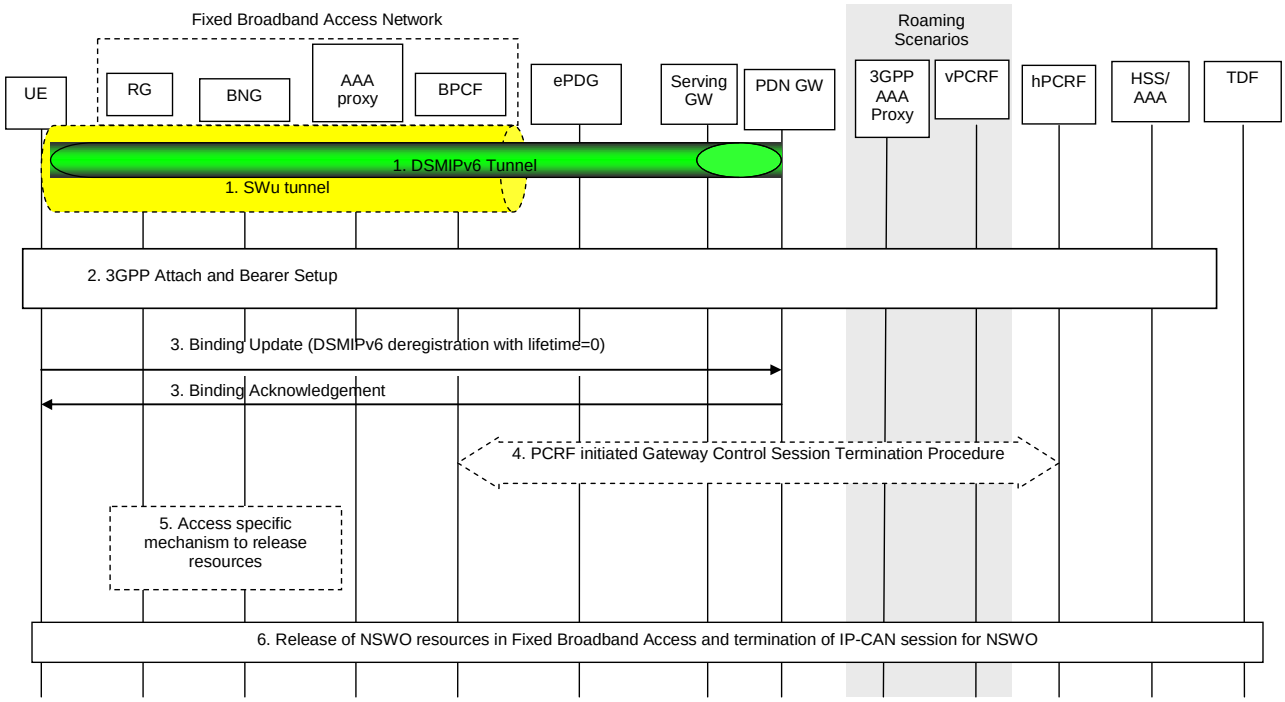

Figure 8.3.6-1: Fixed Broadband Access with S2c (DSMIPv6) to 3GPP access handover

If dynamic policy provisioning over S9a is not deployed, the optional step 4 does not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. The UE uses a Fixed Broadband Access system. It has a SWu session with the ePDG and a DSMIPv6 session with the PDN GW.

2-5. The description of these steps is the same as for steps 2-6 in clause 8.2.6.

6. If the NS-WLAN offloaded connection is released (e.g. if the UE moves out of WLAN coverage), the Fixed Broadband Access executes the access specific resource release procedure and initiates termination of the IP-CAN session for NS-WLAN offloaded traffic as described in steps 4-6 in clause 8.2.2.

8.3.7 Network-Initiated Dynamic PCC for S2c when accessing untrusted Fixed Broadband Access for EPC-routed Traffic

This procedure is applicable if the UE accesses over a Fixed Broadband Access network which is considered untrusted.

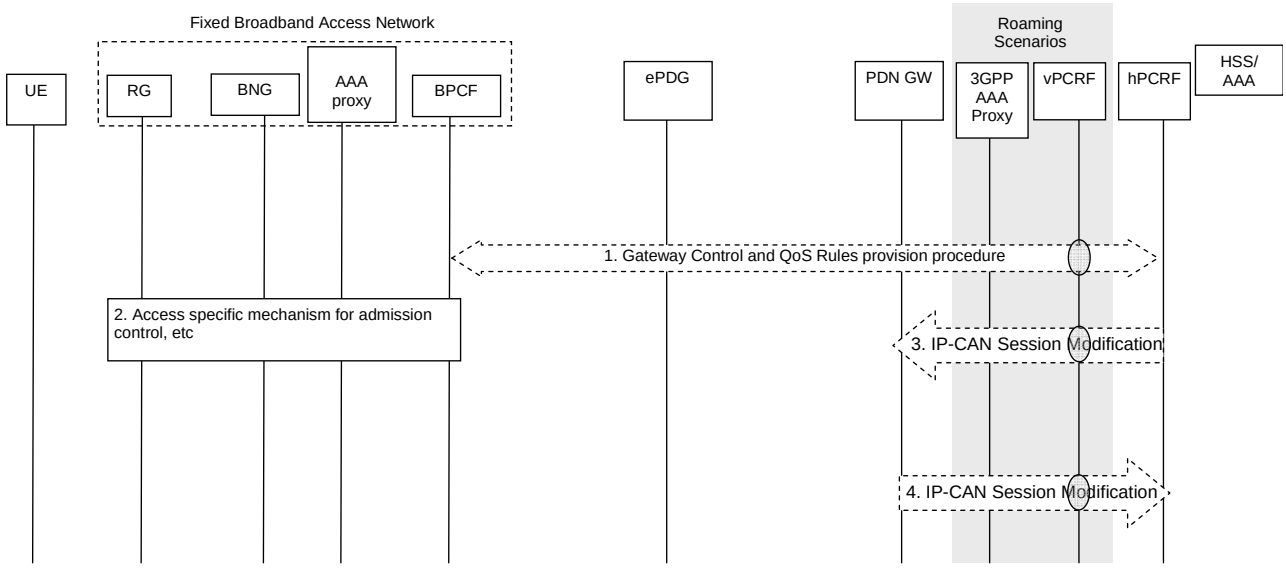

Figure 8.3.7-1: Network-initiated dynamic policy control procedure in un-trusted BBF IP Access for DSMIPv6 on S2c

This procedure concerns both the non-roaming (as Figure 4.2-3) and roaming case (as Figure 4.2-6). In the roaming case, the vPCRF in the VPLMN forwards messages between the BPCF and the hPCRF in the HPLMN. In the case of Local Breakout (as Figure 4.2-9), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures, step 1 and 3, only occur if dynamic policy provisioning is deployed. Otherwise Fixed Broadband Access network may employ BBF local policies.

1-3. The description of these steps is the same as for steps 1-3 in clause 7.6.

4. The PCEF acknowledges the provisioning of PCC Rules in the PCEF. For details please refer to TS 23.203 [4].

8.3.8 Network-Initiated Dynamic PCC for S2c when accessing untrusted Fixed Broadband Access for NS-WLAN offloaded Traffic

The information flow of "Network-Initiated Dynamic PCC for DSMIPV6 on S2c when accessing untrusted Fixed Broadband Access for offloaded Traffic" is same as S2b case, which is defined in clause 7.7.

8.3.9 UE-Initiated Connectivity to Additional PDN with DSMIPv6 on S2c over untrusted Fixed Broadband Access

This clause is related to the case when the UE has an established PDN connection and wishes to establish one or more additional PDN connections.

Since DSMIPv6 is used to establish connectivity with the additional PDN, the UE does not need to establish a separate SWu instance (i.e. a separate IPSec tunnel) for each additional PDN.

There can be more than one PDN connection per APN if the PDN GW supports that feature.

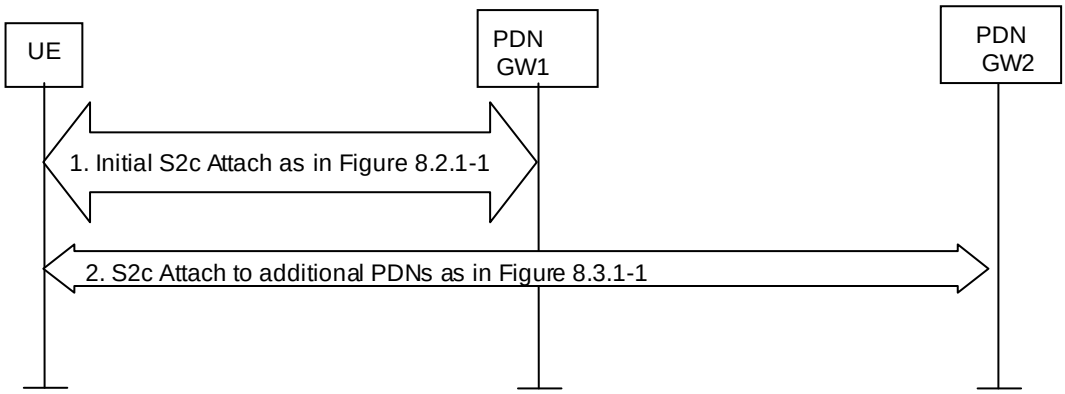

Figure 8.3.9-1: UE-Initiated connectivity to additional PDN from untrusted Non-3GPP IP Access with DSMIPv6 on S2c

1. The UE has performed the Initial S2c attach procedure as defined in clause 8.3.1 and has an established PDN connection.

2. The UE repeats the procedure steps 6-9 of clause 8.3.1, Figure 8.3.1-1 (Initial attachment when S2c is used for roaming, non-roaming and LBO) for each additional PDN the UE wants to connect to. For network supporting multiple mobility protocols, if there was any dynamic IPMS decision in step 1, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.

    - In Step 8, if no Gateway Control session over S9a for this UE, then the PCRF initiates the Gateway Control Session Establishment procedure with the BPCF. Otherwise, the PCRF provide new QoS rules corresponding to the new PDN connection to the BPCF using the Gateway Control and QoS Rules Provisioning procedure.

8.3.10 IPSec tunnel modified on S2c over untrusted Fixed Broadband Access

This clause is related to the case where the IPSec tunnel between the UE and the ePDG has been modified due to the UE initiated IPSec tunnel update procedure or a UE local IP address update. This procedure is only applicable if MOBIKE is supported by the UE.

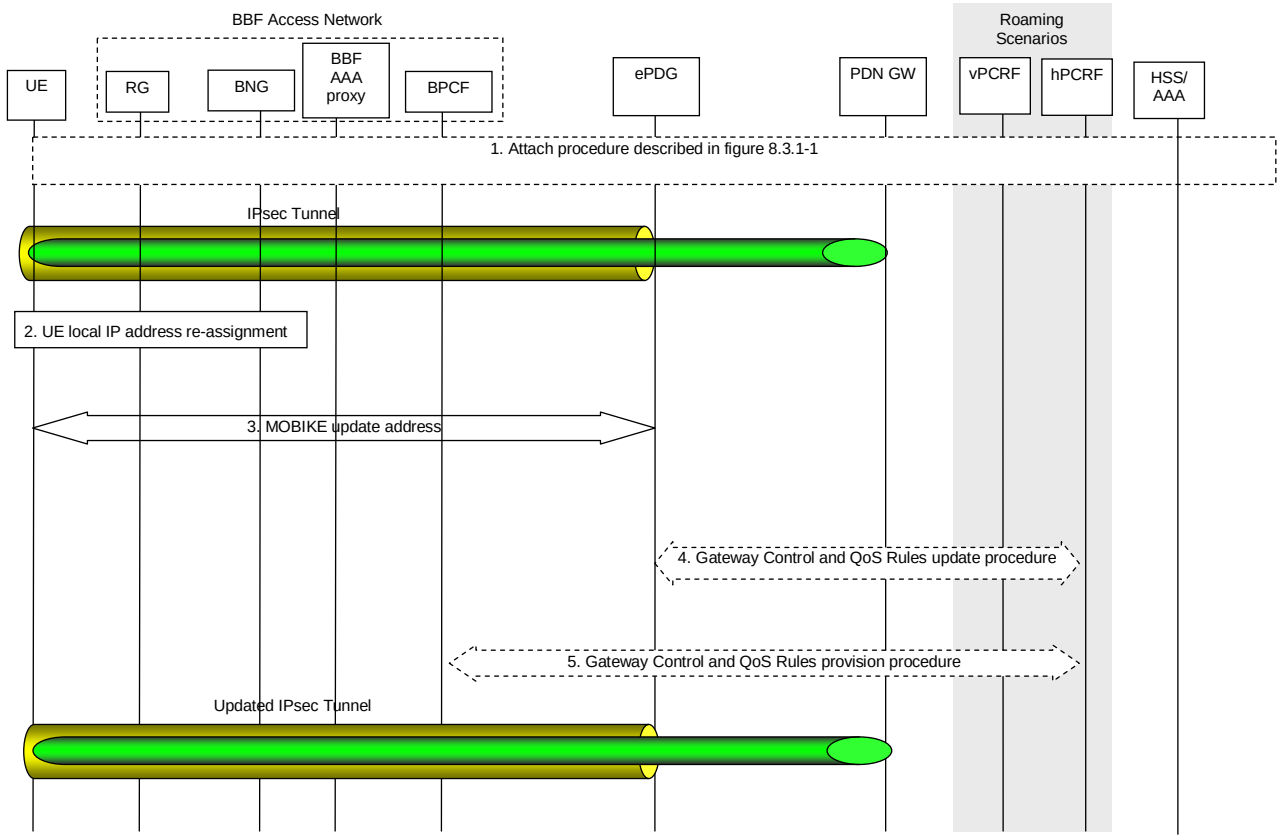

Figure 8.3.10-1: IPSec tunnel modified on S2c over untrusted Fixed Broadband Access

If dynamic policy provisioning over S9a is not deployed, the optional step 4 and 5 do not occur. Instead, the Fixed Broadband Access network may employ local policies.

1. UE attaches to EPC from untrusted BBF access network via ePDG, as described in clause 8.3.1. The IPSec tunnel is established between ePDG and UE; another IPSec tunnel is established between the PDN GW and UE. This clause only defines the outer IPSec tunnel (between the UE and ePDG) modification.
2. The description of this step is the same as step 2 in clause 7.11.
3. The description of this step is the same as step 3 in clause 7.11.
4. The description of this step is the same as step A.1 in clause 7.11.
5. The description of this step is the same as step A.2 in clause 7.11.

9 Functional Description and Procedures for Fixed Broadband Access network using H(e)NB

9.1 Procedures for Fixed Broadband Access network using HeNB

9.1.1 E-UTRAN Initial Attach and UE requested PDN connection Establishment

This clause is related to the case when the UE performs initial attachment or UE requests connectivity to an additional PDN to the E-UTRAN network via a HeNB. The HeNB is already registered in the network.

The HeNB sends the HeNB local IP address and the UDP port if NAT/NAPT is detected in the fixed Broadband access networks to the MME in UE associated S1 signalling (refer to the definition of Initial UE Message in TS 36.413 [29]).

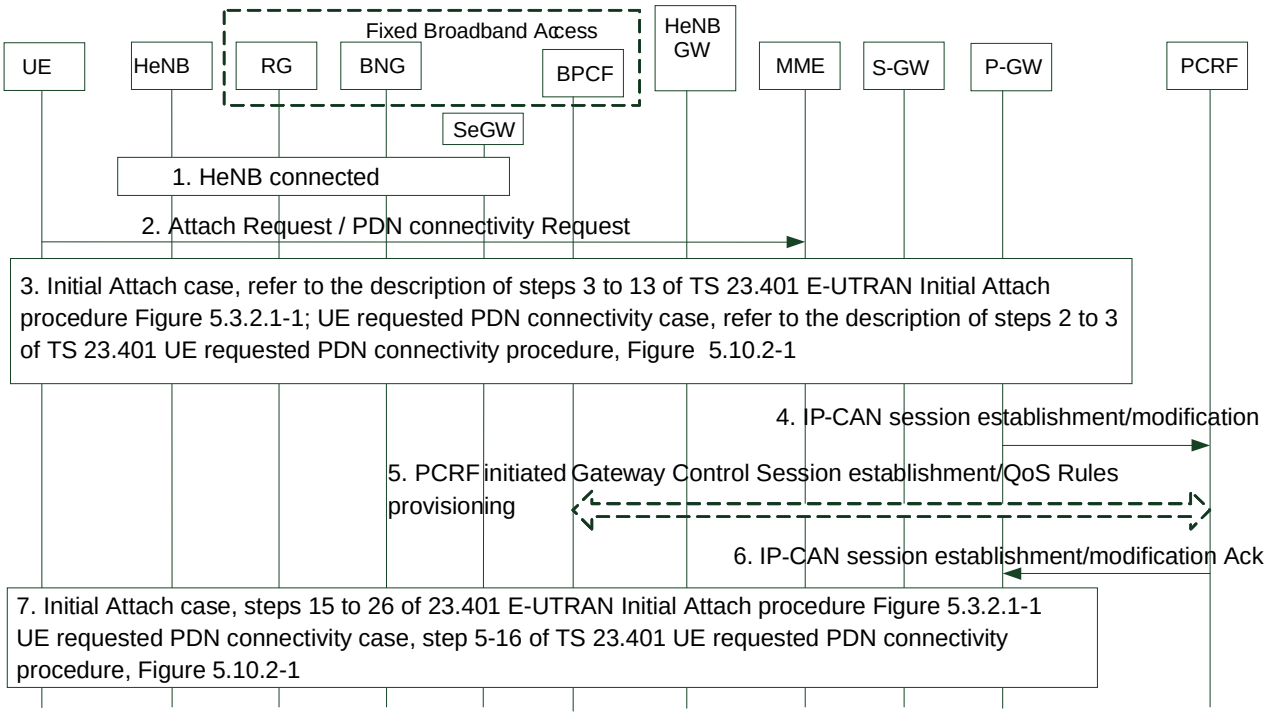

Figure 9.1.1: UE Attach and UE requested PDN connection Establishment procedure via HeNB

1. The HeNB is already registered in the network.

2. The description of this step is the same as for step 1 and 2 in TS 23.401 [2], clause 5.3.2.1 (Initial attach case), or is the same as for step 1 in TS 23.401 [2], clause 5.10.2 (UE requested PDN connection Establishment case) with the addition that HeNB includes the following additional information: the HeNB local IP address and the UDP port if NAT/NAPT is detected in the S1 signalling (refer to the definition of Initial UE Message in TS 36.413 [29]) and sends them to MME.

3. This step is the same as steps 3-13 in TS 23.401 [2] clause 5.3.2.1 (Initial attach case) or steps 2-3 in TS 23.401 [2] clause 5.10.2 (UE requested PDN connection Establishment case), with the following additional information included in Create Session Request message sending between MME and S-GW, and between S-GW and P-GW: HeNB Local IP address and the UDP port if NAT/NAPT is detected.

4. The PDN GW initiates the IP-CAN session establishment/modification procedure with the PCRF per TS 23.203 [4]. The message includes the IMSI, the HeNB local IP address and the UDP port if NAT/NAPT is detected.

5. The PCRF sends the Gateway Control Session establishment/QoS Rules provisioning message to the BPCF according to TS 23.203 [4]. The message includes the IMSI, HeNB local IP address and UDP port if NAT/NAPT is detected.

   Once this step completes the PCRF is aware the fact that the UE is connected to the network via a 3GPP H(e)NB and checks first whether sufficient resources are available in the BBF access before it provisions PCC rules at the PCEF.

6. The PCRF acknowledges the IP-CAN session establishment/modification.

7. This step is the same as steps 15-26 in TS 23.401 [2] clause 5.3.2.1 (Initial attach case) or steps 5-16 in TS 23.401 [2] clause 5.10.2 (UE requested PDN connection Establishment case) with the following additions: If the H(e)NB local IP address and UDP port number change reporting triggers are received from the PCRF, the PDN GW should set the H(e)NB local IP address and UDP port number Information Reporting accordingly. If the H(e)NB local IP address and UDP port number Reporting Request is received for this PDN connection, then the MME shall report to the PCEF/PCRF changes of HeNB local IP address and/or port (if available).

9.1.2 Detach procedure for E-UTRAN

This clause is related to detach procedure for E-UTRAN, and contains the following cases: UE-initiated Detach procedure, MME-initiated Detach procedure, and HSS-initiated Detach procedure.

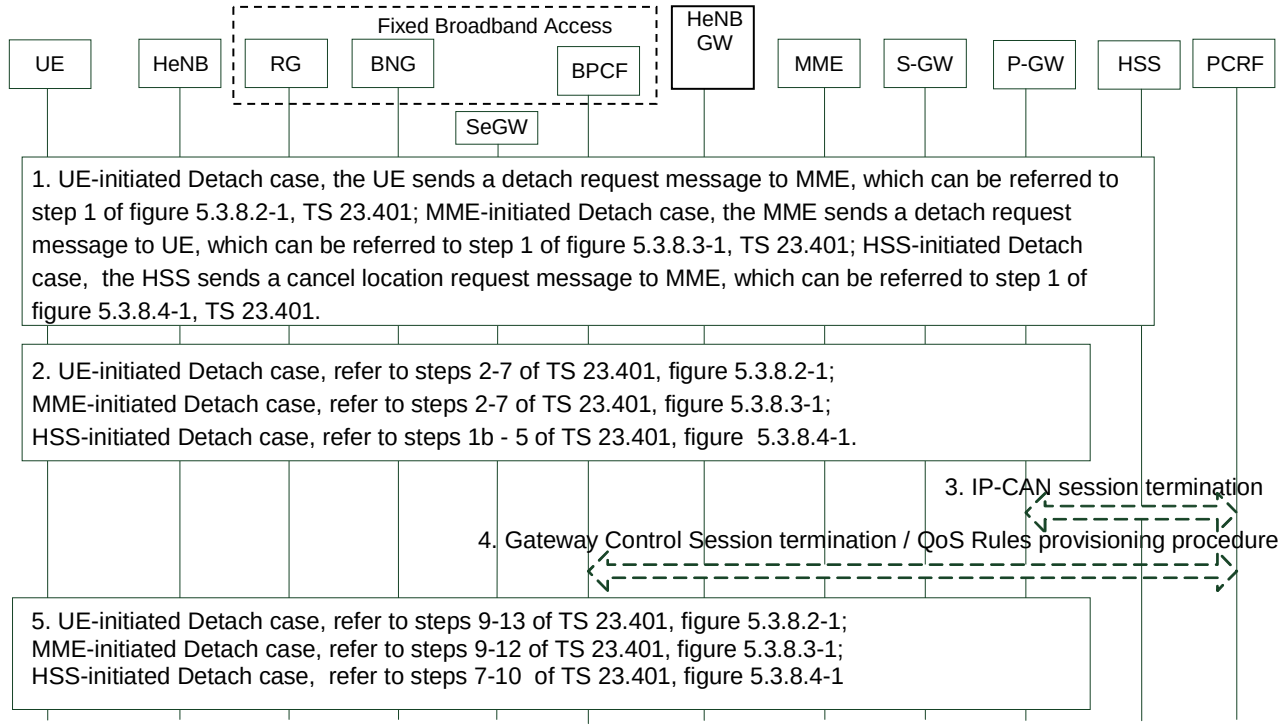

Figure 9.1.2: Detach Procedure via HeNB- UE camping on E-UTRAN

1. UE-initiated Detach case, the UE sends a detach request message to MME, which can be referred to step 1 of figure 5.3.8.2-1, TS 23.401 [2]; MME-initiated Detach case, the MME sends a detach request message to UE, which can be referred to step 1 of figure 5.3.8.3-1, TS 23.401 [2]; HSS-initiated Detach case, the HSS sends a cancel location request message to MME, which can be referred to step 1 of figure 5.3.8.4-1, TS 23.401 [2].

2. UE-initiated Detach case, refer to steps 2-7 per TS 23.401 [2], figure 5.3.8.2-1; MME-initiated Detach case, refer to steps 2-7 per TS 23.401 [2], figure 5.3.8.3-1; HSS-initiated Detach case, refer to steps 1b - 5 per TS 23.401 [2], figure 5.3.8.4-1.

3. The P-GW initiates the IP-CAN session termination procedure with the PCRF per TS 23.203 [4].

4 The PCRF initiates the Gateway Control session termination procedure according to TS 23.203 [4]. The PCRF sends the QoS Rules Provisioning procedure when there is one or more Gx sessions linked to the S9a session.

5. UE-initiated Detach case, refer to steps 9-13 per TS 23.401 [2], figure 5.3.8.2-1; MME-initiated Detach case, refer to steps 9-12 per TS 23.401 [2], figure 5.3.8.3-1; HSS-initiated Detach case, refer to steps 7-10 per TS 23.401 [2], figure 5.3.8.4-1.

9.1.3 Network initiated bearer activation, modification and deactivation

This clause is related to Network initiated Bearer operation procedure and contains the following cases: Dedicated bearer activation, Bearer modification with bearer QoS update, and Bearer deactivation.

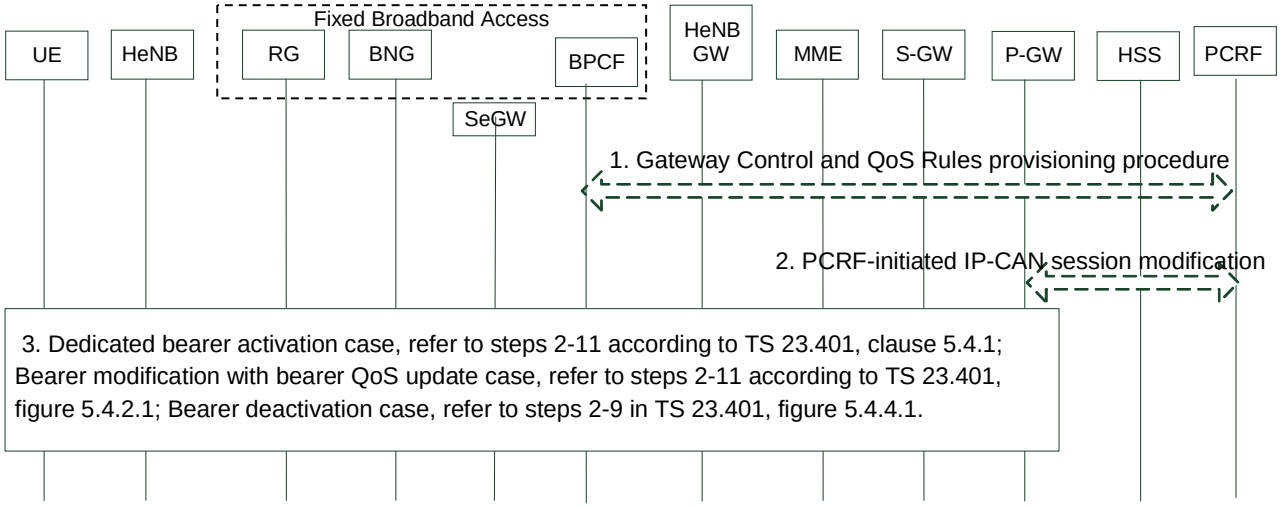

Figure 9.1.3 Network initiated Bearer activation, modification, and deactivation for HeNB

1. The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to request BPCF to reserve resource for traffic flow (Dedicated bearer activation), or to request allocation of resources in the BBF access network (Bearer modification with bearer QoS update), or to de-allocate resources in the BBF access network (Bearer deactivation). The message includes the QoS rules (SDF, QCI, ARP, GBR, MBR) according to TS 23.203 [4].

2. The PCRF initiates the IP-CAN session modification procedure with the P-GW/PCEF according to TS 23.203 [4].

3. Dedicated bearer activation case, refer to steps 2-11 according to TS 23.401 [2], 5.4.1; Bearer modification with bearer QoS update case, refer to steps 2-11 according to TS 23.401 [2], figure 5.4.2.1; Bearer deactivation case, refer to steps 2-9 according to TS 23.401 [2], figure 5.4.4.1.

NOTE: Step 1 may be triggered by service resource request from AF.

9.1.4 UE requested bearer resource modification

This procedure is executed per TS 23.401 [2], clause 5.4.5 when the PCRF determines that the UE's request result in allocation/de-allocation of resources in the BBF access.

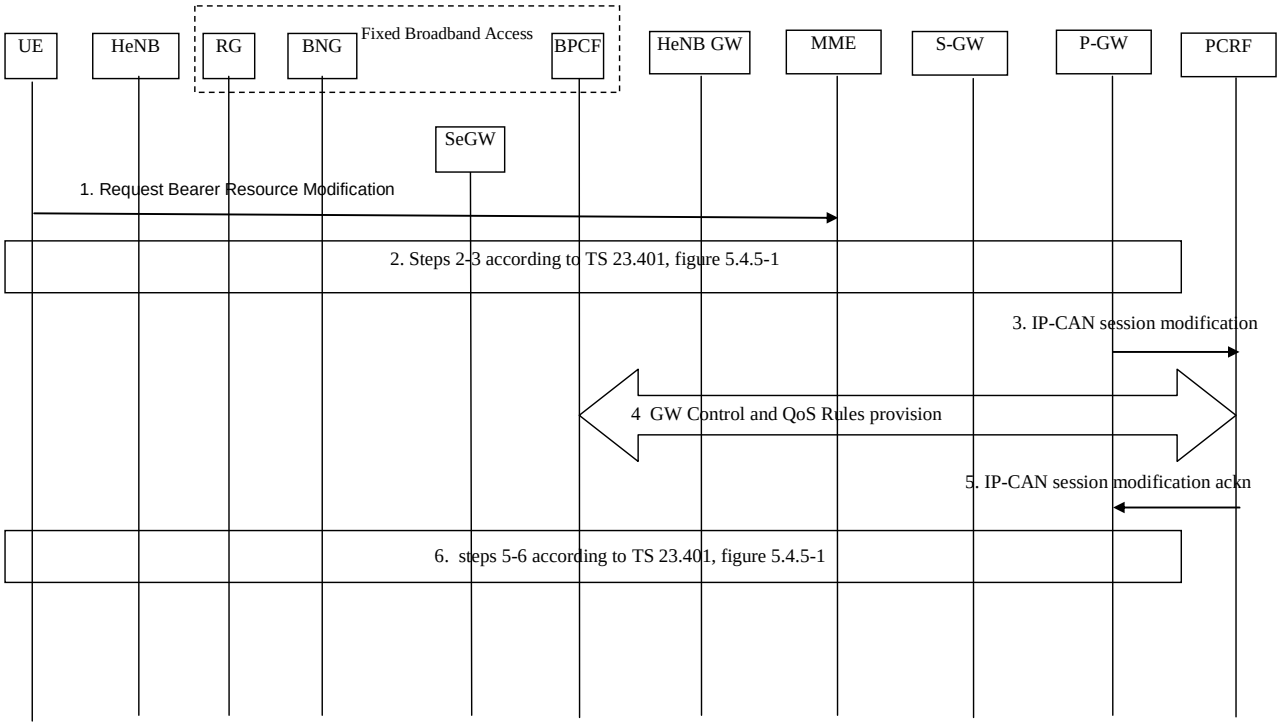

Figure 9.1.4: UE requested bearer resource modification

1. The description of this step is the same as for step 1 in TS 23.401 [2], clause 5.4.5.
2. The description of this step is the same as for step 2-3 in TS 23.401 [2], clause 5.4.5.
3. The P-GW initiates the IP-CAN session modification procedure with the PCRF per TS 23.203 [4].
4. The PCRF initiates the Gateway Control QoS Rules provision procedure with the BPCF to request allocation/de-allocation of BBF access network resources according to TS 23.203 [4].
5. The PCRF acknowledges the IP-CAN session establishment/modification.
6. The description of this step is the same as for step 5-6 in TS 23.401 [2], clause 5.4.5.

9.1.5 Service Request and Handover Procedures

This clause specifies the Service Request and Handover Procedures with updating the following information to fixed broadband access network: the HeNB local IP address and the UDP port if NAT/NAPT is detected.

This clause contains the following cases:

- UE initiated Service Request(clause 5.3.4.1, TS 23.401 [2])
- X2-based handover without Serving GW relocation(clause 5.5.1.1.2, TS 23.401 [2]),
- X2-based handover with Serving GW relocation(clause 5.5.1.1.3, TS 23.401 [2]),
- S1-based handover (clause 5.5.1.2.2 , TS 23.401 [2]),
- inter-RAT Handover from UTRAN Iu Mode to E-UTRAN (clause 5.5.2.2.2, TS 23.401 [2]),
- inter-RAT handover from GERAN A/Gb Mode to E-UTRAN(clause 5.5.2.4.2, TS 23.401 [2]).

The MME shall report changes in HeNB local IP address and/or port to the PCEF/PCRF if

- the PCRF has subscribed to reporting of changes of the local H(e)NB IP address and UDP port number; and
- the UE moves from one (e)NB to a HeNB, or from one HeNB to another HeNB with the fixed network backhaul changed, or the UE moves from a HeNB to a (e)NB.

The MME does not update the PCEF/PCRF in particular when the UE enter connected mode if there is no change in HeNB local IP address and UDP port number, or when the UE enters idle mode.

If the S-GW needs to update the PCEF/PCRF (e.g. send a Modify Bearer Request over S5/S8) for any other reasons not listed above (e.g. time zone change, S-GW relocation), the S-GW shall include the current values for H(e)NB local IP address and UDP port if the UE is accessing the network from a HeNB.

This following call flow only shows the changed steps, and the steps without change can be referred to the corresponding clauses in TS 23.401 [2].

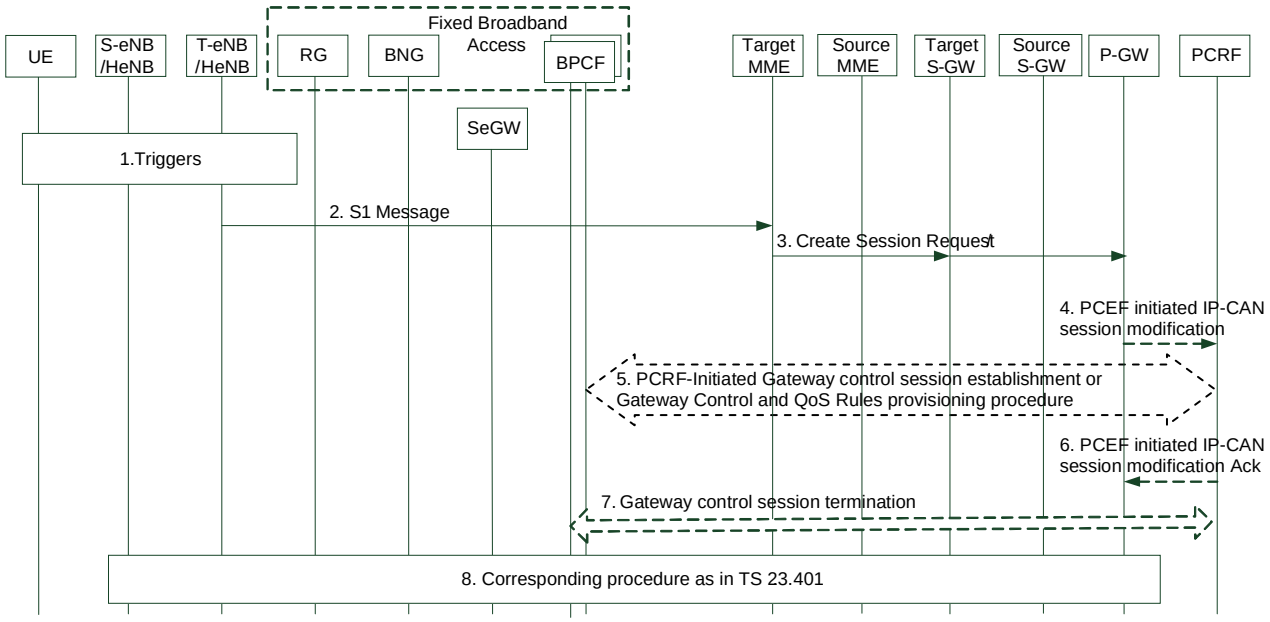

Figure 9.1.5: Service Request and Handover Procedures

1. UE initiated Service request procedure, or intra-EUTRAN Handover procedure, or inter-RAT handover is initiated, which can be referred to the descriptions of the corresponding clause4 in TS 23.401 [2].

2. This step is the same as that in TS 23.401 [2], with the addition that target HeNB includes the following additional information: the target HeNB local IP address and the UDP port if NAT/NAPT is detected in the S1 message and sends them to MME. For the service request case, the S1 message carrying the "NAS: Service request" from UE to MME is Initial UE Message; for the X2 based handover case, the S1 message is the Path Switch Request message; for the S1 based handover or the inter-RAT handover, the S1 message is the Handover Notify Message.

3. This step is the same as that in TS 23.401 [2], with the following additional information included in create session request message or Modify bearer Request message sending between MME and S-GW, and Modify Bearer Request Message sending between S-GW and P-GW (when a Modify Bearer Request message needs to be sent over S5/S8): target HeNB Local IP address and the UDP port if NAT/NAPT is detected.

4. The P-GW sends IP-CAN session modification request message to the PCRF including the Target HeNB local IP address and the UDP port if NAT/NAPT is detected as defined in TS 23.203 [4].

   If the Modify bearer Request message received by P-GW in step 3 contains none of the additional information: HeNB Local IP address and the UDP port if NAT/NAPT is detected. The P-GW determines that the UE leaves femto cell and will inform this event to PCRF.

5. If the UE moves from eNB to a HeNB, the PCRF will initiate PCRF-initiated Gateway control session establishment procedure as defined in TS 23.203 [4] if the UE is the first UE attaching the target HeNB for that PCRF; if the UE moves from one HeNB to another HeNB without fixed network backhaul changed or if the UE moves to a new HeNB and there has been one Gateway Control Session for that HeNB, the PCRF will initiate Gateway control and QoS rule provisioning procedure with BPCF as defined in TS 23.203 [4]. The HeNB local IP address and the UDP port if NAT/NAPT is detected shall be included in the PCRF-Initiated Gateway control session establishment procedure and in Gateway Control and QoS rule provisioning procedure.

6. The PCRF acknowledges the IP-CAN session modification.

7. If UE moves from one HeNB toeNB, the PCRF will terminate the old Gateway control session if this is the last UE under the source HeNB for that PCRF; if the UE moves from eNB to a HeNB, or the UE moves from one HeNB to another HeNB without fixed network backhaul changed, or there are other UEs attached the source HeNB, this step will be skipped.

8. This step can refer to the corresponding procedure as in TS 23.401 [2].

NOTE: The interaction between the BPCF and the BNG is out of scope.

9.2 Procedures for Fixed Broadband Access network using HeNB - PMIP

9.2.1 Initial E-UTRAN Attach with PMIP-based S5/S8

This clause is related to the case when the UE performs initial attachment to the E-UTRAN network via a HeNB. The HeNB is already registered in the network.

The HeNB sends the HeNB local IP address and UDP port if NAT/NAPT is detected to the MME in UE associated S1 signalling (refer to the definition of Initial UE Message in TS 36.413 [29]).

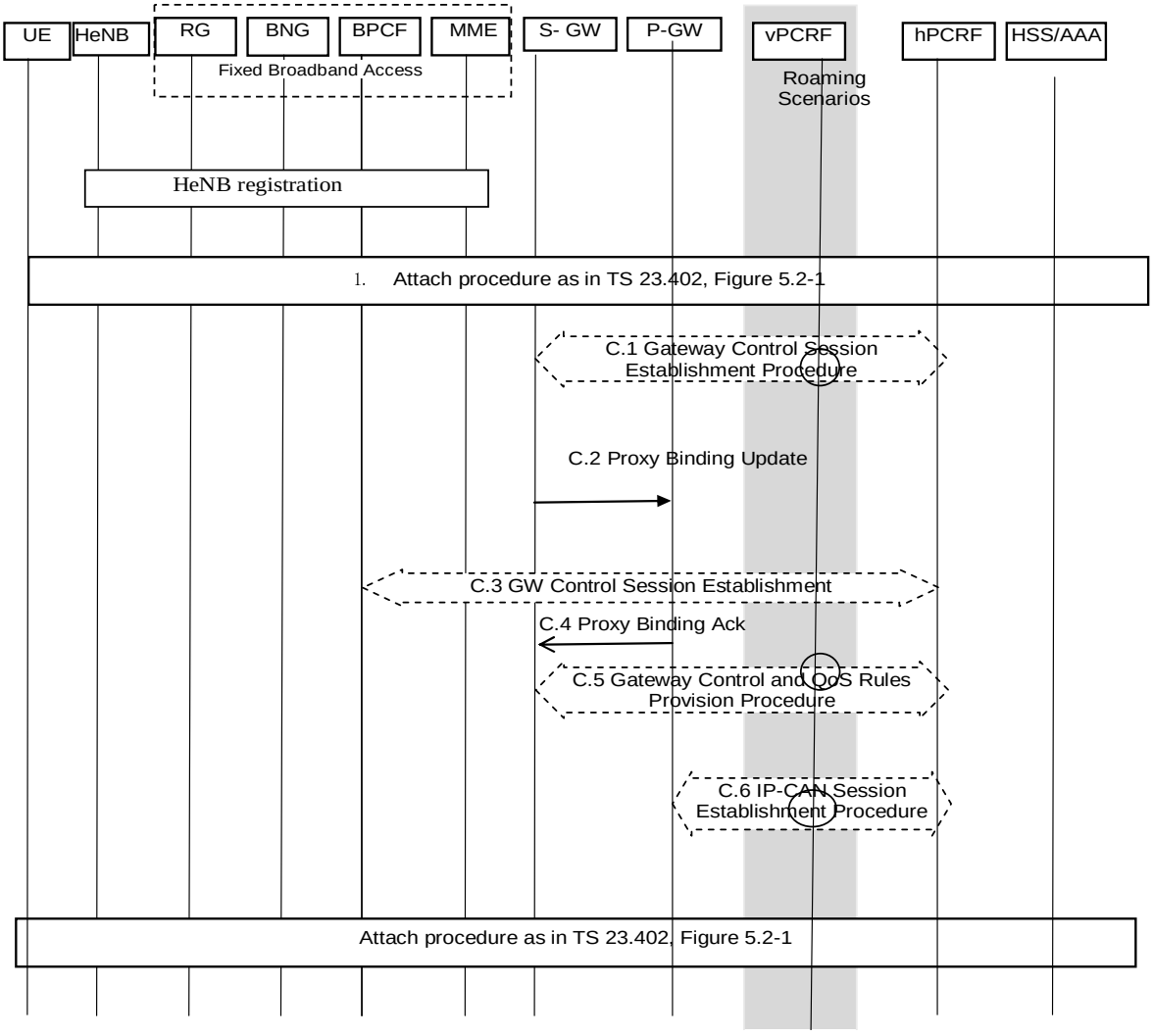

Figure 9.2.1-1 : Initial E-UTRAN attach with PMIP-based S5/S8

This procedure is the same as described in TS 23 402 [3], clause 5.2 with the modification of the existing steps and addition of the new step described below.

1. This step is the same as for attach procedures as in TS 23 402[3], figure 5.2-1, with the exception as defined for the corresponding steps for GTP case, clause 9.1.1.

C.1 The S-GW initiates the Gateway control session establishment procedure with the PCRF, and the following additional information: the HeNB local IP address and the UDP port if NAT/NAPT is detected needs to be forwarded to the PCRF during this procedure.

C.3 The PCRF sends the Gateway Control Session establishment/QoS Rules provisioning message to the BPCF according to TS 23.203 [4]. The message includes the IMSI, HeNB local IP address and UDP port if NAT/NAPT is detected.

Once this procedure completes the PCRF is aware the fact that the UE is connected to the network via the a 3GPP Femto and checks first whether sufficient resources are available in the BBF access before it provisions QoS and PCC rules at the BBER and PCEF, respectively.

9.2.2 Detach for PMIP-based S5/S8

The procedure in this clause provides the PMIPv6-based S5/S8 variants to all E-UTRAN Detach Procedures, including UE, MME or HSS initiated detach procedure (TS 23.401 [2] clause 5.3.8).

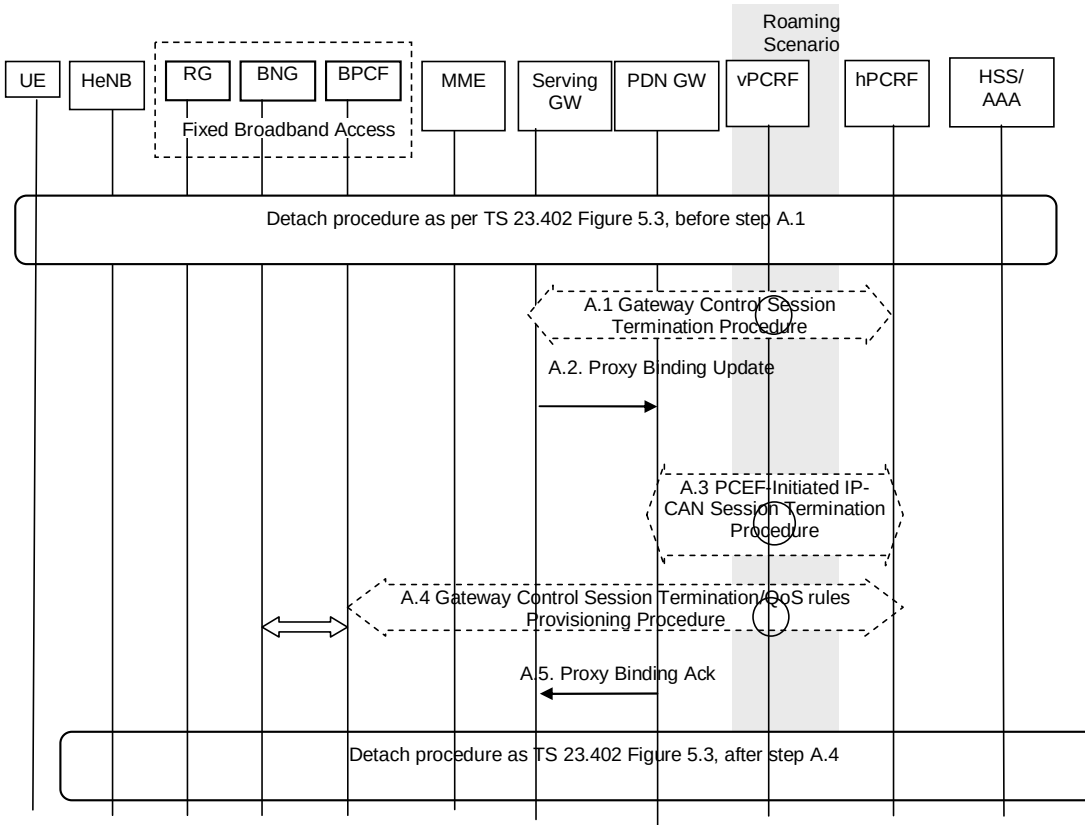

Figure 9.2.2-1: E-UTRAN Detach Procedure for PMIP-based S5/S8

This procedure is the same as described in TS 23 402 [3], clause 5.3 with the addition of the new step described below.

A.4. The PCRF initiates the Gateway Control session termination/ QoS Rules Provisioning procedure with BPCF according to TS 23.203 [4].

NOTE: The interaction between the BPCF and the BNG is out of scope.

9.2.3 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8

The dedicated bearer procedure for a PMIP based S5/S8 is based on TS 23 402 [3], clause 5.4.1 It applies to dedicated bearer activation/modification/deactivation procedures.

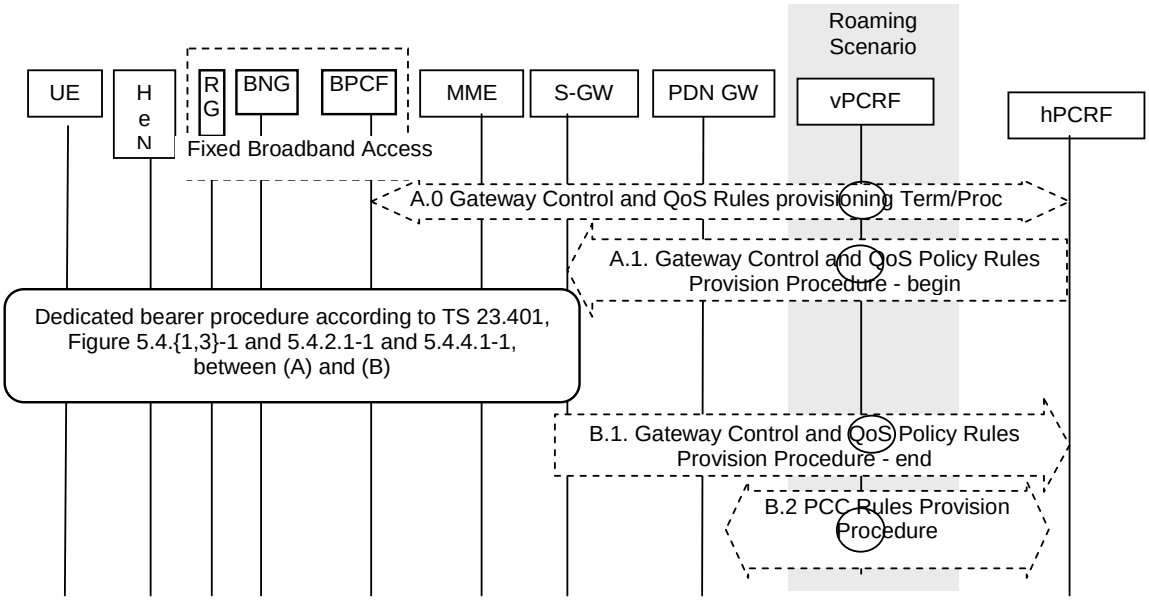

Figure 9.2.3-1: Dedicated Resource Allocation/Deallocation Procedure, UE in Active Mode

This procedure is the same as described in TS 23 402 [3], clause 5.4.1 with the addition of the new step described below:

A.0 The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to request or de-allocate resources in the BBF access network. The message to request resources includes the QoS Information (SDF, QCI, ARP, GBR, MBR) according to TS 23.203 [4].

9.2.4 HSS-Initiated Subscribed QoS Modification

The HSS triggers a change to the default beater QoS attributes that, depending on the decision of the PCRF, may impact the resources allocated in the BBF access.

The HSS Initiated Subscribed QoS Modification for a PMIP-based S5/S8 is depicted in TS 23 402 [3], Figure 5.4.3.2-1.

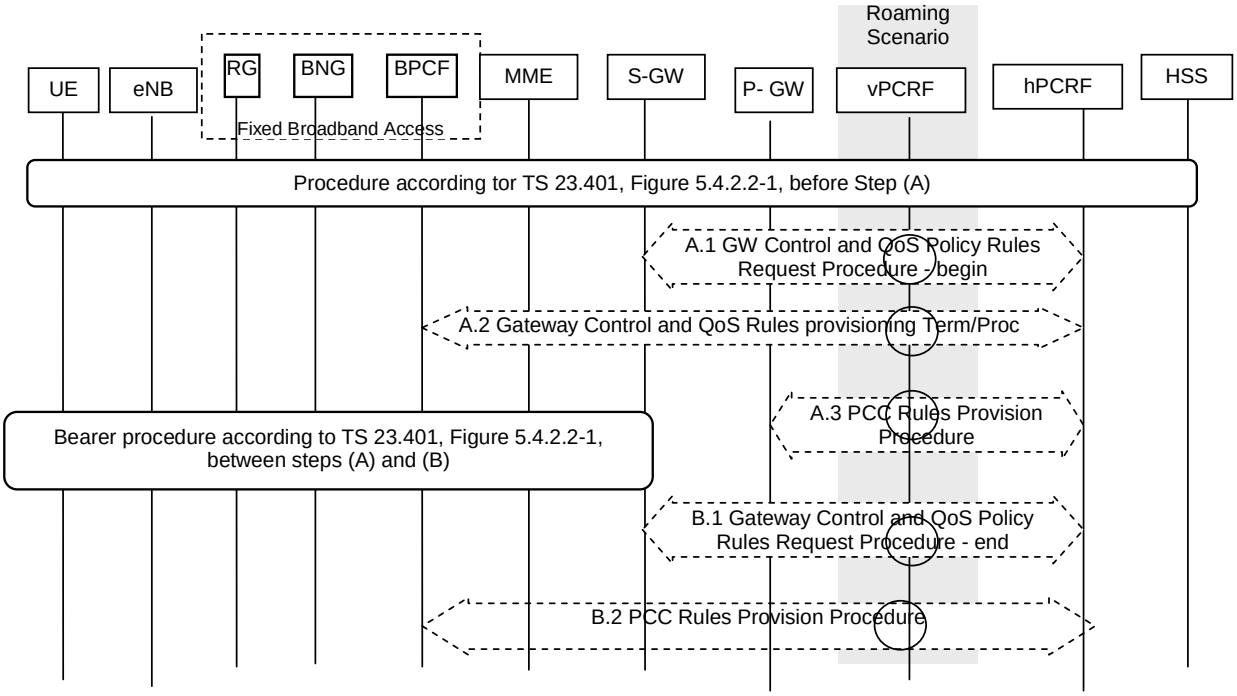

Figure 9.2.4-1 HSS-initiated Subscribed QoS Modification

This procedure is the same as described in TS 23 402 [3], clause 5.4.3.2 with the addition of the new step described below:

A.2. The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to either request allocation/de-allocation of BBF resources. The message includes the QoS Information (QCI, ARP, GBR, MBR) according to TS 23.203 [4].

9.2.5 MME-initiated Dedicated Bearer Deactivation

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the procedure defined in TS 23.401 [2], clause 5.4.4.2 for -MME initiated dedicated bearer deactivation.

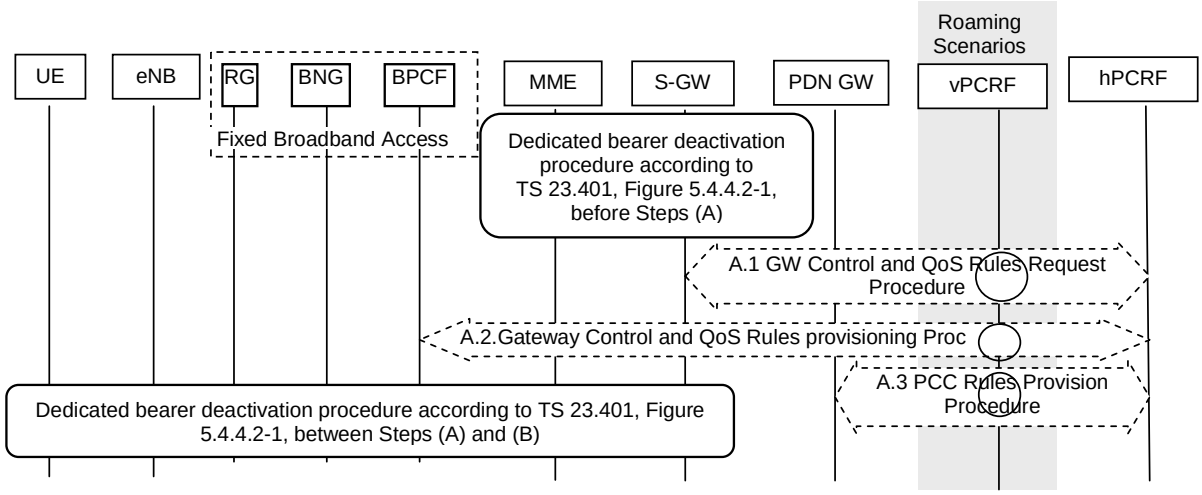

Figure 9.2.5-1: MME-initiated Dedicated Bearer Deactivation

This procedure is the same as described in TS 23 402 [3], clause 5.4.5.3 with the addition of the new step described below:

A.2 The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to either request de-allocation of BBF resources for the affected QoS rule(s) according to TS 23.203 [4].

9.2.6 UE-initiated Resource Request and Release

This procedure is executed per TS 23 402 [3], clause 5.5, with modifications, when the PCRF determines that the UE's request result in allocation/de-allocation of resources in the BBF access.

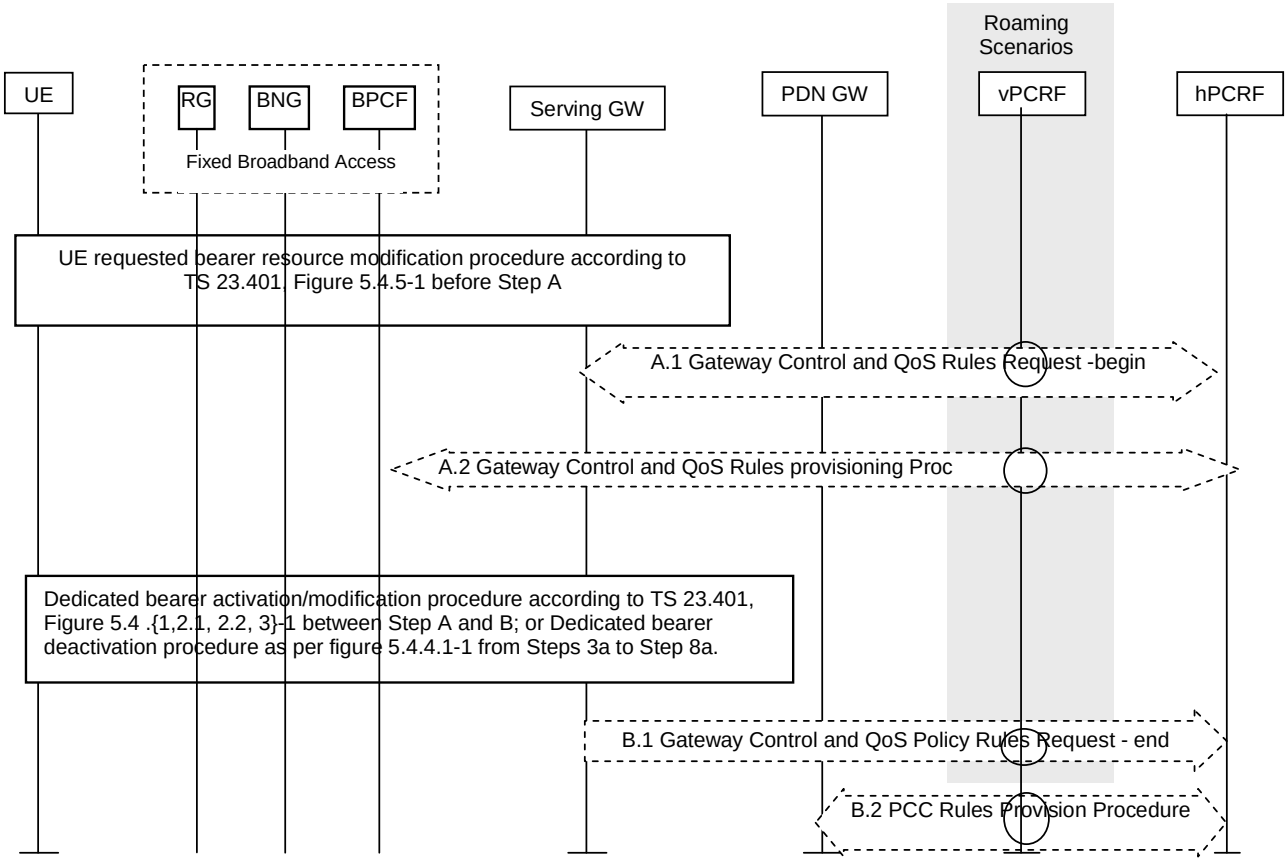

Figure 9.2.6-1: UE-initiated resource request/release with PMIP-based S5/S8

This procedure is the same as described in TS 23 402 [3], clause 5.5 with the addition of the new step described below.

The UE requests to add, delete or modify filter and may include the QCI and GBR if needed. Depending on the decision of the PCRF new BBF resource may be required. For instance, the PCRF may decide to initiate the activation of a new dedicated bearer.

A.2. The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to, depending on the UE's request, either request allocation/de-allocation of BBF resources. If resources are de-allocated the message includes the QoS rule affected. If additional BBF resources are required then the PCRF includes the QoS rule and QoS Information (SDF, QCI, ARP, GBR, MBR) according to TS 23.203 [4].

NOTE: The interaction between the BPCF and the BNG is out of scope.

9.2.7 UE requested PDN connectivity

The UE requested PDN connectivity procedure for E-UTRAN is depicted in figure 5.6.1-1, TS 23 402 [3]. The procedure allows the UE connected to a HeNB to request for connectivity to an additional PDN over E-UTRAN.

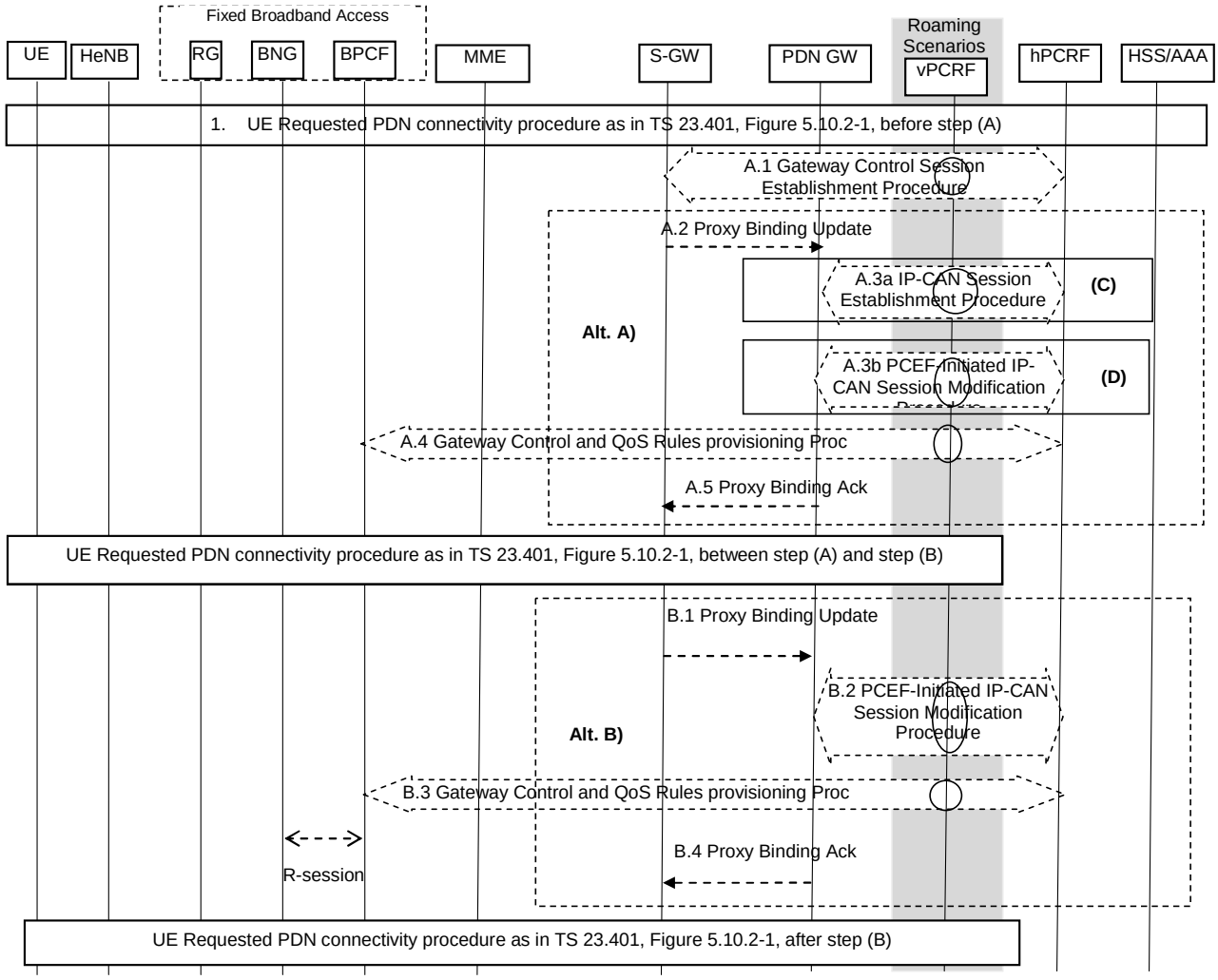

Figure 9.2.7-1: UE requested PDN connectivity with PMIP-based S5 or S8

This procedure is the same as described in TS 23 402 [3], clause 5.6.1 with modification of the existing steps and the addition of the new step described below.

The procedure is executed when the UE requests an additional PDN connection or re-establishes an existing one after a HO.

1. This step is the same as for PDN connectivity procedures as in TS 23.401 [2], figure 5.10.2-1 before step (A), with the exception as defined for the corresponding steps for GTP case, clause 9.1.1.

A.1. The description of this step is the same as step C.1 in clause 9.2.1.

If Alt.A is selected then the PCRF executes step A.4.

A.4. The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to modify BBF resources associated with an existing QoS rules or to request new BBF resources. In either case the message includes the QoS Information (SDF, QCI, ARP, GBR, MBR) according to TS 23.203 [4].

If Alt.B is selected then the PCRF executes step B.3.

B.3. The PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to modify BBF resources associate with an existing QoS rule. The message includes the QoS Information (SDF, QCI, ARP, GBR, MBR) according to TS 23.203 [4].

NOTE: The interaction between the BPCF and the BNG is out of scope.

9.2.8 Service Request and Handover Procedures

This clause specifies the Service Request and Handover Procedures with updating the following information to Fixed Broadband Access network: the HeNB local IP address and the UDP port if NAT/NAPT is detected.

This clause is similar to clause 9.1.5, with the difference that the S5/8 interface is PMIP-based. This following call flow only shows the description on S5/S8 interfaces and Gx/Gxx/S9a interfaces.

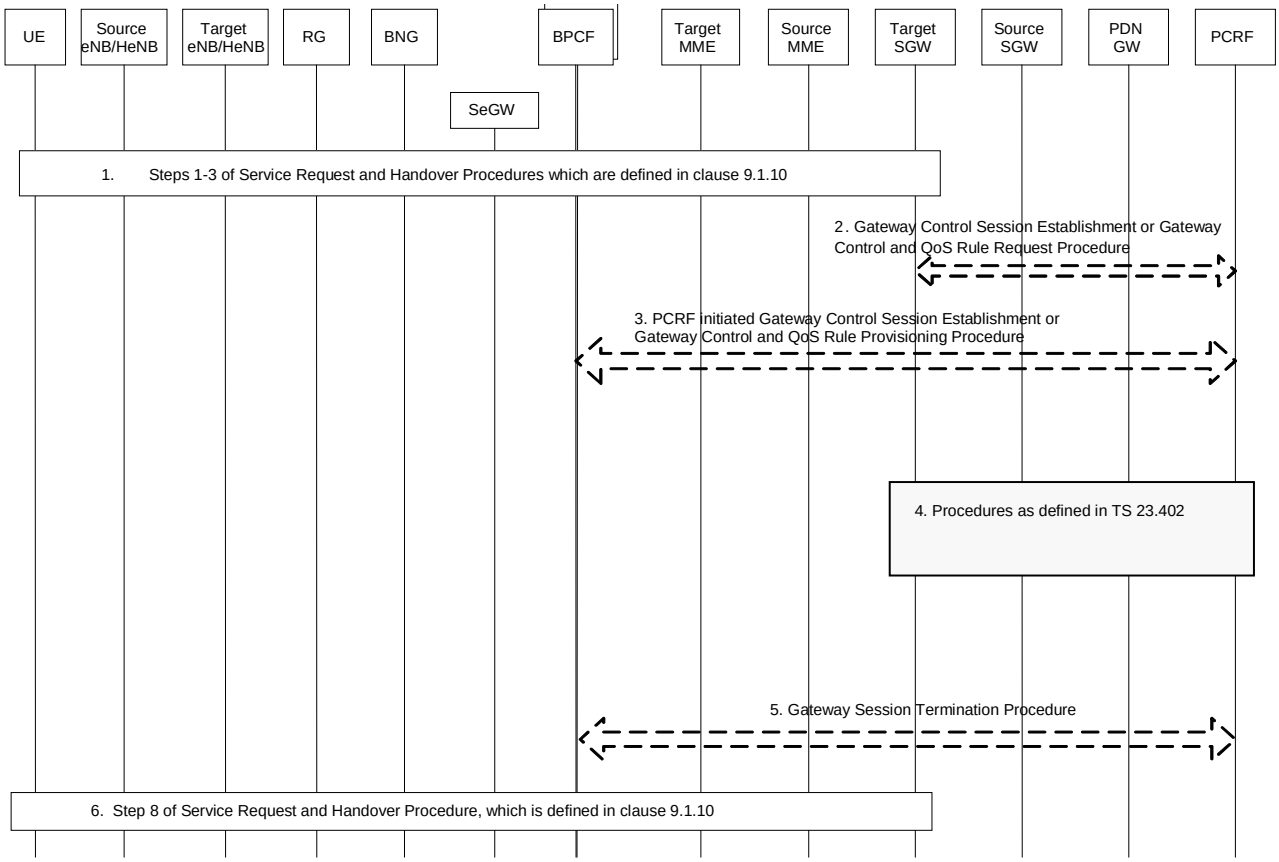

Figure 9.2.8-1: Service Request and Handover Procedures-S5/S8 PMIP-based

1. UE initiated Service request procedure, or intra-EUTRAN Handover procedure, or inter-RAT handover is initiated, which can be referred to the corresponding descriptions of clause 9.1.5, Service Request and Handover Procedures (GTP case).

2. The (target) S-GW initiates the Gateway control session establishment (with S-GW relocated) procedure or Gateway Control and QoS Rule Request procedure (without S-GW relocated) with the PCRF, and the following additional information: the HeNB local IP address and the UDP port if NAT/NAPT is detected needs to be forwarded to the PCRF during this procedure.

   If the Create Session Request message (with S-GW relocated) or Modify bearer Request message (without S-GW relocated) received by S-GW in step 1 contains none of the additional information: HeNB Local IP address and the UDP port if NAT/NAPT is detected The S-GW determines that the UE leaves femto cell and will inform this event to PCRF.

3. The description of this step is the same as step 5 in clause 9.1.5.

4. This step is the same as the corresponding steps defined in handover procedures for PMIP-based S5/S8 interface clause 5.7, and UE-triggered Service Request for PMIP-based S5/S8, clause 5.9, TS 23 402 [3]. The description of this step is the same as step 7 in clause 9.1.5.

5. This step can refer to the corresponding procedure as in clause 9.1.5.

NOTE: The description is the same as note 2 and note 3 in clause 9.1.5.

9.3 Procedures for Fixed Broadband Access network using HNB for PS services

9.3.1 PDP Context Activation

The HNB is already registered in the network. The HNB GW sends the HNB local IP address and the UDP port number if NAT/NAPT is detected to the SGSN in the [RANAP] INITIAL UE MESSAGE message (for the message refer to TS 25.413 [28]).

Depicted in Figure 9.3.1-1 is the PDP Context Activation procedure.

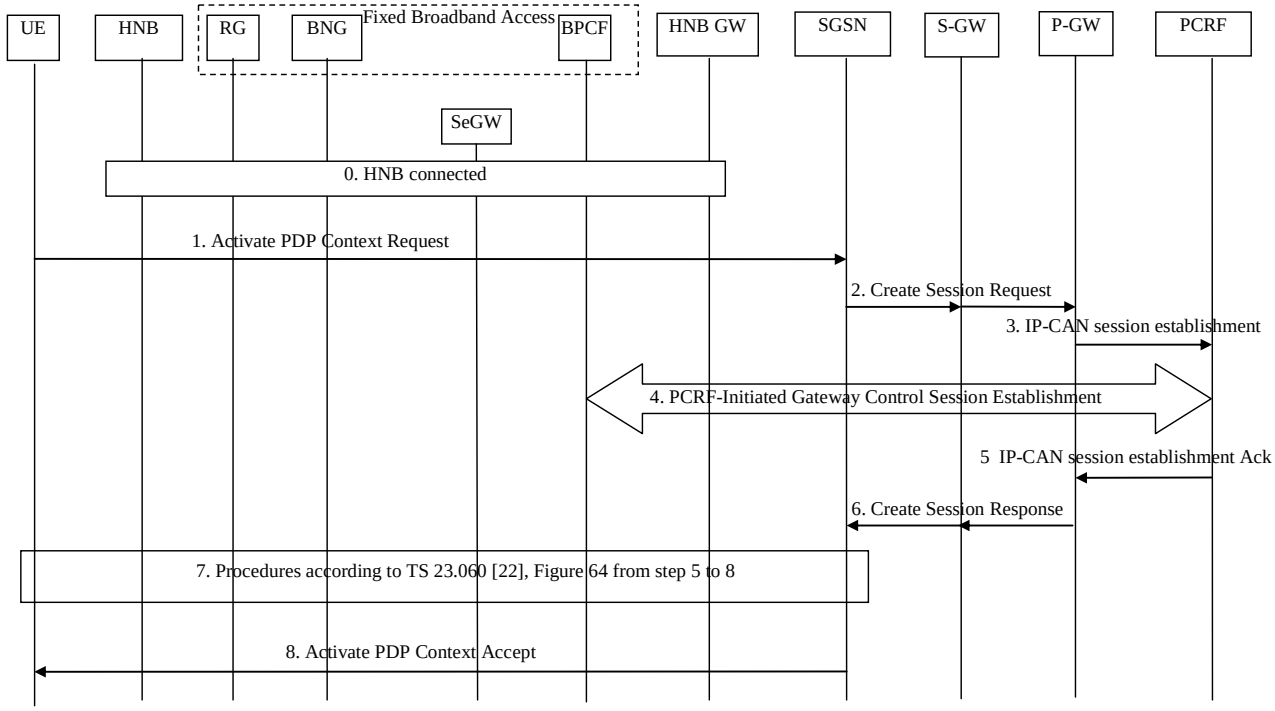

Figure 9.3.1-1: PDP Context Activation Procedure for EPS-connected 3G access

0. The HNB connected. The HNB GW received the HNB Local IP address and the UDP port number if NAT/NAPT is detected.

1. This step is the same as step 1 in TS 23.060 [22] clause 9.2.2.1, with the addition that the HNB GW includes in the [RANAP] INITIAL UE MESSAGE message the HNB Local IP address and the UDP port number if NAT/NAPT is detected.

2. This step is the same as step A in TS 23.060 [22] clause 9.2.2.1A, with the addition that the S4-SGSN also includes HNB Local IP address and the UDP port number if NAT/NAPT is detected in the Create Session Request sent to the S-GW and in turn to P-GW.

3. The P-GW sends the IP-CAN session establishment request to the PCRF according to TS 23.203 [4]. The message includes HNB Local IP address and the UDP port number if NAT/NAPT is detected.

4. The PCRF sends the Gateway Control Session establishment message to the BPCF according to TS 23.203 [4]. The message includes the IMSI, HNB local IP address, the UDP port number if NAT/NAPT is detected.

Once this step completes the PCRF is aware the fact that the UE is connected to the network via a 3GPP H(e)NB and checks first whether sufficient resources are available in the BBF access before it provisions PCC rules at the P-GW.

5. The PCRF acknowledges the IP-CAN session establishment ack to the P-GW.

6. This step is the same as step D in TS 23.060 [22] clause 9.2.2.1A Figure 64a with the following additions. If the local H(e)NB IP address and UDP port number information change reporting triggers are received from the PCRF, the PDN GW should set the H(e)NB local IP address and UDP port number reporting accordingly. If the

H(e)NB local IP address and UDP port number Reporting Request is received for this PDP context, then the SGSN shall report to the PCEF/PCRF changes of HNB local IP address and/or port (if available).

7-8. Steps 7 and 8 are the same as steps 4-9 in TS 23.060 [22] clause 9.2.2.1 Figure 64.

Editor's note: In order to handle mobility from macro cells, the tunnel information needs to be added in other RANAP messages (RELOCATION COMPLETE and INITIAL UE MESSAGE).

9.3.2 Secondary PDP Context Activation and PDP Context Modification Procedure

This procedure is executed when secondary PDP context is activated and QoS needs to be allocated to it or when PDP context/bearer is modified and its QoS needs to be updated. This clause contains the following cases:

- Secondary PDP Context Activation Procedure, PDP Creation part, using S4 (TS 23.060 [22], clause 9.2.2.1.1A).
- Network Requested Secondary PDP Context Activation Procedure using S4 (TS 23.060 [22], clause 9.2.2.3A).
- SGSN-Initiated EPS Bearer Modification Procedure using S4 (TS 23.060 [22], clause 9.2.3.1A and clause 9.2.3.1B).
- P-GW Initiated EPS Bearer Modification Procedure, using S4 (TS 23.060 [22], clause 9.2.3.2A).
- UE-Initiated EPS Bearer Modification Procedure using S4 (TS 23.060 [22], clause 9.2.3.3A , clause 9.2.3.3B and clause 9.2.3.3C).

Depicted in Figure 9.3.2-1 is the corresponding procedure. It only shows the changed steps, and the steps without change can be referred to the corresponding clauses in TS 23.060 [22].

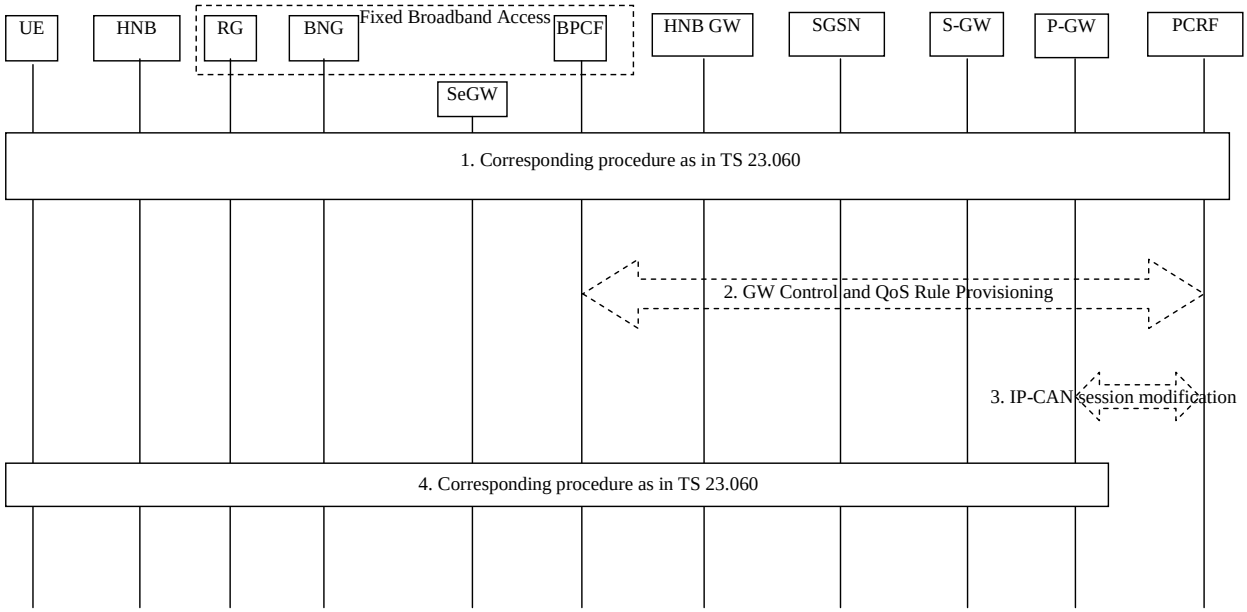

Figure 9.3.2-1: Secondary PDP context Activation or PDP Context Modification Procedure for EPS-connected 3G access

1. This step is the same as the corresponding procedure in TS 23.060 [22].

   For UE-Initiated secondary PDP context activation procedure, refer to steps A and B in TS 23.060 [22], clause 9.2.2.1.1A. For UE-Initiated bearer modification procedure, refer to clause 9.2.3.3A, Figure 72c. For SGSN-Initiated bearer modification procedure, refer to steps A and B in clause 9.2.3.1A, Figure 70c. For all cases, the P-GW sends a QoS authorization request to the PCRF.

2. The PCRF initiates Gateway control and QoS rule provision procedure with the BPCF in order to update the resources allocation in the BBF access network as per TS 23.203 [4], Annex P.7.4.1.

3. IP-CAN session modification procedure is performed by the PCRF to provide PCC rule(s) to the P-GW.

4. The execution and response part of UE-Initiated secondary PDP context activation are the same as steps C to F in TS 23.060 [22], clause 9.2.2.1.1A. For network requested secondary PDP context activation, refer to clause 9.2.2.3A. For UE-Initiated bearer modification procedure, refer to clause 9.2.3.3B and clause 9.2.3.3C. For SGSN-Initiated bearer modification procedure, refer to steps C and D in clause 9.2.3.1A. For P-GW or PCRF-Initiated bearer modification procedure, refer to clause 9.2.3.2A.

9.3.3 Detach, PDP Context and EPS-Bearer Deactivation Procedures

This procedure is executed when the PDP context or EPS-bearer is released. This clause contains the following cases:

- SGSN interaction during Detach Procedure when using S4 (clause 6.6.3, TS 23.060 [22])
- UE and SGSN Initiated PDN connection Deactivation Procedure using S4 (clause 9.2.4.1A.1, TS 23.060 [22])
- UE and SGSN Initiated Bearer Deactivation Procedure (clause 9.2.4.1A.2, TS 23.060 [22])
- P-GW initiated Bearer Deactivation Procedure using S4 (clause 9.2.4.3A and clause 9.2.4.3B, TS 23.060 [22])

Depicted in Figure 9.3.4-1 is the Detach or PDP Context/Bearer Deactivation procedure. It only shows the changed steps, and the steps without change can be referred to the corresponding clauses in TS 23.060 [22].

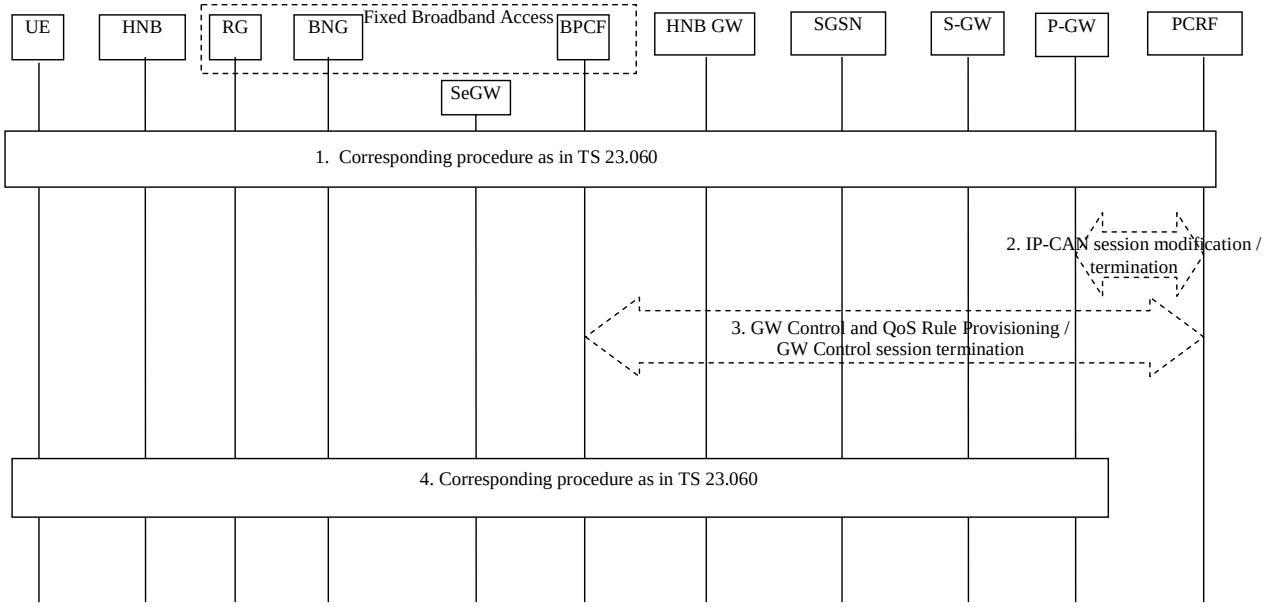

Figure 9.3.3-1: PDP Context/Bearer Deactivation Procedure for EPS-connected 3G access

1. This step is the same as the corresponding procedure in TS 23.060 [22]. (For Detach procedure, refer to steps A and B in clause 6.6.3; For UE or SGSN initiated PDN connection deactivation, refer to steps A and B in clause 9.2.4.1A.1; For UE or SGSN initiated bearer deactivation, refer to steps A and B in clause 9.2.4.1A.2).

2. For the UE detaches from the network or the PDN connection deactivation case, the P-GW initiates IP-CAN session termination with the PCRF. Otherwise, the P-GW initiates IP-CAN session modification with the PCRF.

3. The PCRF initiates the Gateway Control and QoS Rule provision procedure or the Gateway control session termination with the BPCF in order to release resources in the BBF access network as per Annex P.7.4.1, TS 23.203 [4].

4. This step can refer to the corresponding procedure as in TS 23.060 [22]. For Detach procedure, refer to Steps C and D in clause 6.6.3. For UE or SGSN initiated bearer deactivation, refer to Steps C to F in clause 9.2.4.1A.2. For UE or SGSN initiated PDN connection deactivation, refer to Steps C and D in clause 9.2.4.1A.1. For P-GW or PCRF initiated bearer deactivation, refer to clause 9.2.4.3A and clause 9.2.4.3B.

9.3.4 Service Request and Handover Procedures

This clause specifies the Service Request and Handover Procedures with updating the following information to fixed broadband access network: the HNB local IP address and the UDP port if NAT/NAPT is detected.

This clause contains the following cases:

- Inter SGSN Routeing Area Update and Combined Inter SGSN RA / LA Update using S4 (TS 23.060 [22], clause 6.9.1.2.2a).
- Routeing Area Update Procedure using S4 (TS 23.060 [22], clause 6.9.2.1a).
- Serving RNS Relocation Procedure, Combined Hard Handover and SRNS Relocation Procedure, and Combined Cell / URA Update and SRNS Relocation Procedure Using S4 (TS 23.060 [22], clause 6.9.2.2.1a).
- Enhanced Serving RNS Relocation Procedure using S4(TS 23.060 [22], clause 6.9.2.2.5a).
- UE Initiated Service Request Procedure Using S4(TS 23.060 [22], clause 6.12.1A).
- Iu mode to A/Gb mode Intra SGSN Change using S4(TS 23.060 [22], clause 6.13.1.1.2).
- A/Gb mode to Iu mode Intra-SGSN Change using S4 (TS 23.060 [22], clause 6.13.1.2.2).
- Iu mode to A/Gb mode Inter-SGSN Change using S4 (TS 23.060 [22], clause 6.13.2.1.2).
- A/Gb mode to Iu mode Inter-SGSN Change using S4 (TS 23.060 [22], clause 6.13.2.2.2).

Depicted in Figure 9.3.5-1 is the service request or handover procedure. It only shows the changed steps, and the steps without change can be referred to the corresponding clauses in TS 23.060 [22].

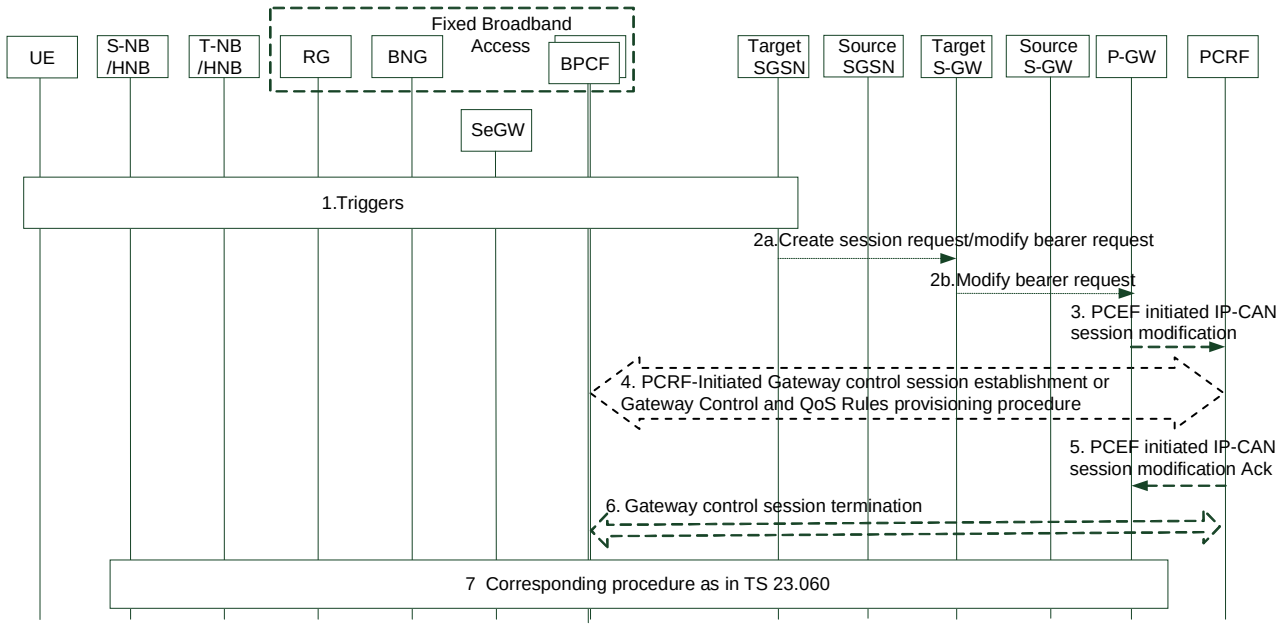

Figure 9.3.4-1: Service Request and Handover Procedures for EPS-connected 3G access

1. UE initiated Service request procedure or Handover procedure, which can be referred to the descriptions of the corresponding clause in TS 23.060 [22], with the addition that target HNB sends the target HNB local IP address and the UDP port if NAT/NAPT is detected to the target SGSN in the [RANAP] RELOCATION COMPLETE message or ENHANCED RELOCATION COMPLETE REQUEST message (for the messages refer to TS 25.413 [28]).

2. Step 2a and 2b are the same as that in TS 23.060 [22]:

   2a. If there is a change in S-GW, the target SGSN sends the Create session request message to the target S-GW. If the S-GW is not changed, the (target) SGSN sends the modify bearer request message to the S-GW. The

following information may be included: target HNB Local IP address and the UDP port if NAT/NAPT is detected.

2b. The (target) S-GW sends the modify bearer request message to the P-GW, based on conditions specified in TS 23.401 [2] (e.g. the S-GW is changed) or if the following information is received in step 2a: target HNB Local IP address and the UDP port if NAT/NAPT is detected.

3. The P-GW sends IP-CAN session modification request message to the PCRF including the Target HNB local IP address and the UDP port if NAT/NAPT is detected as defined in TS 23.203 [4], Annex P.7.4.1.

   If the Modify bearer Request message received by P-GW in step 3 contains none of the additional information: HNB Local IP address and the UDP port if NAT/NAPT is detected., the P-GW determines that the UE leaves the H(e)NB and will inform this event to PCRF.

4. If the UE moves from macro NB to a HNB, or the PCRF will initiate PCRF-initiated Gateway control session establishment procedure as defined in TS 23.203 [4] if the UE is the first UE attaching the target HNB; if the UE moves from one HNB to another HNB without fixed network backhaul changed or if the UE moves to a new HNB and there has been one Gateway Control Session for that HNB, the PCRF will initiate Gateway control and QoS rule provisioning procedure with BPCF as defined in TS 23.203 [4]. The HNB local IP address, the UDP port if NAT/NAPT is detected, shall be included in the PCRF-Initiated Gateway control session establishment procedure and in Gateway Control and QoS rule provisioning procedure.

5. The PCRF acknowledges the IP-CAN session modification.

6. If UE moves from one HNB to macro cell, the PCRF will terminate the old Gateway control session if this is the last UE under the source HNB; if the UE moves from macro NB to a HNB, or the UE moves from one HNB to another HNB without fixed network backhaul changed, or there are other UEs attached the source HNB, this step will be skipped.

7. This step can refer to the corresponding procedure as in TS 23.060 [22].

NOTE: The interaction between the BPCF and the BNG is out of scope.

9.4 3GPP HNB procedure - CS support

9.4.0 General

The CS service is provided by the serving network. Therefore, in the roaming case the HNB GW is connected to the V-PCRF and the V-PCRF connects to the BPCF via the S9a interface.

9.4.1 S15 session establishment at HNB registration

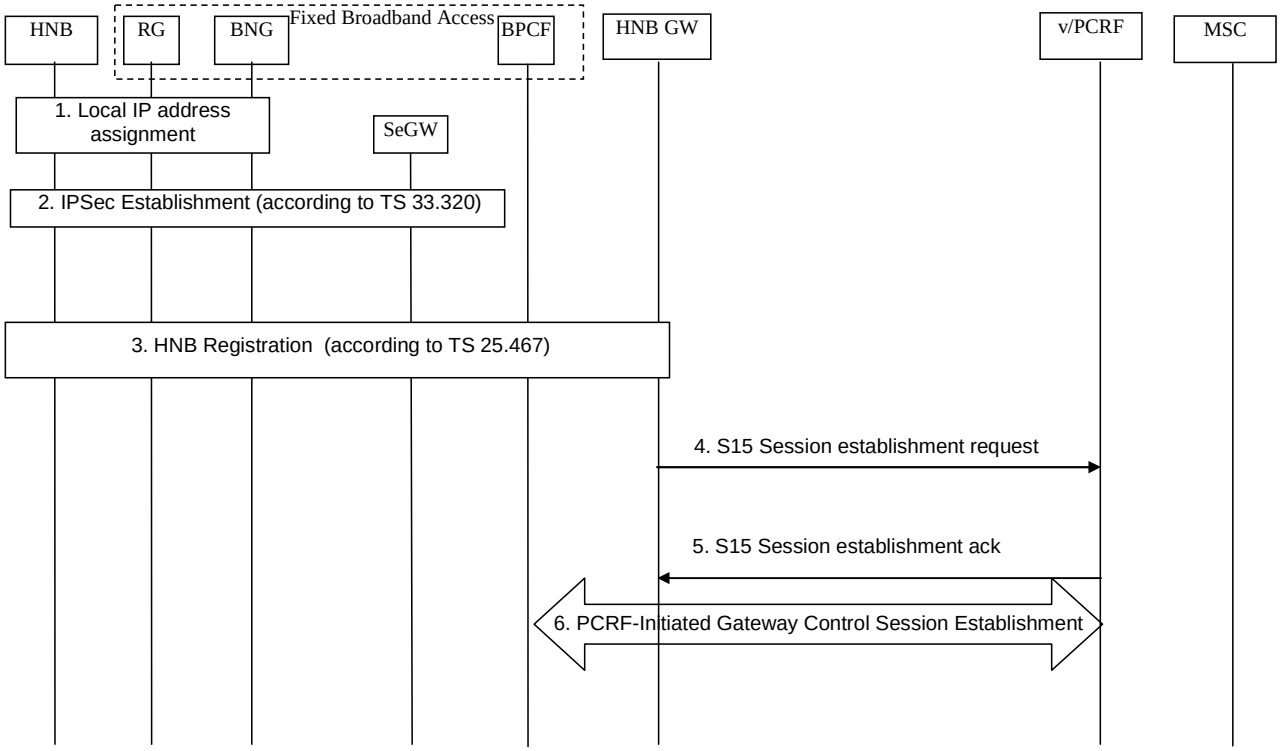

Figure 9.4.1-1: S15 Session Establishment

1) When the HNB powers on, it receives a local IP address from the BBF Access Network. HNB Local IP address assignment by BBF is out of 3GPP scope.

2) The HNB establish IPSec tunnel with SeGW as defined in TS 33.320 [15].

3) The HNB initiates the Registration to HNB GW including HNB IP address, HNB local IP address, and the UDP port number(s) if NAT/NAPT is detected per TS 25.467 [12].

4) The HNB GW initiates the establishment of the S15 session with the v/PCRF and sends the including information about the HNB such as, HNB local IP address and the UDP port number(s) if NAT/NAPT is detected.

5) The PCRF responds to the S15 session establishment request.

6) The PCRF initiates the Gateway Control session Establishment to establish Gateway Control Session and sends the HNB local IP address and optionally the UDP port number(s) if NAT/NAPT is detected to the BPCF according to TS 23.203 [4], Annex P.

9.4.2 HNB GW initiated S15 session modification

This procedure is executed when the first UE or a subsequent UE connecting to a HNB requests a CS call.

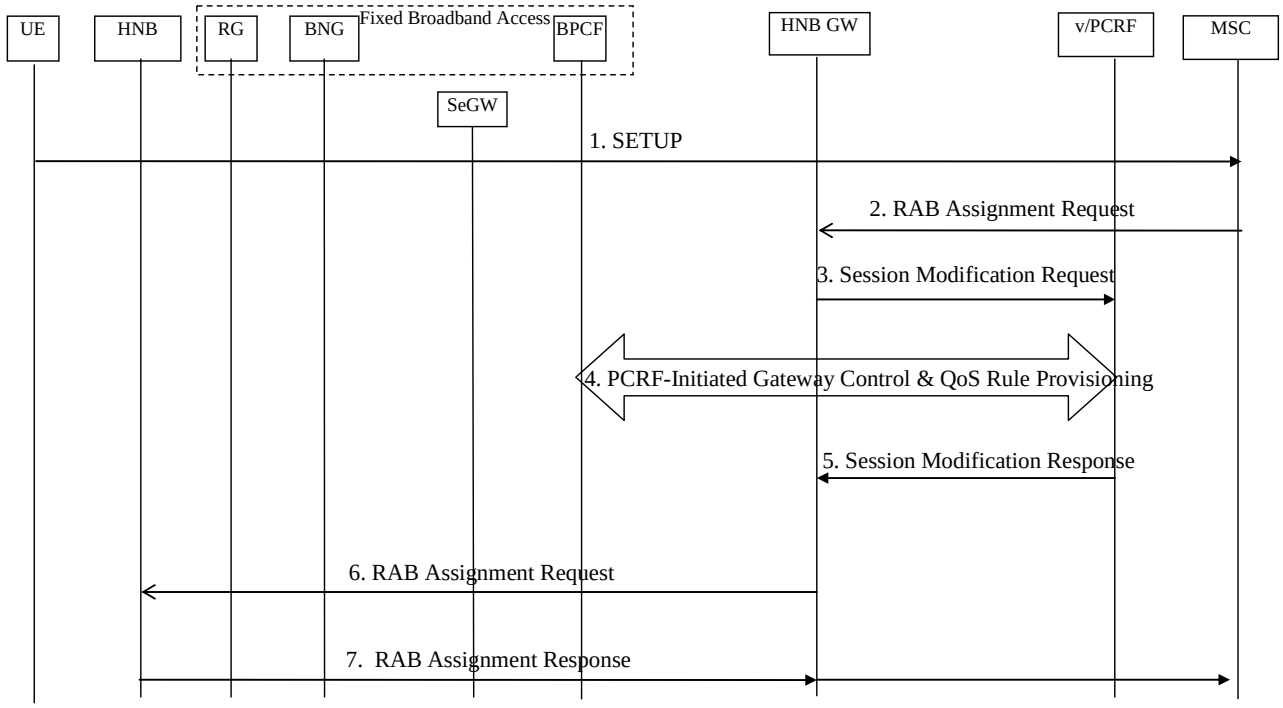

Figure 9.4.2-1: HNB GW initiated S15 session modification

NOTE: This flow does not include all the steps associated with CS call setup.

1) The UE initiates call setup to the MSC using a SETUP message.

2) The MSC sends a RAB Assignment Request message towards the HNB.

3) The HNB GW intercepts the RAB assignment message and sends the S15 session modification message to the PCRF that includes the HNB Local IP address, the UDP port number(s) if NAT/NAPT is detected and the QoS information derived from the RAB message.

4) The PCRF initiates the GW Control and QoS Rules Provisioning procedure according to TS 23.203 [4], Annex P.

5) The PCRF responds with the outcome of the authorisation request .If no resources are available then the HNB GW rejects the RAB assignment and initiates the "RAB assignment failure" procedure.

6) The HNB GW sends the RAB assignment message to the HNB.

7) The remainder of the call setup procedure completes.

9.4.3 S15 session termination

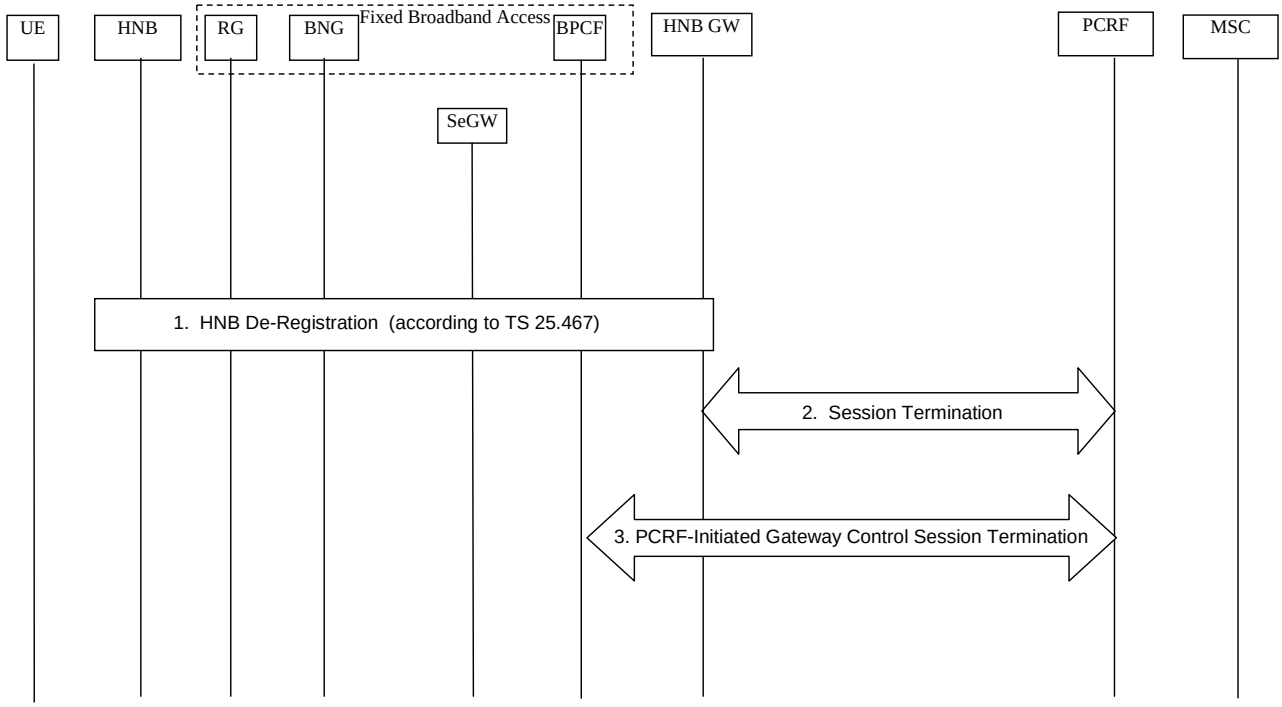

Figure 9.4.3-1: S15 session Release

1) The HNB GW initiates/receives a Deregistration request for the HNB per TS 25.467 [12].

2) The HNB GW requests S15 session termination to the PCRF.

3) The PCRF initiates the GW control session termination over S9a toward the BPCF per TS 23.203 [4], Annex P and the PCRF acknowledges the request for termination of S15 session.

9.4.4 PCRF initiated S15 session modification

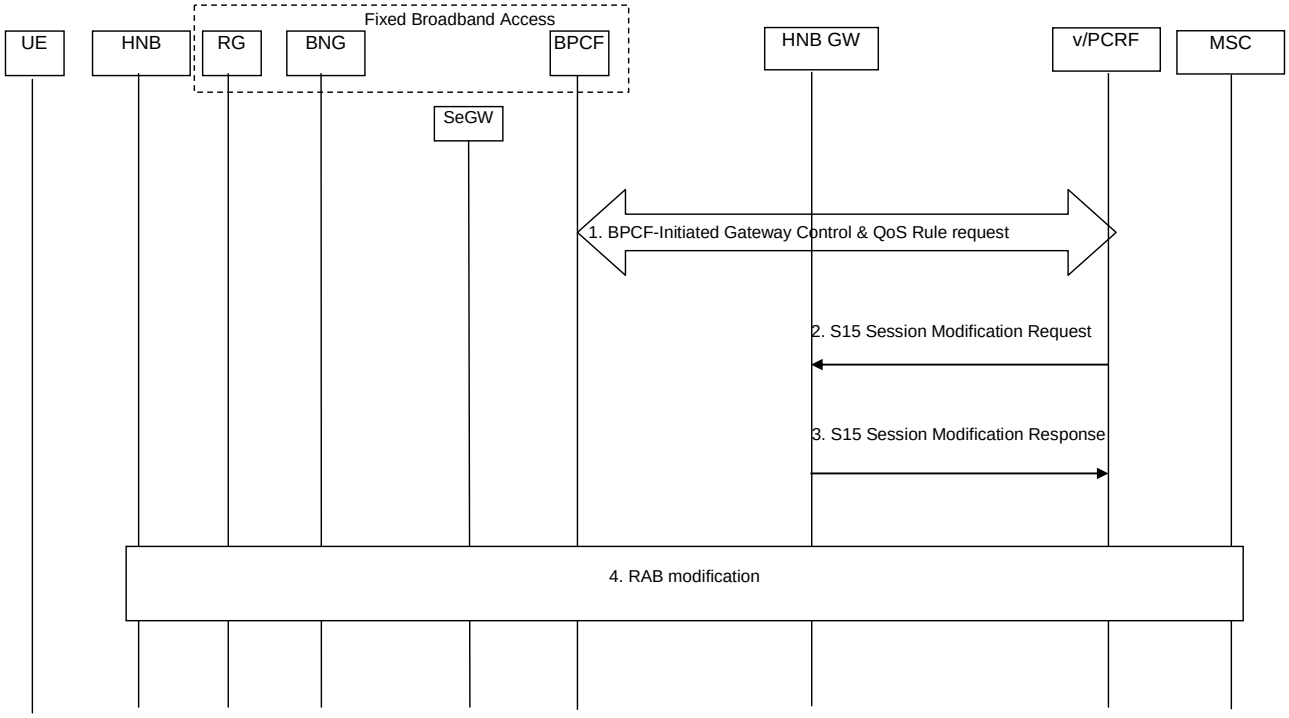

Figure 9.4.4-1: PCRF initiated S15 session modification

1) The BPCF initiates Gateway Control and QoS Rule Request to report QoS Rule failure to (v)PCRF, which can be referred to the corresponding description in step 1 of TS 23.203 [4], clause P.8.4.

2) The (v)PCRF sends the S15 session modification request message to the HNB GW. The (v)PCRF includes the report identifying the QoS Rules that failed and a reason derived from the BPCF.

3) The BPCF response the S15 session modification to the (v)PCRF.

4) Based the trigger got in step 2, the HNB GW initiates the RAB modification which is outside the scope of the present document.

Annex A (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2012-03	SP-55	-	-	-	-	MCC Editorial update to version 11.0.0 after TSG SA Approval (Release 11)	2.0.0	11.0.0
2012-06	SP-56	SP-120241	0001	1	F	Some corrections to the functional description and procedures	11.0.0	11.1.0
2012-06	SP-56	SP-120241	0002	2	F	Correction to UE reflective QoS notification	11.0.0	11.1.0
2012-06	SP-56	SP-120241	0004	2	F	Clarification of accounting requirement and assumptions	11.0.0	11.1.0
2012-06	SP-56	SP-120241	0007	2	F	Corrections on TS 23.139	11.0.0	11.1.0
2012-06	SP-56	SP-120241	0008	3	F	UE local IP address update procedure for S2c case	11.0.0	11.1.0
2012-06	SP-56	SP-120241	0016	1	F	SeGW DL DSCP Marking for EPC Routed Traffic	11.0.0	11.1.0
2012-09	SP-57	SP-120478	0020	1	F	Correction to untrusted S2c procedure	11.1.0	11.2.0
2012-09	SP-57	SP-120478	0024	1	F	Notification of PGW IP address in case of PDN disconnection	11.1.0	11.2.0
2012-09	SP-57	SP-120478	0027	-	F	Corrections of wrong references	11.1.0	11.2.0
2012-12	SP-58	SP-120755	0032	2	F	Correction to UE reflective QoS notification	11.2.0	11.3.0
2013-03	SP-59	SP-130082	0037	2	F	PCRF initiated S15 session modification	11.3.0	11.4.0
2013-03	SP-59	SP-130082	0039	1	F	Alignment of BBAI H(e)NB Local IP Address Signalling with RAN WG3 decisions	11.3.0	11.4.0
2013-06	SP-60	SP-130228	0043	1	B	Conclusion on S2a for P4C_TI	11.4.0	**12.0.0**
2014-09	SP-65	SP-140425	0045	1	F	Correction of figure of DSCP Marking	12.0.0	12.1.0
2015-03	SP-67	SP-150109	0046	-	F	Corrections to BBF related references	12.1.0	12.2.0
2015-12	SP-70	SP-150602	0047	1	F	Removal of support of EAP-SIM	12.2.0	12.3.0
2015-12	-	-	-	-	-	Update to Rel-13 version (MCC)	12.3.0	**13.0.0**
2017-03	-	-	-	-	-	Update to Rel-14 version (MCC)	13.0.0	**14.0.0**
2018-06	SP-80	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**
2020-07	SP-88E	-	-	-	-	Update to Rel-16 version (MCC)	15.0.0	**16.0.0**
2022-03	SP-95E	-	-	-	-	Update to Rel-17 version (MCC)	16.0.0	**17.0.0**
2024-03	-	-	-	-	-	Update to Rel-18 version (MCC)	17.0.0	**18.0.0**
2025-09	-	-	-	-	-	Update to Rel-19 version (MCC)	18.0.0	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication