3GPP TR 23.839 V2.0.0 (2013-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Support of BBF Access Interworking (Release 12)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
3GPP, Broadband, BBAI

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2013, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword

This Technical Report 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.

Introduction

The collaborative work between 3GPP and BBF resulted in a Workshop in February 2010 focusing on Fixed -Mobile Convergence. As a result of this work, it has been identified that several working groups in 3GPP will need to work on: requirements, architecture, security and OA&M. This TR focuses on the architecture aspects of this study. The work includes three building blocks containing specific aspects of the study which are to be conducted within this technical report.

1 Scope

Based on requirements documented in the stage 1 specifications, this technical report addresses system architecture impacts to support BBF Access Interworking. The study includes multiple phases and covers aspects such as basic connectivity, mobility, authentication and authorisation, policy and QoS aspects, IP Flow mobility, traffic offload, convergence etc.

In each Building Block, the TR describes what changes are expected to normative TSs, e.g. TS 23.402 [3] and TS 23.203 [4].

The work is divided into three separate Building Blocks. See clause 4 for an outline of the content of each building block.

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 WT-203 "Interworking between Next Generation Fixed and 3GPP Wireless Access" (work in progress).

[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 WT-145 "Multi-service Broadband Network Functional Modules and Architecture " work in progress.

[11] Broadband Forum WT-134 "Policy Control Framework " work in progress.

[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] BBF TR-092: "Broadband Remote Access Server (BRAS) Requirements".

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

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

[23] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking".

[24] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[25] 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS): Applications and interfaces".

[26] IETF Internet-Draft, draft-ietf-netext-pmip6-qos-01: "Quality of Service Option for Proxy Mobile IPv6", work in progress.

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 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 (NS WLAN-offload) is a capability of a UE supporting routing specific IP flows over the WLAN access without traversing the EPC as defined in clause 4.1.5 of TS 23.402 [3].

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.

Fixed Access session: is an abstraction for the connectivity service in BBF network which is related to one fixed network subscriber, irrespective of access type (e.g. IPoE Subscriber Line session, PPPoE session, IP session) or access technology (e.g. copper or fiber). The session can be created and removed dynamically as example, but not limited to, at power on of RG, when a BBF device starts a PPPoE session, A BBF device may have multiple sessions in series or in parallel if the BBF network supports that**.**

Default QoS for fixed access session: is defined as QoS rules which apply to the entire traffic of a fixed access session. Default QoS is installed during session setup and may be modified during the lifetime of fixed access session.

Access Line Identifier is defined as: the identifier of the Line composed by couple Logical Access ID and Physical Access ID.

Logical Access ID contains a Circuit-ID (as defined in RFC 3046). The Logical Access ID may explicitly contain the identity of the Virtual Path and Virtual Channel carrying the traffic.

Physical Access ID Identifies the physical access to which the user equipment is connected. Includes a port identifier and the identity of the access node where the port resides.

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
BBF	Broadband Forum
BRAS	Broadband Remote Access Server
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
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
P-GW	PDN Gateway
PMIP/PMIPv6	Proxy Mobile IP version 6
RG	Residential Gateway
S-GW	Serving GW
V-ANDSF	Visited-ANDSF

4 Building Blocks

The architecture study is planned to be performed within three Building Blocks, with the following scope for each BB.

Editor's note: The text below is copied from the Work Item Description.

The following aspects will be covered in Building Block I:

- Aspects on basic connectivity, host-based mobility (S2c), and network-based mobility for untrusted accesses (S2b) on top of Release 10 baseline architecture including network discovery/selection functions and IP address allocation;
- Interworking between 3GPP and BBF architectures for authentication, including identities, on top of Release 10 baseline architecture;
- Policy and QoS interworking between 3GPP and BBF architectures considering the following scenarios:
  - When H(e)NB is being used and traffic is routed back to the EPC;
  - When WLAN is being used and traffic is routed back to the EPC;
- Multi-access PDN Connectivity;
- IP Flow Mobility and seamless WLAN offloading;

The following aspects will be covered in Building Block II (building on interworking functionality of Building Block I):

- Policy and QoS interworking between 3GPP and BBF architectures considering the following scenarios:
  - When WLAN is being used and traffic is offloaded in the local wireline network (i.e. non-seamless WLAN offloading).

The following aspects will be covered in Building Block III (building on overall results of Building Block I):

- Converged policy management and charging for the scenarios with traffic routed to EPC and offloaded at the BBF access network for operators providing both 3GPP and BBF accesses.

NOTE: For the offloading scenarios only WLAN offloading will be considered in this release.

5 Building Block I

Editor's note: This clause will contain items being part of Building Block I.

Editor's note: This clause may not be up-to-date; please refer to the normative TS 23.139 and TS 23.203 [4] for up-to-date content.

5.1 Architecture

Editor's note: This clause will identify the architectural requirements and assumptions as well as architecture common for building block I. Intent is to capture the architectural agreements made during the 3GPP-BBF WS.

Editor's note: If the work with the proceeding building blocks concludes that some or all architectural requirements and assumptions can be applied to several building blocks then those can be moved to a new chapter outlining a baseline architecture for all building blocks.

5.1.1 Architectural requirements and assumptions for building block I

The interworking architecture is based EPC reference architecture defined in TS 23.401 [2] and TS 23.402 [3] and on BBF access network defined by BBF TR-058 [7], BBF TR-101 [8], WT-134 [11].

The interworking architecture supports trusted and untrusted model for the host-based mobility (S2c) and the network based mobility for the untrusted model based on s2b. The trusted/untrusted Non-3GPP access network detection is performed as defined in clause 4.1.4 of TS 23.402 [3].

The architecture supports an 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 an 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 reference architecture for the support of HeNB is 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].

5.1.2 Architecture for building block I BBF interworking via WLAN access connection

5.1.2.1 Architecture reference model

Figures 5.1.2.-1, 5.1.2-2 and 5.1.2-3 show the reference architecture for the non-roaming scenario and with the traffic routed to the mobile core network. Figures 5.1.2-4. 5.1.2-5 and 5.1.2-6 show the reference architecture for the roaming scenario with the traffic routed to the home network. Figures 5.1.2-7, 5.1.2-8 and 5.1.2-9 show the reference architecture for the roaming scenario with the local breakout in Visited PLMN.

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.

- Gxb* is only needed in untrusted s2c and PMIP-s2b cases where the ePDG uses Gxb* to trigger the PCRF to initiate the S9a session establishment towards the BPCF. Clause 5.2.2.1.2 contains additional details regarding S9a session establishment.

- S2b is enhanced to carry UE location information (UE local IP address) in cases where information provided in S2b and Gx triggers the PCRF to initiate the S9a session establishment towards the BPCF. Clause 5.2.2.1.2 contains additional details regarding S9a session establishment.

- S9 is used between the hPCRF and vPCRF in roaming scenario.

- S9a (used between 3GPP and BBF domains) is used between the PCRF and BPCF* in scenarios where both 3GPP and BBF access networks belong to the same operator or to different operators.

- the reference points internal to the BBF access network are defined or are under definition by Broadband Forum and are out of the scope of this Technical Report.

NOTE 1: SWu shown in Figure 5.1.2-1 also applies to architectural reference for untrusted scenario in Figures 5.1.2-3, 5.1.2-4, 5.1.2-6, 5.1.2-7 and 5.1.2-9, 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].

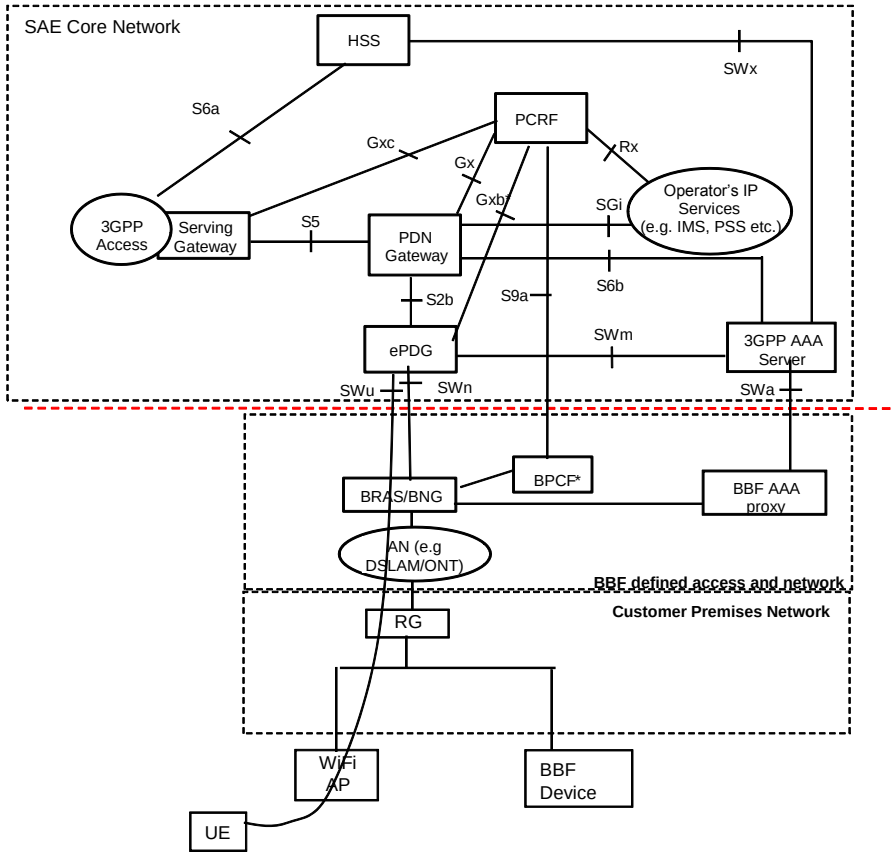


Figure 5.1.2-1: Non-Roaming Architecture for untrusted BBF access network based on S2b

NOTE 2: The reference architecture is applicable when the 3GPP and BBF access networks belongs to the same network operator or to different network operators.

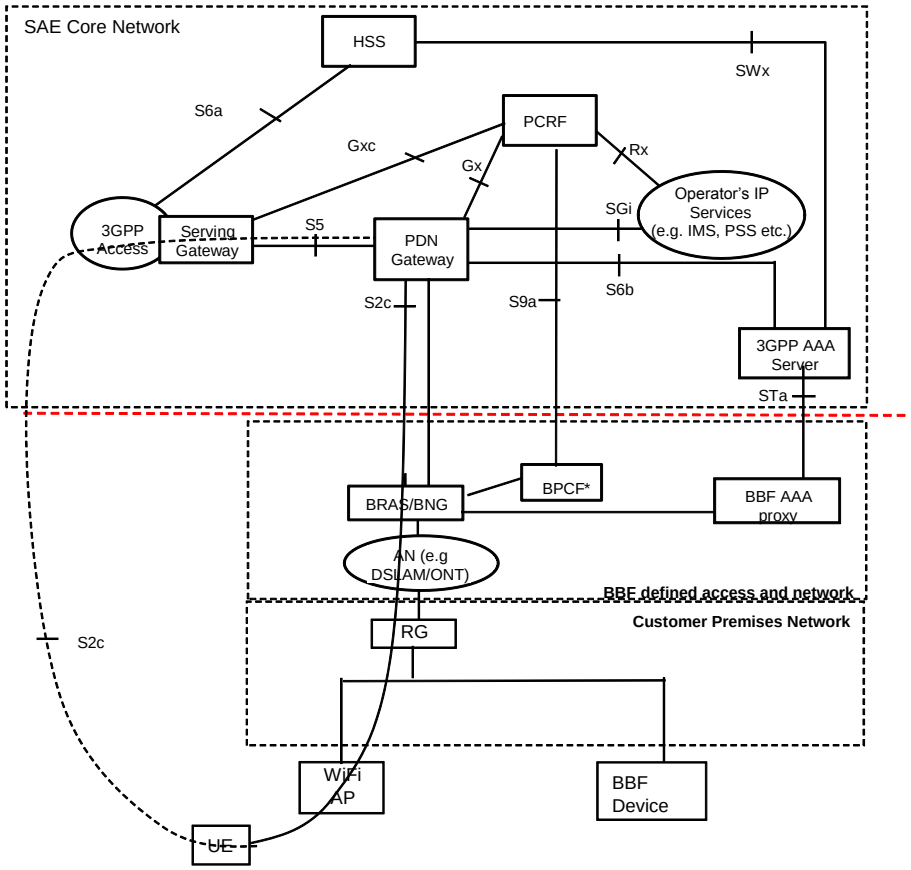


Figure 5.1.2-2: Non-Roaming Architecture for trusted BBF access network based on S2c

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

NOTE 4: The connection between the BRAS/BNG and PDN Gateway is IP transport connection.

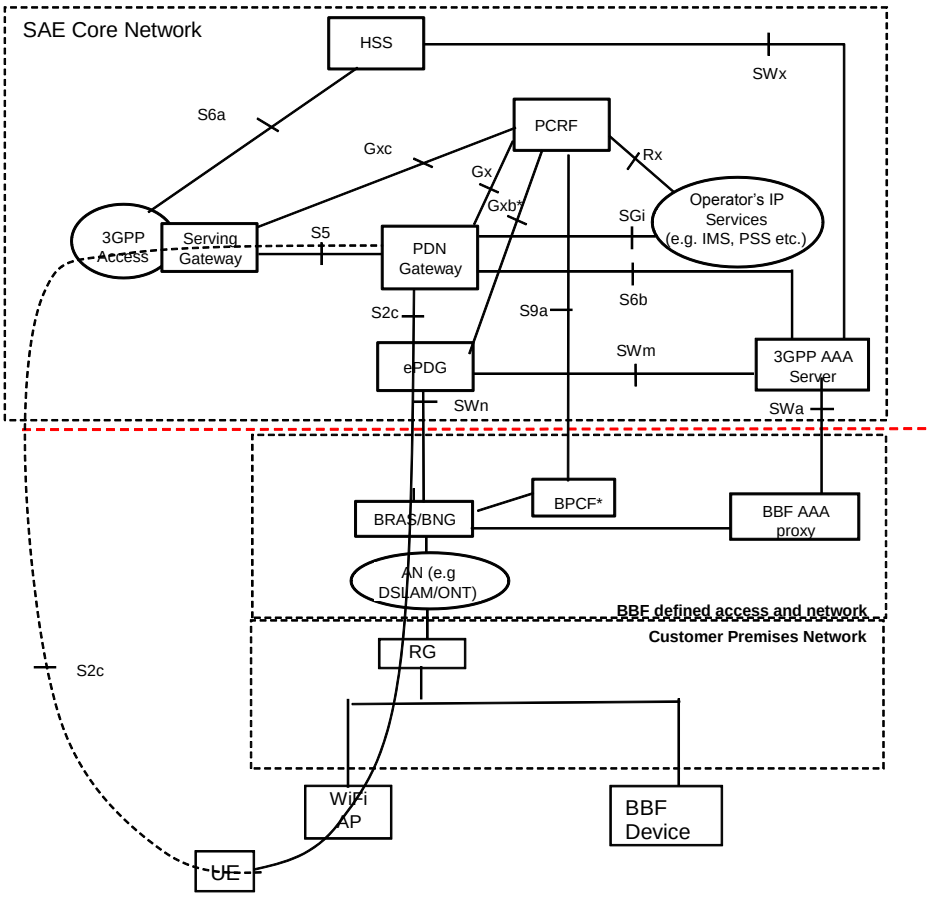


Figure 5.1.2-3: Non-Roaming Architecture for untrusted BBF access network based on S2c

NOTE 5: The reference architecture is applicable when both 3GPP and BBF network belongs to the same network operator or to different network operators.

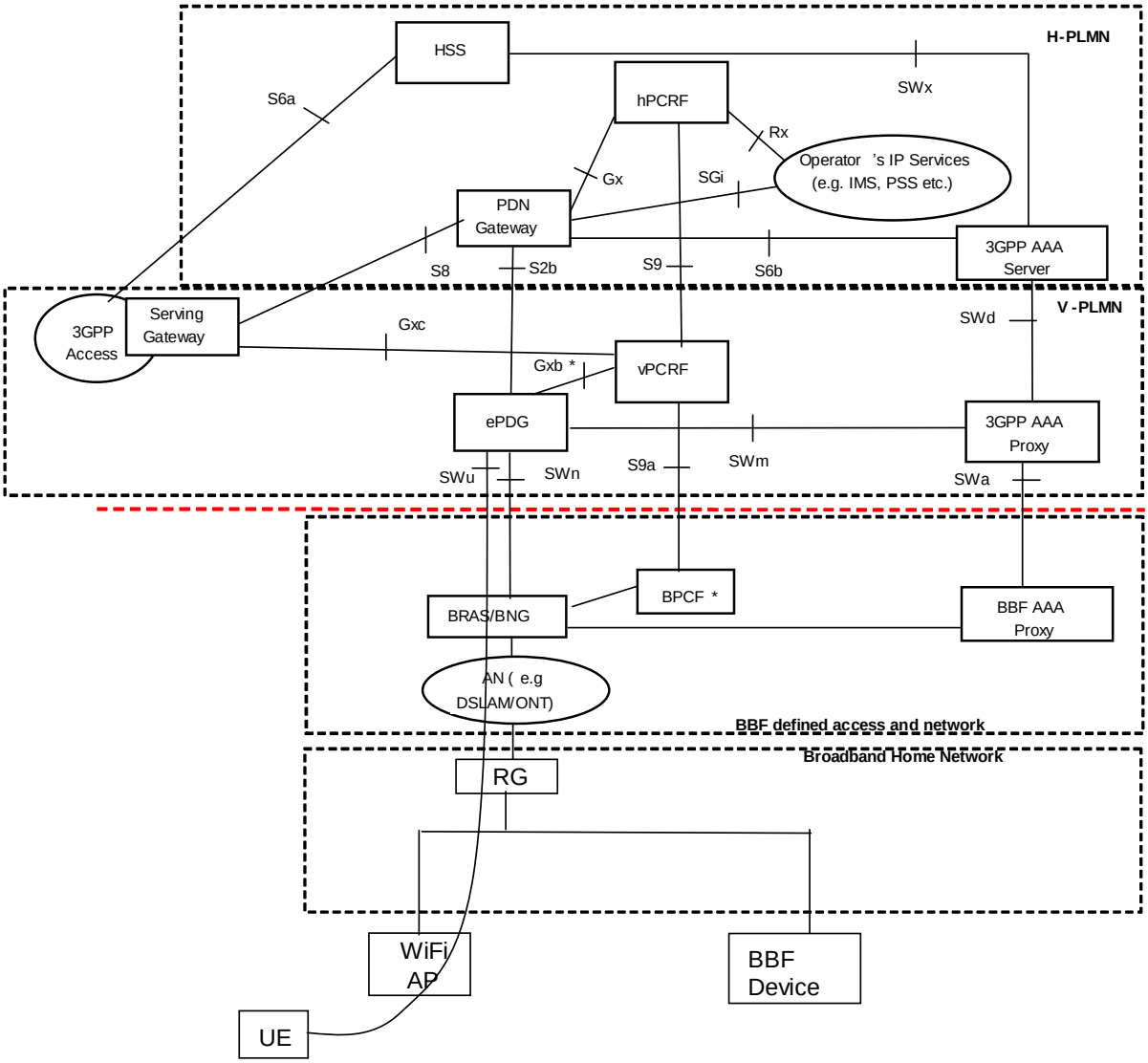


Figure 5.1.2-4: Roaming Architecture for untrusted BBF access network based on S2b - Home routed traffic

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

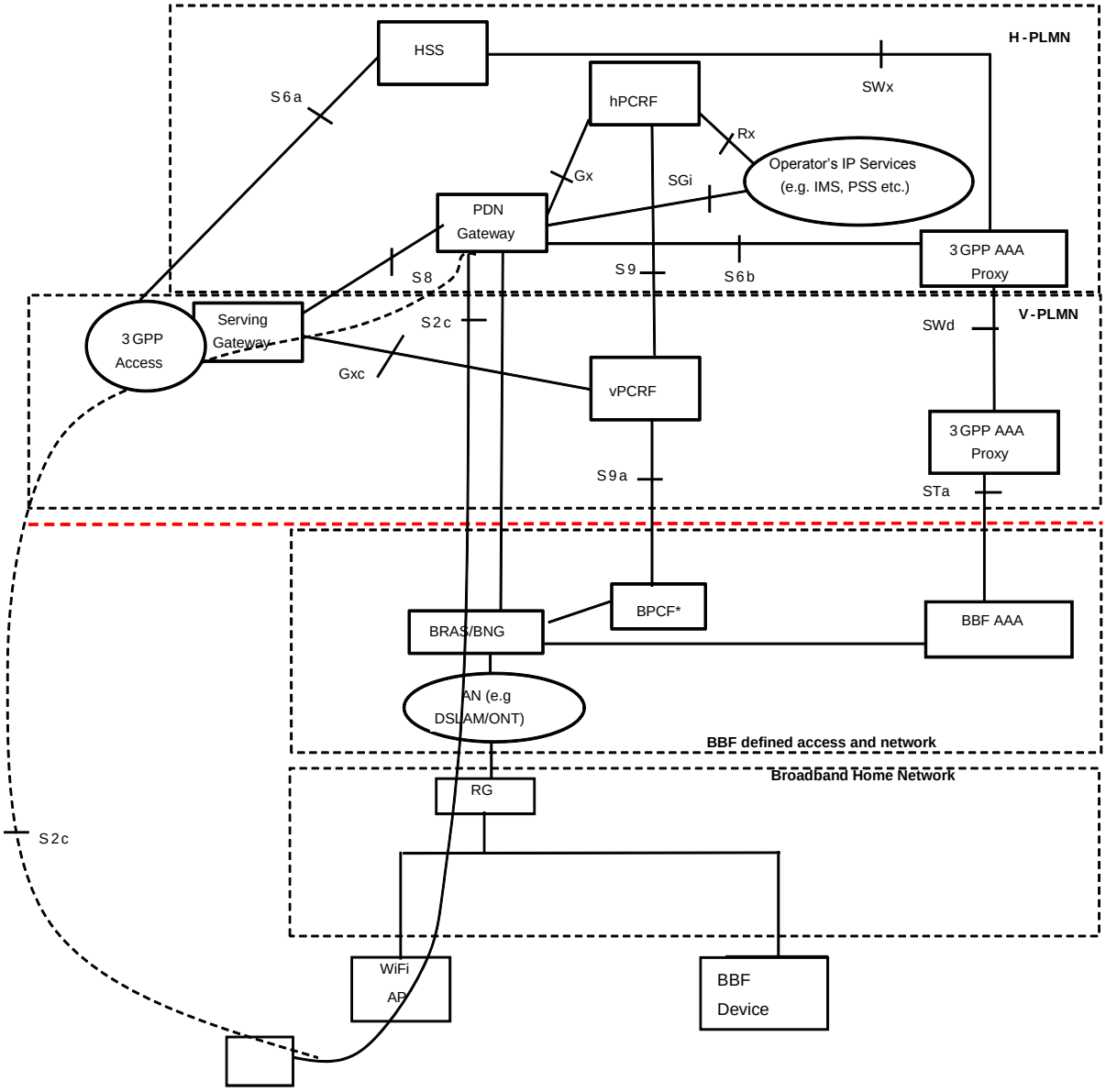


Figure 5.1.2-5: Roaming Architecture for trusted BBF access network using s2c - Home Routed

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

NOTE 8: The connection between the BRAS/BNG and PDN Gateway is an IP transport connection.

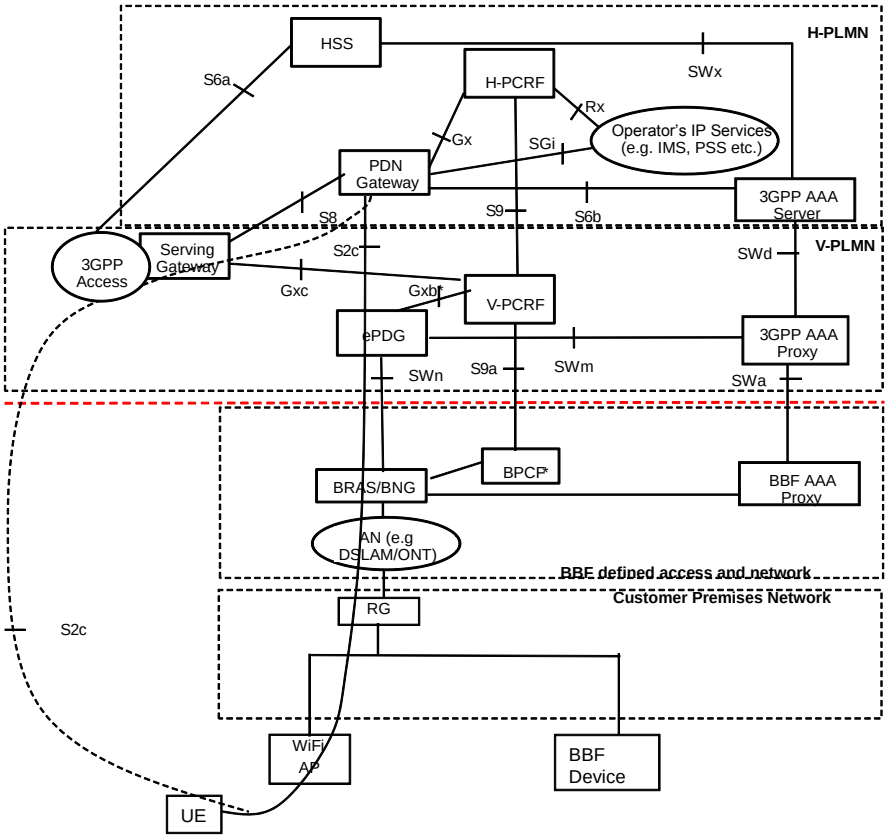


Figure 5.1.2-6: Roaming Architecture for untrusted BBF access network using s2c - Home Routed

NOTE 9: The reference architecture is applicable when both 3GPP and BBF network belongs to the same VPLMN network operator or to different network operators.

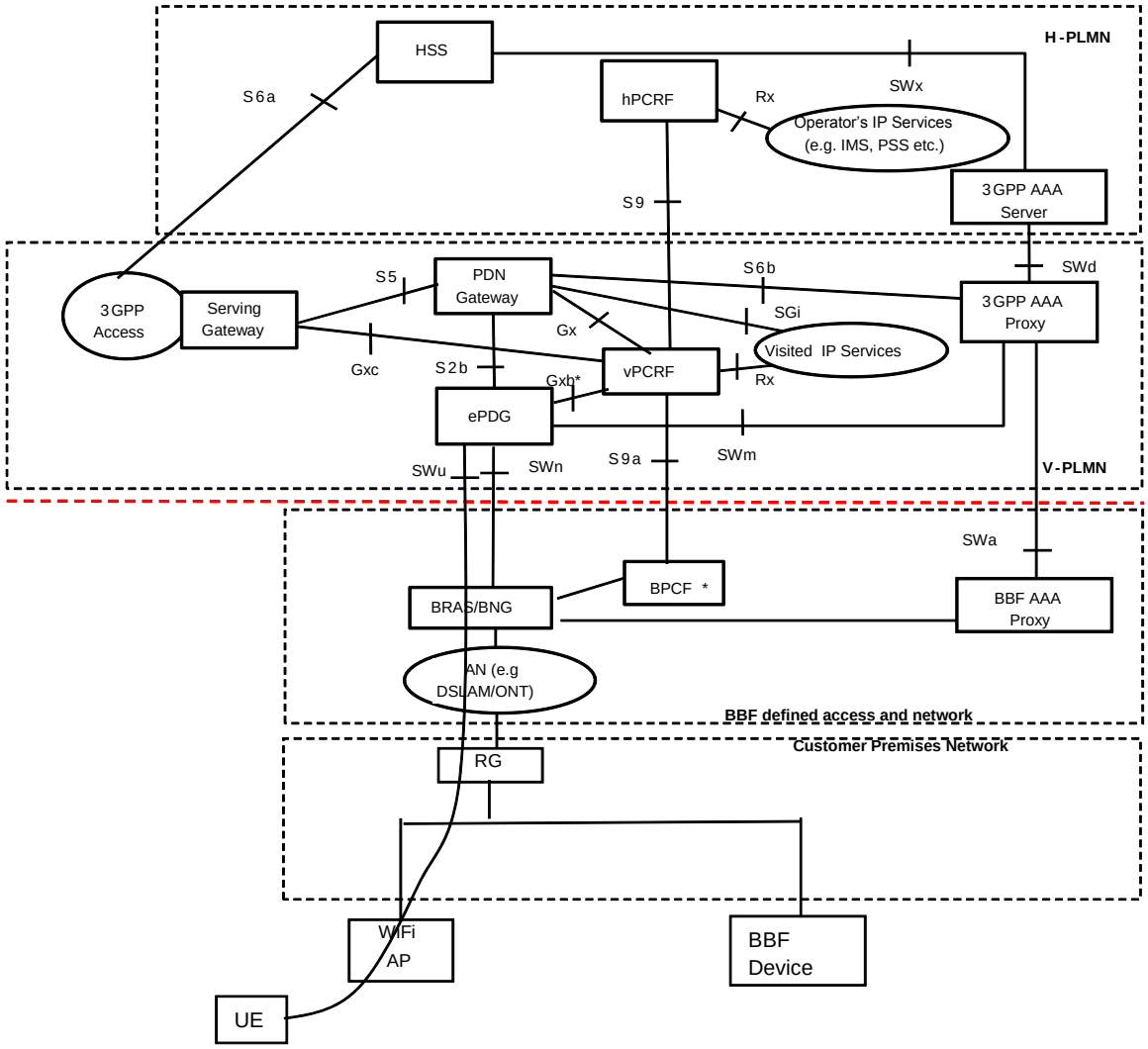


Figure 5.1.2-7: Roaming Architecture for untrusted BBF access network using s2b - Local breakout in V-PLMN

NOTE 10: The two Rx instances in Figure 5.1.2-7 apply to different application functions in the HPLMN and VPLMN.

NOTE 11: The reference architecture is applicable when both 3GPP and BBF network belongs to the same VPLMN network operator or to different network operators.

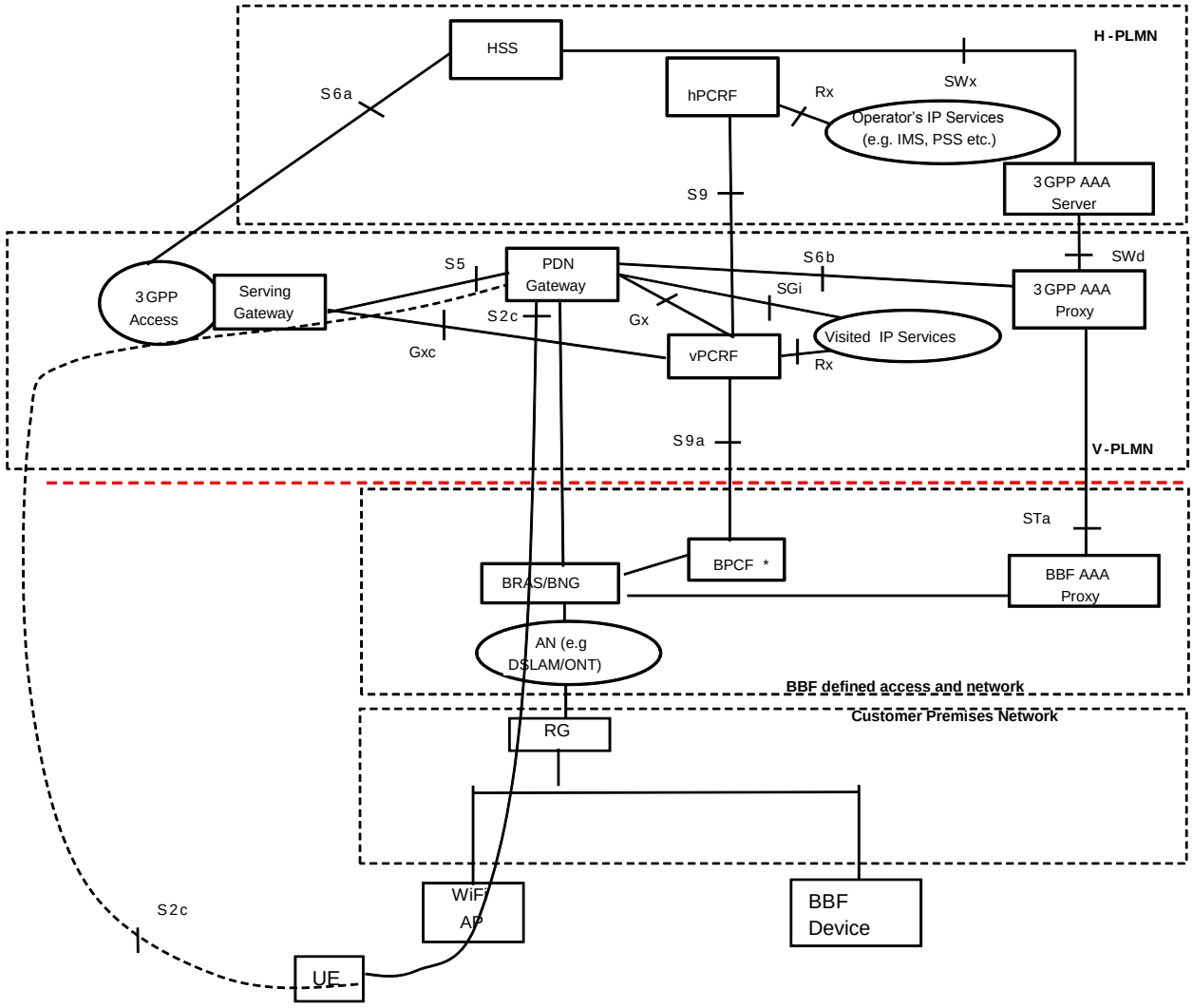


Figure 5.1.2-8: Roaming Architecture for trusted BBF access network using s2c - Local breakout in V-PLMN

NOTE 12: The reference architecture is applicable when both 3GPP and BBF network belongs to the same VPLMN network operator or to different network operators.

NOTE 13: The two Rx instances in Figure 5.1.2-8 apply to different application functions in the HPLMN and VPLMN.

NOTE 14: The connection between the BRAS/BNG and PDN Gateway is a IP transport connection.

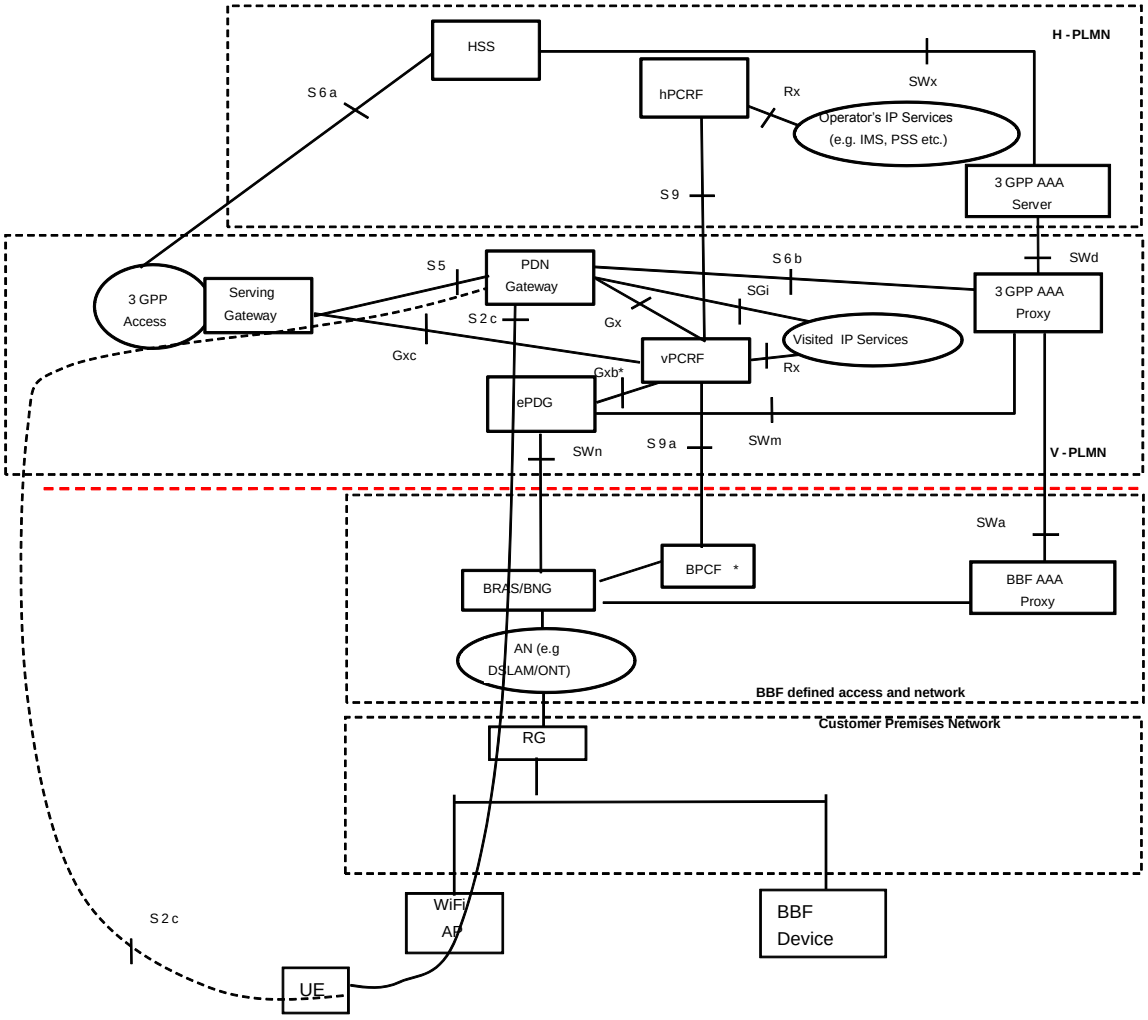


Figure 5.1.2-9: Roaming Architecture for untrusted BBF access network using s2c - Local breakout in V-PLMN

NOTE 15: The reference architecture is applicable when both 3GPP and BBF network belongs to the same VPLMN network operator or to different network operators.

NOTE 16: The two Rx instances in Figure 5.1.2-9 apply to different application functions in the HPLMN and VPLMN.

5.1.2.2 Network Elements

The 3GPP network elements are defined in details in TS 23.401 [2] and TS 23.402 [3].

To support initiation of S9a session from the PCRF when using untrusted access procedures, the ePDG is enhanced to transport the access information of the UE, e.g. the outer header of the IP-sec tunnel, to the PCRF via the Gxb* or the S2b reference points as described in 5.2.2.1.2.

The BBF network elements BRAS, BNG, RG, BPCF* are defined in details in BBF TR-058, TR-101, WT-145 [7] and WT-134 [8].

The BBF device represents any devices defined by broadband Forum or supported by BBF access, as a PC, Media centre, etc, and they are considered outside the scope of 3GPP.

NOTE: The definition of BPCF* for enhancements to support Policy & QoS interworking with mobile networks is under discussion in BBF WT-134 [8].

5.1.2.3 Reference Points

The reference point S1-MME, S1-U, S3, S4, S10, S11 are defined in TS 23.401 [2]. The reference points S2b, S2c, S6a, S6b, SWx, SWa, SWm, SWn, SWu, SGi, Rx, Gxc are defined in TS 23.402 [3].

Gx It provides transfer of dynamic QoS control policies (QoS) and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW.

Gxb* It connects the ePDG with the PCRF and transports access information, e.g. the outer header of the IPSec tunnel. It is only used for scenarios in which the ePDG provides the access information via Gxb* to trigger the PCRF to initiate the S9a session.

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 BBF access network for CS sessions.

S9 It provides transfer of dynamic QoS control policies (QoS) and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function. In all other roaming scenarios, S9 has functionality to provide dynamic QoS control policies from the HPLMN. For BBF interworking for WLAN UE roaming with home routed access and S2b/Gx being used to trigger the PCRF to initiate the S9a session establishment, or for BBF interworking using GTP Home Routed Traffic for H(e)NB, the S9 interface is enhanced to carry from the hPCRF to the vPCRF the IP tunnel information (including UE/H(e)NB local IP address) and/or FQDN of BBF access network at which the H(e)NB is connected to.

S9a For building block 1 it provides transfer of dynamic QoS control policies (QoS) from the Home PCRF to the BBF Policy BPCF and in roaming scenario from the Visited PCRF and to the BBF Policy BPCF function in order to provide the interworking between PCRF and the BBF policy framework. Furthermore the S9a carry from the hPCRF to the vPCRF the IP tunnel information (including UE/H(e)NB local IP address) and/or FQDN of BBF 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.

NOTE: In Building Block 1 traffic is routed back to EPC and charging control is done by HPLMN.

SWa It connects the BBF AAA proxy with the 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information in a secure manner.

STa It connects the BBF AAA proxy with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.

The Reference points within the BBF access network are defined in BBF TR-058, TR-101, WT-145 and WT-134 and they are considered out of the scope of 3GPP.

5.1.3 Architectures for H(e)NB interworking

5.1.3.1 Architecture Alternative 1 - H(e)NB specific policies

5.1.3.1.1 General Principles

The principle behind this architecture assumes that the relationship towards the fixed access is with the mobile network / H(e)NB operator and not individual UEs connecting to the H(e)NB. This is especially true if inbound roamers are permitted to CSG resources.

Since H(e)NB traffic is encapsulated within IPSec whilst traversing the BBF access, the BRAS/BNG is not able to recognise UE specific traffic when using the H(e)NB. The policies in this alternative are defined to be H(e)NB specific and therefore the H(e)NB GW is responsible for the policy interactions.

The normal PCC architecture, servicing UEs, has no direct interaction with the 3GPP-BBF interworking solution.

The architecture highlights the S9a interface between a H(e)NB policy function and the BBF PCF (BPCF) for H(e)NB access. The interface S15 between H(e)NB GW and H(e)NB PF, where then H(e)NB GW provides the policy/QoS requirement to H(e)NB policy function for authorization. The H(e)NB policy function then further requests BPCF for

admission control in BBF network. The H(e)NB policy function performs control based on bearers (EPS bearers or PDP contexts) made visible to it.

The function of the S9a interface is to convey sufficient information to the BPCF to enable it to identify the BNG the H(e)NB connects to, and perform admission control based on the bandwidth requirements and QoS attributes of the bearers or aggregate of bearers with similar QoS characteristics being established.

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

NOTE 1: For HeNB, a HeNB GW may be required to enable BBF interworking.

NOTE 2: UE policies applied at the PCRF and the P-GW are independent of H(e)NB policy function operations.

NOTE 3: There may be 2 S9a sessions for a single UE if the UE is simultaneously connected via H(e)NB and some other access means connected to the same BBF connection e.g. WLAN.

NOTE 4: An assumption is made that a mapping between IP address used by the H(e)NB connection (outer IPSec header) and the H(e)NB is made available to policy architecture.

5.1.3.1.2 Non-Roaming

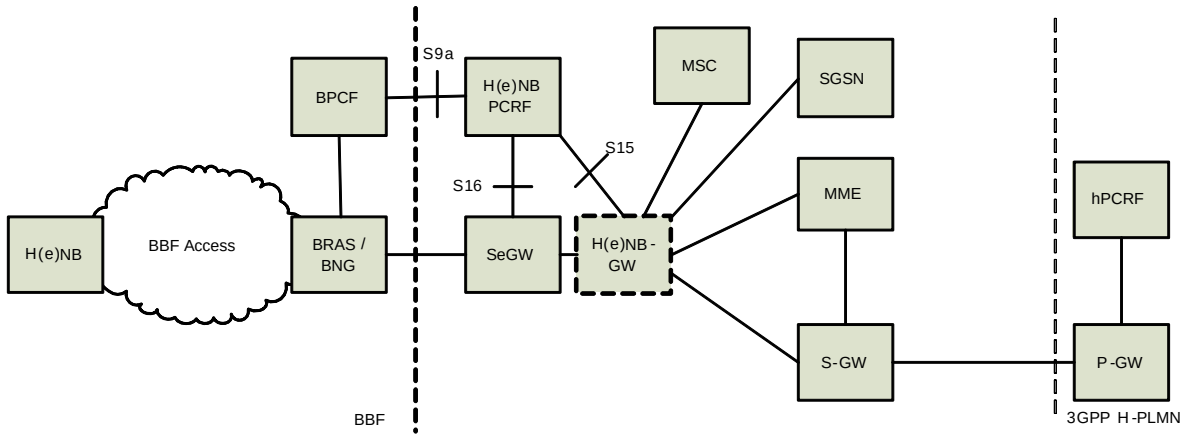


Figure 5.1.3.1.2-1: Non-Roaming

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.2-1.

NOTE 2: The CS domain is not applicable for the HeNB.

NOTE 3: If HeNB GW is not deployed, S15 interface is between H(e)NB Policy Function and MME.

5.1.3.1.3 Roaming - Home Routed Traffic

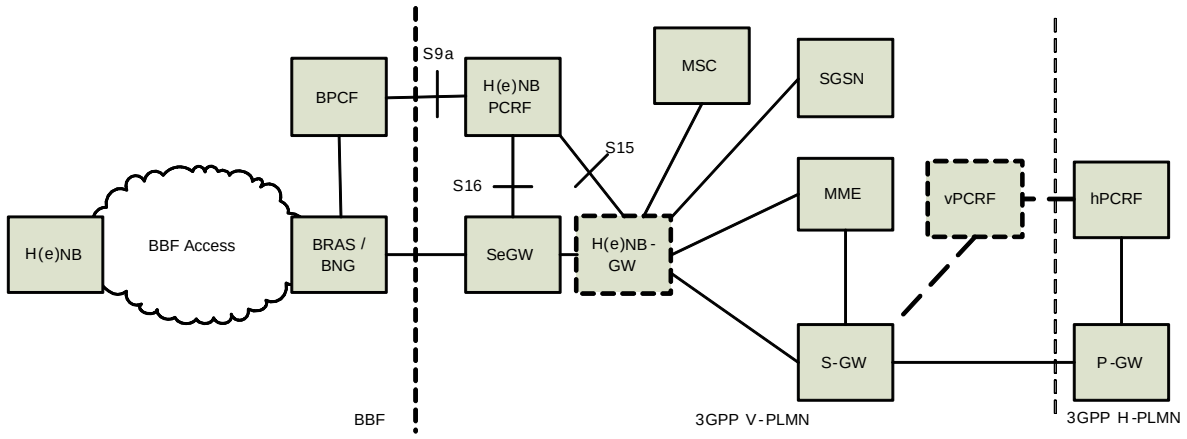


Figure 5.1.3.1.3-1: Roaming - Home Routed Traffic

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.3-1.

NOTE 2: The CS domain is not applicable for the HeNB.

NOTE 3: If HeNB GW is not deployed, S15 interface is between H(e)NB Policy Function and MME.

5.1.3.1.4 Roaming - Visited Access/LBO

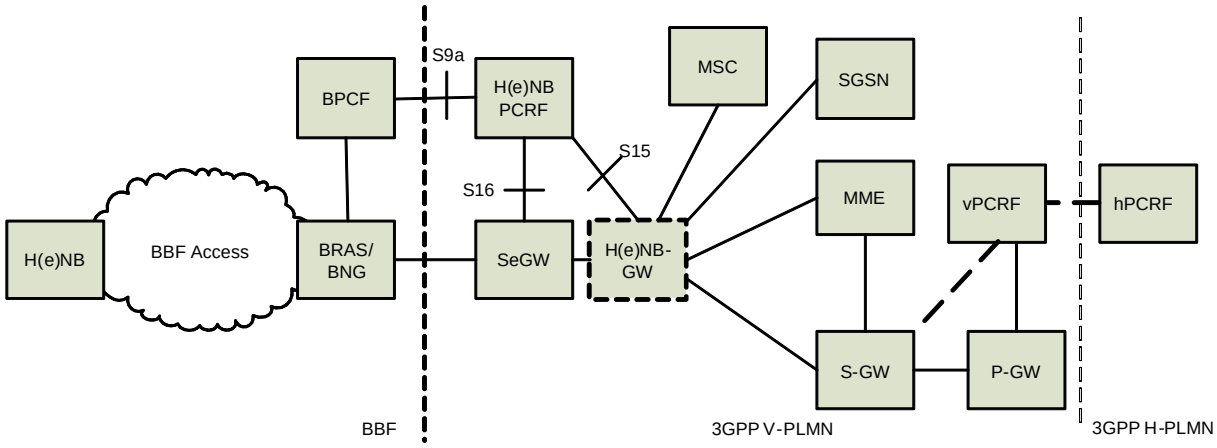


Figure 5.1.3.1.4-1: Roaming - Local breakout

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.4-1.

NOTE 2: The CS domain is not applicable for the HeNB.

NOTE 3: If HeNB GW is not deployed, S15 interface is between H(e)NB Policy Function and MME.

5.1.3.1.5 Interworking functions

5.1.3.1.5.1 H(e)NB policy function

General

The role of the H(e)NB policy function is to convert bearer information (as received on the S1-MME or Iu) into generic QoS authorisation requests. If no BPCF is discovered then the H(e)NB policy function will take no further authorisation decisions and positively acknowledge the bearer action towards the H(e)NB GW / MME.

The H(e)NB Policy Function may apply policies associated with the identified fixed access operator before forwarding any QoS authorisation requests to the BPCFs. The H(e)NB Policy Function may perform one or more of the following:

- Request QoS authorisation on a per bearer basis (e.g. for GBR bearers).
- aggregate a new bearer action into an existing authorisation for the same H(e)NB and not forward the request to BPCF (e.g. for non-GBR bearers where the addition of a bearer does not exceed the resources already authorised).
- aggregate a new bearer action into an existing authorisation for the same H(e)NB and forward the request to the BPCF (e.g. for non-GBR bearers where the new aggregate resource is greater than that which was authorised previously).
- Reject the bearer action if deemed out of policy for H(e)NB operation (e.g. VoIP is not permitted over H(e)NB).

NOTE 1: The H(e)NB policy function may apply different actions depending on whether the request is pertaining to a UE that is accessing the open or closed side of the H(e)NB, but requires the CSG membership to be signalled from the node performing access control. For example, H(e)NB policy may map temporary members / non-members to the lowest priority aggregate whilst a permanent member maps to the highest priority aggregate. The BBF access does not need to be aware of CSG membership status.

NOTE 2: The H(e)NB policy function is a logical function and may be physically located independently, within the H(e)NB GW or within a PCRF.

BPCF discovery

The BPCF is discovered by the H(e)NB policy function using the IP address assigned to the CPE (or H(e)NB if the CPE is operating in bridge mode).

Bearer Handling in H(e)NB Policy Function

In addition to normal bearer admission control performed at the H(e)NB, the H(e)NB Policy Function performs bearer authorization based on resource authorized in the BBF access (either pre-existing, if aggregation is performed, or new authorisations) before passing the bearer action to the H(e)NB. When receiving rejection for a QoS authorization request from BPCF, the H(e)NB Policy Function shall perform pre-emption based on CSG membership and ARP to decide whether to reject or admit the new bearer action, e.g. to allow the emergency call to pre-empt non-emergency call(s) if regulation allows.

NOTE 3: The H(e)NB Policy Function may pre-empt existing bearer(s) by initiating release of the existing bearer(s), request the BPCF to release related resources, and request for admission control toward the BPCF for the new bear action.

Editor's note: How the ARP based pre-emption performed in H(e)NB Policy Function co-exist with the ARP based pre-emption in BPCF needs further study.

5.1.3.1.5.2 BPCF

Operates as per normal with no H(e)NB specific requirements.

5.1.3.1.5.3 H(e)NB

DSCP marking appropriate for the QoS of the PDP context / EPS bearer in both inner and outer IP header of the IPSec connection for the UL packets. The mapping between QoS and DSCP needs to be configured in the H(e)NB (e.g. via the management system).

5.1.3.1.5.4 H(e)NB GW

The H(e)NB GW passes all bearer activations / modifications / deactivations towards the H(e)NB policy function for authorisation.

The H(e)NB GW shall select the same H(e)NB policy function for all requests associated to a H(e)NB using a function similar to PCRF selection mechanism in TS 23.203 [4] where the H(e)NB policy function is equivalent to a PCRF, that may include the use of enhanced DRA.

The H(e)NB GW shall accept the authorisation response from the H(e)NB policy function. This may result in the rejection of the bearer action if the authorisation is rejected.

DSCP marking appropriate for the QoS of the PDP context / EPS bearer.

5.1.3.1.5.5 SeGW

If present, Updates the H(e)NB of the current binding between the IP address assigned to the CPE (outer IP address) and the IP address assigned to the H(e)NB (inner IP address) within the H(e)NB subsystem. If the SeGW resides within the H(e)NB GW, then the H(e)NB GW shall perform in addition the functions associated with the SeGW.

Editor's note: It is FFS whether this mechanism is necessary or can be handled through the management system.

Copying the DSCP marking on received DL packets to the outer IP header of the IPSec tunnel.

The SeGW shall select the same H(e)NB Policy Function for all requests associated to a H(e)NB using a function similar to PCRF selection mechanism in TS 23.203 [4] where the H(e)NB policy function is equivalent to a PCRF, that may include the use of enhanced DRA.

5.1.3.1.5.6 MME

If the HeNB GW is not present in a deployment or the S1-MME is encrypted between MME and HeNB, the MME performs the same functions as the H(e)NB GW as specified in clause 5.1.3.1.5.4.

If the HeNB GW is present in a deployment, there are no H(e)NB interworking specific requirements on the MME.

5.1.3.1.5.7 SGSN

Due to the mandatory presence of the HNB GW, there are no additional requirements on the SGSN.

5.1.3.1.5.8 MSC

Due to the mandatory presence of the HNB GW, there are no additional requirements on the MSC.

5.1.3.1.6 Reference Points

5.1.3.1.6.1 S9a

General

An S9a session (for the purpose of H(e)NB interworking) represents an individual H(e)NB and is established for the duration of the H(e)NB being powered up and connected to the H(e)NB GW/MME. This avoids the need for the BPCF to discover the H(e)NB policy function and also does not require the H(e)NB to be specifically identifiable in the fixed access.

Editor's note: The exact model under which the S9a operates is for further study.

Information Transfer over S9a

The H(e)NB Policy Function will transfer QoS rule over S9a interface. If the H(e)NB Policy Function has aggregated the new bearer action into an existing authorization for the same H(e)NB, the H(e)NB Policy Function is responsible to aggregate the QoS rules of these bearers to form an aggregated QoS rule to be transmitted over S9a interface for admission control.

5.1.3.1.6.2 S15 (H(e)NB GW / MME to H(e)NB policy function)

A session on S15 is established per H(e)NB and it transports the messages for each bearer as seen by the H(e)NB GW or MME. In addition to signalling bearer actions, the H(e)NB GW / MME includes an indication of the membership status to the CSG of the UE for which the bearer action is being performed.

5.1.3.1.6.3 S16 (SeGW to H(e)NB policy function)

This reference point is used to inform H(e)NB policy function the IPSec tunnel header information of specific H(e)NB. IPSec tunnel information. In order to binding IPSec tunnel information to specific H(e)NB, an identifier of H(e)NB must be send to H(e)NB policy function, such as H(e)NB IP address or (e)CGI.

5.1.3.1.7 H(e)NB PF Selection

In order to ensure that all sessions for a certain H(e)NB reach the same H(e)NB PF when multiple and separately addressable H(e)NB PFs have been deployed in one network, it is proposed that DRA is be enhanced to support the H(e)NB PF selection.

When the enhanced DRA first receives a request from the SeGW for a certain H(e)NB PF, the enhanced DRA selects a suitable H(e)NB PF for the H(e)NB and stores the map of the selected H(e)NB PF address and the H(e)NB IP address. Subsequently, the enhanced DRA can retrieve the selected H(e)NB PF address according to the H(e)NB IP address carried by the incoming requests from the H(e)NB GW/MME.

When the H(e)NB is powered off, the enhanced DRA shall remove the information about the H(e)NB.

5.1.3.2 Architecture Alternative 2 - Femto Architecture Diagrams

5.1.3.2.1 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 WT-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 BW requirements and QoS attributes of a new/modified UE service data flow/s (via the 3GPP Femto).

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

Editor's note: The solution on how to the H(e)NB's public IP address and the port number can be obtained for the case when NAT/NAP-T is present between the H(e)NB and SeGW is FFS. The following notes apply to all diagrams in the subsections below.

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: For simplicity, the connection between the HNG GW and the SGSN over the Iu-PS interface is not shown

NOTE 3: The diagrams are based on the architecture diagrams agreed at the 3GPP-BBF workshop

NOTE 4: The connection between the BRAS/BNG and the SeGW is IP transport connection

NOTE 5: When the 3GPP and BBF access networks belong to different Service Providers security arrangement are analogous to those between the hPCRF and the vPCRF, and can be based on TS 33.210 [16] or TS 33.310 [17]

5.1.3.2.2 Non-Roaming

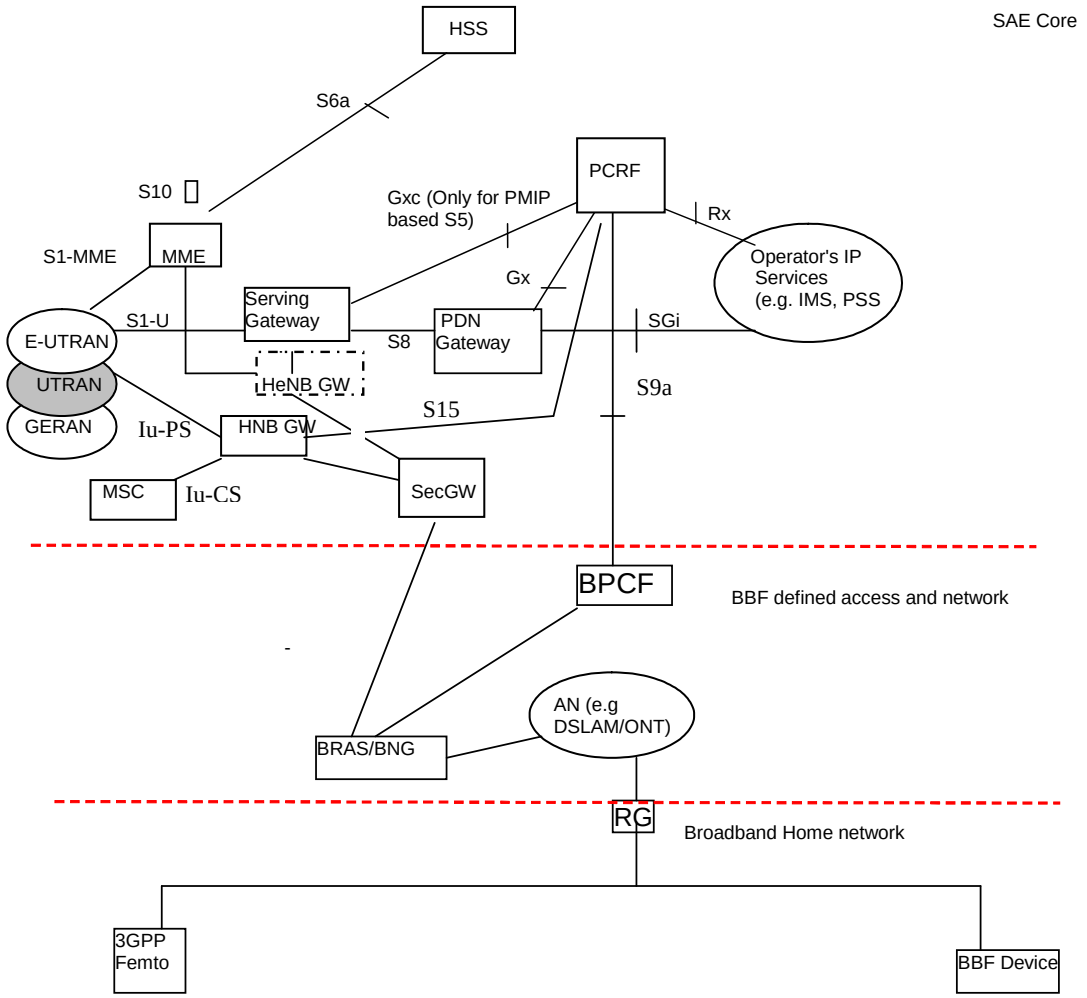


Figure 5.1.3.2.2-1: Non-Roaming

NOTE 1: The reference architecture is applicable when both 3GPP and BBF 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.

5.1.3.2.3 Roaming - Home Routed Traffic

The GTP version of the architecture for the macro network does not require vPCRF in the connection because the HPLN does not provision QoS rules in the VPLMN. Since there is no vPCRF in VPLMN the solution relies on the hPCRF to initiate the S9 session to a selected vPCRF that, in turn, initiates the S9a session 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. For a roaming 3GPP UE connecting to a H(e)NB in the BBF with GTP Home Routed Traffic, the hPCRF sends to the vPCRF over the S9 interface the IP tunnel information (including H(e)NB local IP address) and/or FQDN of BBF access network at which the H(e)NB is connected to.

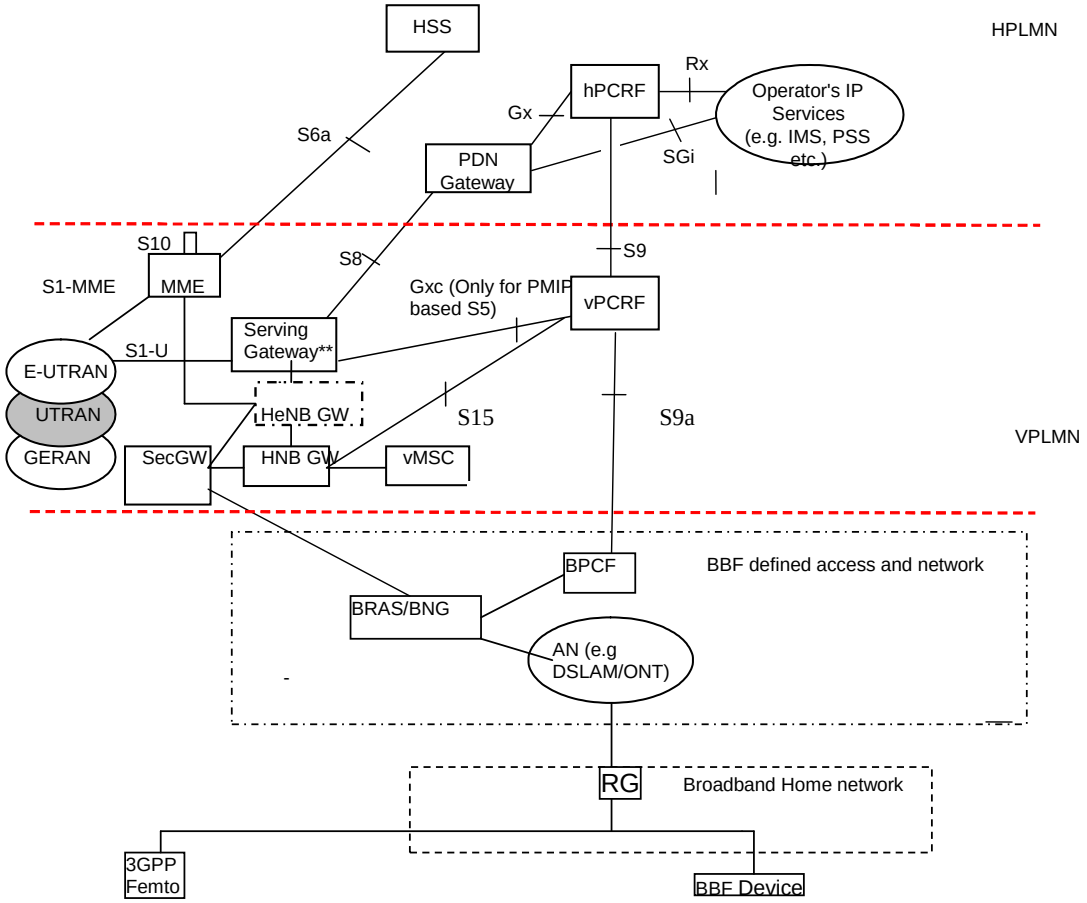


Figure 5.1.3.2.3-2: Roaming - Home Routed Traffic

NOTE 1: The reference architecture is applicable when both 3GPP VPLMN and BBF 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.

Editor's note: It is FFS how the hPCRF discovers the vPCRF for the GTP version of the Architecture.

5.1.3.2.4 Roaming - Visited Access/LBO

The hPCRF need not aware the UE is connected via the 3GPP Femto in the VPLMN unless SPs require provisioning of HPLN policies in the VPLMN.

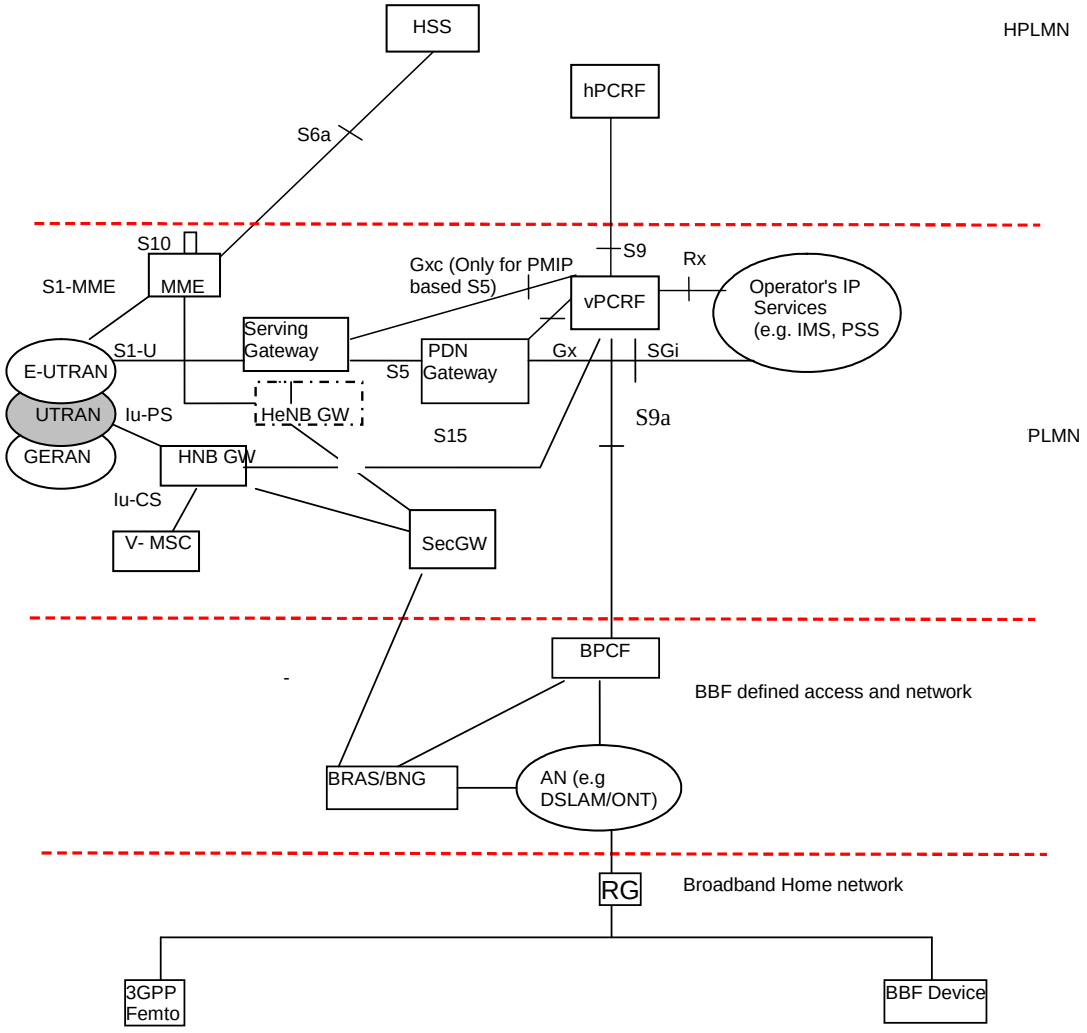


Figure 5.1.3.2.4-1: Roaming - Visited Access/LBO

NOTE 1: The reference architecture is applicable when both 3GPP VPLMN and BBF 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.

5.1.3.3 Architecture Alternative 3 – H(e)NB specific policies

5.1.3.3.1 General Principles

Since H(e)NB traffic is encapsulated within IPSec whilst traversing the BBF access, the BRAS/BNG is not able to recognise UE specific traffic when using the H(e)NB. The policies in this alternative are defined to be H(e)NB specific and therefore H(e)NB is responsible for the policy interactions.

The normal PCC architecture, servicing UEs, has no direct interaction with the 3GPP-BBF interworking solution.

The architecture highlights the S9a interface between a H(e)NB policy function and the BBF PCF (BPCF) for H(e)NB access. The H(e)NB policy function performs control based on bearers (EPS bearers or PDP contexts) made visible to it.

The function of the S9a interface is to convey sufficient information to the BPCF to enable it to identify the BNG the H(e)NB connects to, and perform admission control based on the bandwidth requirements and QoS attributes of the bearers or aggregate of bearers with similar QoS characteristics being established.

When receiving rejection for a QoS authorization request from BPCF, the H(e)NB Policy Function shall perform pre-emption based on CSG membership and ARP to decide whether to reject or admit the new bearer authorization, e.g. to allow emergency call to pre-empt non-emergency call(s) if regulation allows.

NOTE 1: The H(e)NB Policy Function may pre-empt existing bearer(s) by initiating release of the existing bearer(s), request the BPCF to release related resources, and request for admission control toward the BPCF for the new bear action.

Editor's note: How the ARP based pre-emption performed in H(e)NB Policy Function co-exist with the ARP based pre-emption in BPCF needs further study.

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

NOTE 2: UE policies applied at the PCRF and the P-GW are independent of H(e)NB policy function operations.

NOTE 3: There may be 2 S9a sessions for a single UE if the UE is simultaneously connected via H(e)NB and some other access means connected to the same BBF connection e.g. WLAN.

NOTE 4: An assumption is made that a mapping between IP address used by the H(e)NB connection (outer IPSec header) and the H(e)NB is made available to policy architecture.

5.1.3.3.2 Non-Roaming

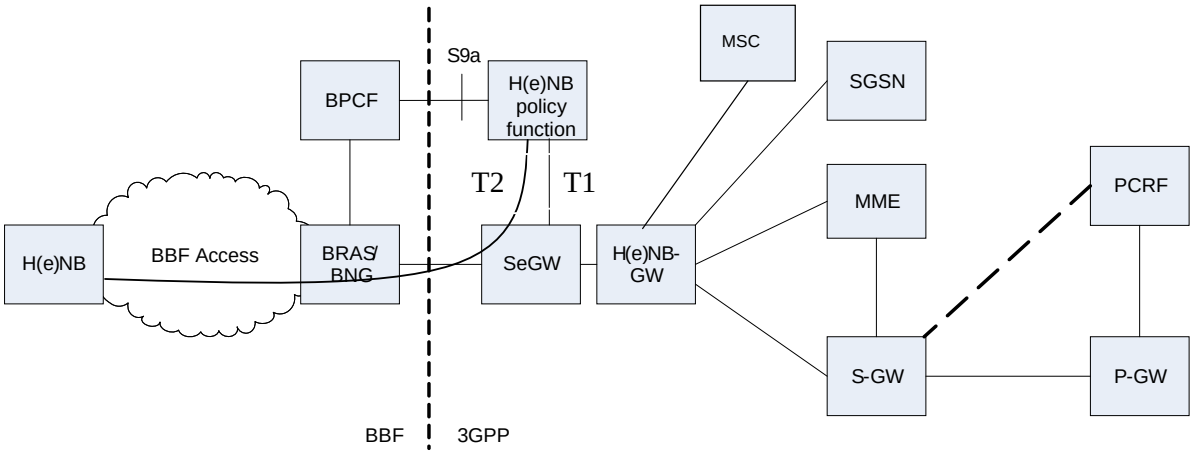


Figure 5.1.3.3.2-1: Non-Roaming

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.2-1.

NOTE 2: The CS domain is not applicable for the H(e)NB.

5.1.3.3.3 Roaming - Home Routed Traffic

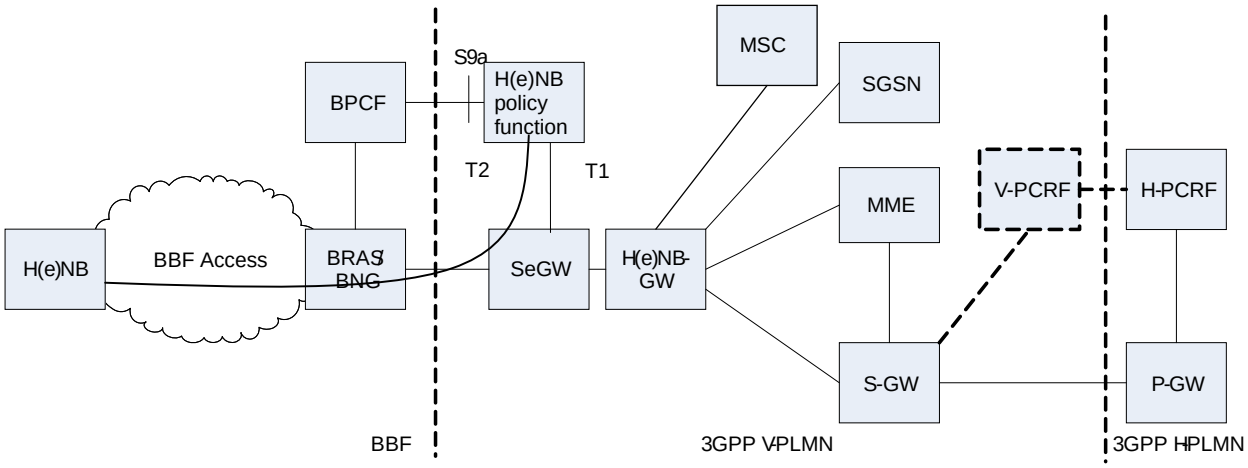


Figure 5.1.3.3.3-1: Roaming - Home Routed Traffic

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.3-1.

NOTE 2: The CS domain is not applicable for the H(e)NB.

5.1.3.3.4 Roaming - Visited Access/LBO

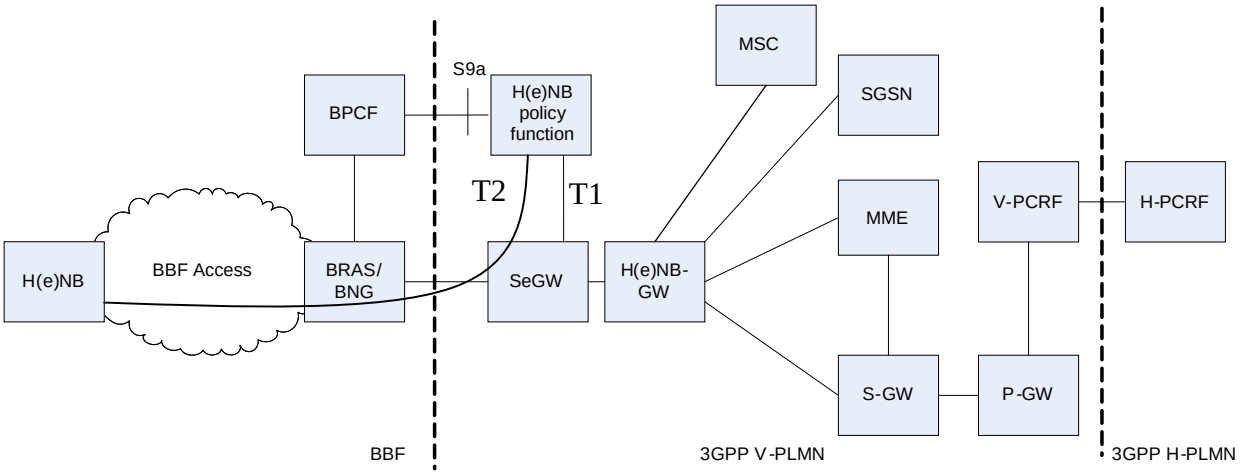


Figure 5.1.3.1.4-1: Roaming - Local breakout

NOTE 1: Not all the 3GPP reference points are shown or labelled in Figure 5.1.3.1.4-1.

NOTE 2: The CS domain is not applicable for the H(e)NB.

5.1.3.3.5 Network elements

5.1.3.3.5.1 General

The 3GPP network elements are defined in details in TS 23.401 [2] and TS 23.402 [3].

The BBF network elements BRAS, BNG, RG, BPCF* are defined in details in BBF TR-058, TR-101, WT-145 [7] and WT-134.

The newly introduced and enhanced network elements are defined as below:

5.1.3.3.5.2 SeGW

Except for the functions defined in TS 33.320 [15], the SeGW has the extra functions:

- If the IPSec tunnel between the H(e)NB and SeGW transverses NAT, the SeGW sends the IPSec tunnel information (IPSec tunnel outer IP address, H(e)NB IP address allocated by MNO) to the H(e)NB PF via the T1 interface during the IPSec tunnel establishment after the H(e)NB powers on. The IPSec tunnel outer IP address is used to identify the BBF BPCF serving the H(e)NB, and will be forwarded to BBF BPCF to enable it to identify the backhaul to which the H(e)NB connects.

- The SeGW shall select the same H(e)NB Policy Function for all requests associated to a H(e)NB using a function similar to PCRF selection mechanism in TS 23.203 [4] where the H(e)NB policy function is equivalent to a PCRF, that may include the use of enhanced DRA.

5.1.3.3.5.3 H(e)NB

The H(e)NB shall have the following extra functions:

- If the H(e)NB receives Session Management request from the H(e)NB GW/MME/SGSN, e.g. S1: Create Bearer Request, Iu:RAB assignment request, the H(e)NB will sent the requested "bandwidth requirements and QoS attributes" in the "Resource allocation Request" signalling to the H(e)NB PF via the T2 interface for admission control of the requested resources in fixed network.

- After the H(e)NB receives the "Resource allocation Response" from the H(e)NB PF, the H(e)NB will admit or reject the S1 request based on the result from the H(e)NB PF.

- The H(e)NB shall select the same H(e)NB Policy Function for all requests associated to a H(e)NB using a function similar to PCRF selection mechanism in TS 23.203 [4] where the H(e)NB policy function is equivalent to a PCRF, that may include the use of enhanced DRA.

5.1.3.3.5.4 H(e)NB PF

After receives IPSec tunnel information from the SeGW, the H(e)NB PF shall initiate the S9a session establishment with BBF BPCF and forward the "IPSec tunnel information" together with the H(e)NB IP address allocated by the SeGW to the BBF BPCF in the S9a signalling. The "IPSec tunnel information" will be used as an identification of the fixed line to which the H(e)NB is connected, and is associated with the S9a session of the H(e)NB. The H(e)NB PF shall also store the mapping between the S9a session and the H(e)NB IP address allocated by the SeGW, the H(e)NB PF may also store the "IPSec tunnel information".

The H(e)NB PF associates the "Resource allocation Request" received from H(e)NB with corresponding S9a session according to the H(e)NB IP address allocated by the SeGW, and forward the "Resource allocation Request" the BPCF via the S9a session.

The H(e)NB PF discovers the BPCF serving the H(e)NB based on IPSec tunnel information.

5.1.3.3.5.5 BPCF

It is assumed that the BPCF can make a mapping between IP address used by the H(e)NB connection (outer IPSec header) and the physical line to which the H(e)NB is connected.

5.1.3.3.6 Reference Point

The reference points S1-MME, S1-U, S3, S4, S10, S11 are defined in TS 23.401 [2]. The reference points S2b, S2c, S6a, S6b, SWx, SWa, SWm, SWn, SWu, SGi, Rx, Gxc are defined in TS 23.402 [3].

The newly introduced and enhanced network elements are defined as below:

T1 interface:

Interface T1 is between H(e)NB PF and SeGW, and is used to convey IPSec tunnel information from SeGW to H(e)NB PF.

T2 interface:

Interface T2 is between H(e)NB and H(e)NB PF, and is used request admission control in fixed network for a certain service data flow or bearer.

S9a interface:

It provides transfer of dynamic QoS control policies (QoS) from the H(e)NB Policy Function to the BBF Policy BPCF. The S9a is based on enhancement of S9 reference point for supporting interworking with BBF Policy Framework

5.1.3.3.7 H(e)NB PF Selection

In order to ensure that all sessions for a certain H(e)NB reach the same H(e)NB PF when multiple and separately addressable H(e)NB PFs have been deployed in one network, it is proposed that DRA is be enhanced to support the H(e)NB PF selection.

When the enhanced DRA first receives a request from the SeGW for a certain H(e)NB PF, the enhanced DRA selects a suitable H(e)NB PF for the H(e)NB and stores the map of the selected H(e)NB PF address and the H(e)NB IP address. Subsequently, the enhanced DRA can retrieve the selected H(e)NB PF address according to the H(e)NB IP address carried by the incoming requests from the H(e)NB.

When the H(e)NB is powered off, the enhanced DRA shall remove the information about the H(e)NB.

5.2 Policy and QoS interworking between 3GPP and BBF architectures

Editors note: The assumption is that an "item" would correspond to a bullet of BB1 as described in clause 4.

5.2.1 Description

Editor's note: This clause will describe the description for the item.

This item covers Policy and QoS interworking between 3GPP and BBF architectures for the following two scenarios:

- When H(e)NB is being used and traffic is routed back to the EPC.
- When WLAN is being used and traffic is routed back to the EPC

5.2.2 Solution

Editor's note: This clause will describe the solution(s) for the item.

5.2.2.1 Policy interworking principles

5.2.2.1.1 PCRF – BPCF Functional split

PCRF is the policy and charging control element in 3GPP network. PCRF functions are described in more detail in TS 23.203 [4]. This clause points out new functionality as well as some of the existing functionality applicable to BBF access interworking. (Note that not all applicable existing functionality is included below).

The BPCF is a policy control entity in the BBF network. This clause describes functionality assumed to reside in the BPCF to support 3GPP-BBF interworking.

In a non-roaming scenario, the functionality of PCRF includes:

- Policy decision and PCC Rule generation e.g. based on the information received from the AF via Rx, operator policies and subscription information via Sp (this is existing functionality described in TS 23.203 [4]).
- Installation of PCC Rules in the PCEF over Gx (this is existing functionality described in TS 23.203 [4]).
- Sends the QoS rules to the BPCF over S9a to request admission control in the fixed access.

- Sends outer IP header information for tunnelled traffic (e.g. UE local IP address) to allow the BBF access to identify the UE traffic that is tunnelled.

The functionality of the BPCF includes the following:

- Performs admission control in fixed access or delegates admission control decision to other BBF nodes (this aspect is out of scope to 3GPP). Based on the admission control, the BPCF accepts or rejects the request received over S9a. As with current S9, the BPCF may include the acceptable QoS in the reply if the request is rejected.

- Translates the QoS rule as received of the S9a interface (i.e. QCI, bit rates, and ARP into access specific QoS parameters applicable in the BBF domain (this aspect is out of scope of 3GPP).

- May install Policy Filters and QoS for a 3GPP UE session over R interface (this aspect is out of scope to 3GPP).

Additional clarifications are needed for the roaming scenario, where both hPCRF and vPCRF are available. No business agreement between HPLMN and BBF operator for roaming scenario is assumed. In a roaming scenario, the functionality of the hPCRF includes the following:

- Generates PCC Rules based on the information received from the AF via Rx or via S9, operator policies and subscribed information via Sp (this is existing functionality described in TS 23.203 [4]).

- For home routed access, installs PCC Rules in the PCEF over Gx. (this is existing functionality described in TS 23.203 [4]).

- For visited access (local breakout), sends PCC Rules to the vPCRF over S9 (this is existing functionality described in TS 23.203 [4]).

- For home routed access, sends QoS rules to the vPCRF to request admission control over S9. (This is new for GTP-based access).

- For BPCF-initiated S9a session establishment, sends outer IP header information for tunnelled traffic (e.g. UE local IP address).

The functionality of vPCRF includes the following:

- For visited access (local breakout), installs PCC Rules in the PCEF over Gx. (this is existing functionality described in TS 23.203 [4]).

- Applies local policies based on the roaming agreement with HPLMN. Also applies local policies based on the business agreement with BBF operator.

- Sends QoS rules to the BPCF over S9a to request admission control in the fixed access.

- For PCRF-initiated S9a session establishment using Gxb*, establishes Gxb* session with the ePDG to receive outer IP header information for tunnelled traffic (e.g. UE local IP address).

- For PCRF-initiated S9a session establishment, sends outer IP header information for tunnelled traffic (e.g. UE local IP address) to the BPCF.

The functionality of the BPCF in a roaming scenario would remain the same as in the non-roaming scenario.

5.2.2.1.2 Procedures on S9a

5.2.2.1.2.1 General

Even though S9a is based on S9, all the S9 procedures and Information Elements may not be applicable to BBF accesses. For example, many of the Information Elements used on S9 applies primarily to 3GPP accesses and other wireless accesses. On the other hand, new procedures and IEs may need to be added to S9 in order to support BBF accesses. As part of this paper, we will identify the parts of S9 that do not apply for BBF accesses and those aspects that are currently missing on S9.

In Building Block 1, policy interworking is considered only for scenarios were traffic is routed back via EPC. In this case charging will be performed in the PDN GW and it is reasonable to assume that sending QoS-rule type of information over S9a is sufficient. Therefore the Gxx variant of S9 is applicable for Building Block 1. The Rx and Gx parts of the S9 reference point are not applicable for S9a in the scope of Building Block 1. Below we discuss the

different procedures defined for S9 in TS 23.203 [4] when the Gxx-variant applies. Note that in TS 23.402 [3] and TS 23.203 [4], for the home routed case, the same stage 2 procedures are used over Gxx and S9 reference points. On stage 3 however, they are implemented with different Diameter applications (Gxx Diameter application and S9 Diameter application. In this contribution we use stage 2 language and thus keep the same name also for the procedures on S9a. Note however that there is no assumption that BBERF functionality such as bearer binding is supported by the fixed access. How S9a is implemented on stage 3 level is out of scope for this document.

5.2.2.1.2.2 Non-Roaming and Roaming Procedures

NOTE: The roaming procedure for GTP Home Routed Traffic for H(e)NB interworking architecture alternative 2 and for WLAN UE is described in clause 5.2.2.1.2.3.

Gateway Control Session Establishment

The Gateway Control Session Establishment results in that an S9a session is established.

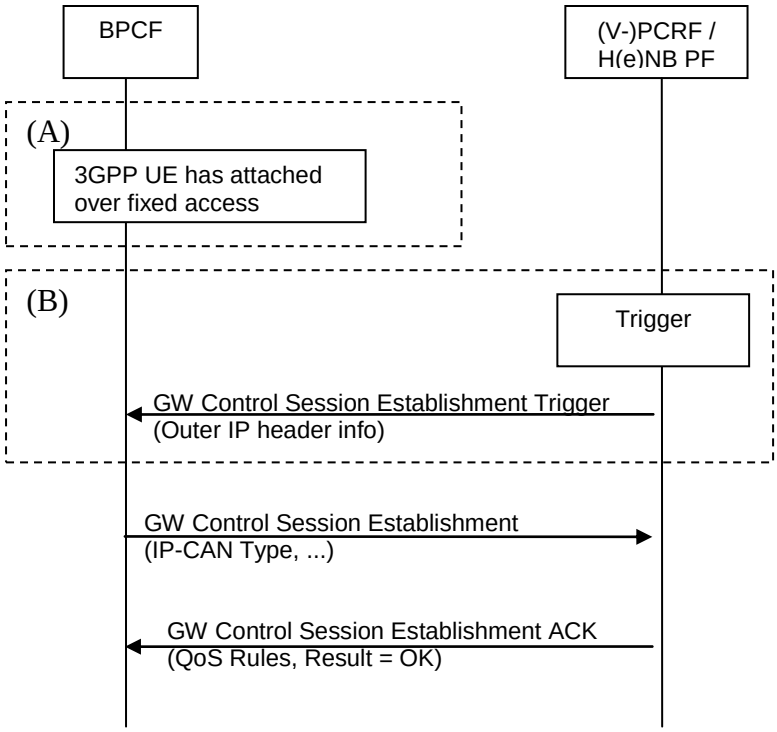


Figure 5.2.2.1.2-1: GW Control Session Establishment

There are two possibilities for how to trigger establishment of an S9a session:

Scenario A: BPCF-initiated Gateway Control Session Establishment network:

- This scenario is valid for WLAN UEs. S9a session establishment is triggered by the BBF access network
- The BPCF can trigger the S9a session establishment if it becomes aware that a 3GPP UE has attached via the BBF access and also learns the IMSI of the subscriber. The BBF access network may become aware of the UE if 3GPP-based access authentication (EAP-AKA/AKA') is performed.
- In the non-roaming case, the BPCF discovers a suitable PCRF domain based on UE NAI realm part.
- The information contained in the request message includes e.g. IMSI, IP-CAN type and local UE IP address. The reply message contains the result code and may also include QoS Rules as described in TS 23.203 [4].
- As a result of the S9a session establishment, the fixed access (BPCF and BNG) is able to associate the aggregate IP traffic plane (tunnel) used by a 3GPP UE with the S9a session towards the PCRF.

Scenario B: PCRF/H(e)NB PF -initiated Gateway Control Session Establishment This scenario is valid for WLAN UE and all 3GPP Femto options. S9a session establishment is triggered by the PCRF/H(e)NB PF:

- For 3GPP Femto the PCRF/H(e)NB PF triggers the GW Control Session Establishment with the BPCF because the signalling between the 3GPP Femto and the EPC network is transparent to the BBF access network. Consequently, the BNG is not in position to trigger the session establishment with the BPCF. For similar reasons the BPCF is not able to initiate session modification requests from the PCRF.

- For WLAN access, in case the BBF access network does not perform 3GPP-based access authentication, the BBF access network will not be aware that a 3GPP UE has attached via the BBF access and will not know the IMSI of the subscriber. In this case, it is assumed that the BBF access cannot trigger the S9a session establishment with the PCRF. Instead the S9a session need be triggered by the PCRF.

- For WLAN UE. the PCRF can trigger the S9a session establishment if it becomes aware that a 3GPP UE has attached via the BBF access and is able to find a corresponding BPCF based on UE local IP address information or CoA received. Depending on scenario, there are two means to trigger the S9a establishment procedure from the PCRF:

  -- The establishment of Gxb* session initiated by ePDG triggers the PCRF to trigger S9a session establishment with the BPCF. The PCRF discovers the BPCF serving the UE based on the UE location information provided by the ePDG via Gxb* reference point (e.g. the outer IP header information of IPSec tunnel). This solution applies when untrusted access procedures with S2c and untrusted PMIP-s2b procedure are used,

  -- The IP-CAN session establishment will trigger the PCRF to initiate the S9a session establishment. The PCRF discovers the BPCF serving the UE based on the UE location information provided by the PDN GW via Gx reference point (e.g. the CoA when S2c is used and UE local IP address in case S2b is used). This solution applies when trusted access procedures with S2c or with untrusted s2b-GTP are used.

NOTE 1: When PCRF receives the IP-CAN session establishment indication, PCRF determines if a S9a session is already present for this IP-CAN session. If S9a session is not already established, the PCRF shall trigger S9a session establishment procedure from the BPCF selected according to UE location.

NOTE 2: ePDG is unaware whether S9a session establishment has been established by the BBF access network, therefore it shall send UE location information to PCRF via Gxb* for untrusted S2c or S2b-PMIP cases or via PDN GW and Gx for S2b-GTP case.

The following clarifications apply for scenario B:

WLAN UE and all 3GPP H(e)NB options:

- The information contained in the request message sending from the PCRF to the BPCF includes e.g. IMSI, IP-CAN type, local IP address (for WLAN UE or H(e)NB) or CoA (WLAN UE only), as described in TS 23.203 [4].

- As a result of the S9a session establishment, the fixed access (e.g. BPCF and BNG) is able to associate the aggregate IP traffic plane (tunnel) used by a 3GPP UE or H(e)NB with the S9a session towards the PCRF.

3GPP H(e)NB Solutions:

- The PCRF/H(e)NB PF uses a single S9a diameter session with the BPCF for all the UEs that request services via the same 3GPP H(e)NB device.

H(e)NB interworking architecture alternative 2:

- The S9a session for 3GPP H(e)NB is established once when the first UE connected to the 3GPP H(e)NB attaches to the networks. Subsequent IP-CAN session establishments and IP Session Modification requests are handled via the PCRF initiated GW Control and QoS Rules Provisioning procedure.

- The V/PCRF determines that the UE is connected to a 3GPP H(e)NB when it receives tunnel information in the IP-CAN Session Establishment message over the Gx interface or in the GW Control Session establishment message over Gxc interface.

- One or more UEs which are attached to the same HeNB may be served by the same PCRF. An UE which is attached to a given HeNB may be served by different PCRFs corresponding to different APNs. Hence, there may

be multiple PCRFs initiating S9a sessions with the same BPCF when UEs connected to the 3GPP H(e)NB are served by different PCRFs.

H(e)NB interworking architecture alternative 1 and 3:

- The H(e)NB PF triggers the S9a session with the BPCF when it receives a message (update H(e)NB binding) from the SeGW.

NOTE: The GW Control Session establishment message does not include any QoS parameters and as such does not request allocation of resources in the BBF access for a UE SDF. See NOTE in clause 5.5.1.

GW Control and QoS Rules Provisioning (admission control request)

WLAN UE and H(e)NB interworking architecture alternative 2:

- For WLAN UE, this procedure would be initiated by the PCRF (non-roaming) or by the vPCRF (roaming). For H(e)NB interworking architecture alternative 2, this procedure would be initiated by the PCRF (non-roaming) or by vPCRF (LBO/VA, or home routed PMIP-based S8). The vPCRF requests the BPCF to perform admission control.

- For H(e)NB interworking alternative 2, the vPCRF initiates the GW Control and QoS Rules provisioning procedure with the BPCF each time the PCRF receives an IP-CAN session establishment or IP-CAN session modification/termination requests.

H(e)NB interworking architecture alternative 1 and 3:

- The H(e)NB PF requests the BPCF to perform admission control.

- The H(e)NB PF initiates the GW Control and QoS Rules provisioning procedure with the BPCF each time the H(e)NB PF receives bearer activation/modification/deactivation request.

- The BPCF takes into account the information contained in the QoS rule but the details for how admission control is performed in the BBF access is out of scope to 3GPP. If the request is accepted the BPCF may provision the BNG with information to allow identification of the traffic flows for a UE and QoS parameters.

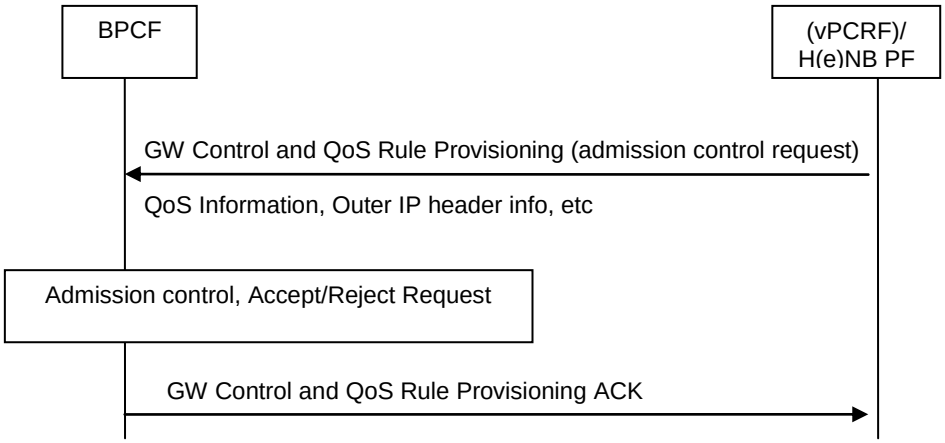


Figure 5.2.2.1.2-3: GW Control and QoS Rule Provisioning

The GW Control and QoS Rule Provisioning includes the following information:

- QoS-Rule with the QoS information (QCI, GBR, MBR, ARP).

- Aggregate Resource for non-GBR bearer.

Editor's note: Whether the Aggregate Resource is used and the definition of Aggregate Resource is FFS based on H(e)Nb alternatives architecture and WLAN scenario.

- Information (e.g. Session ID) that allows the BPCF to associate the request with the existing S9a session so that the fixed access can identify the traffic plane resources that are affected. For encrypted tunnels (for H(e)NB and

untrusted access), there is no immediate need to provide the SDF filters. It is sufficient if the BBF access can associate the request with the right session and perform admission control.

- UE local IP address and UDP source port number if NAT is detected.

The BPCF translates the QoS rule as received of the S9a interface (i.e. QCI, bit rates, and ARP) into access specific QoS parameters applicable in the BBF domain (the details of the mapping from 3GPP QoS parameters on S9a to QoS parameters applicable in the BBF domain is out of 3GPP scope).

The BPCF may respond with a "counter-offer" in form of acceptable bandwidth and/or QoS for one or more SDFs if it cannot provide the requested QoS from the PCRF. The BPCF provides the acceptable QoS in the BBF access using 3GPP QoS parameters on S9a interface (i.e. QCI, bit rates) in the reply if the QoS validation for admission control fails. The PCRF may make a new policy decision, e.g. decide to modify or remove the affected QoS rules.

BPCF-Initiated Gateway Control Session Termination

This procedure would be initiated by the BPCF to terminate a S9a session. The trigger in BPCF for initiating this procedure may be that the 3GPP UE is no longer connected via the BBF access (e.g. if the lease of the local IP address used by the 3GPP UE expires), if the BBF access network is aware of the UE's detachment from the BBF access network. The BPCF may also use this procedure if an admission control request causes all resources of a UE to be pre-empted (if allowed by regulations).

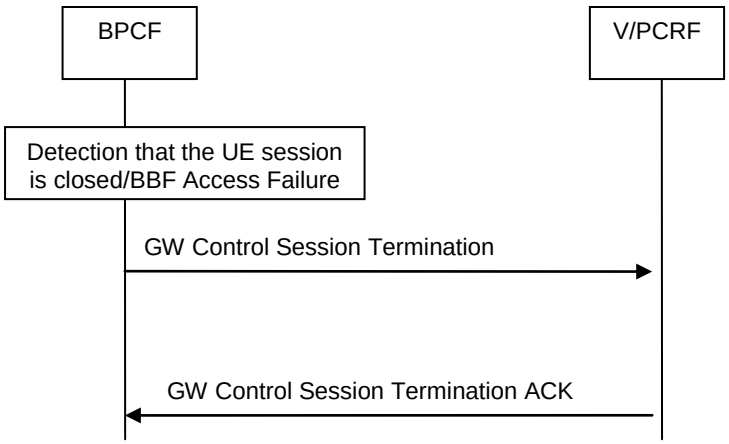


Figure 5.2.2.1.2-4: GW Control Session termination

PCRF-Initiated Gateway Control Session Termination

WLAN and H(e)NB interworking architecture alternative 2 only:

- This procedure would be initiated by the PCRF (non-roaming) or vPCRF (roaming) for S9a to terminate a S9a session.

- In case the S9a session is initiated from the PCRF and PCRF-initiated S9a session establishment is triggered by Gxb* session, the Gxb* session termination from ePDG may serve as a trigger for PCRF-initiated GW Control session termination toward BPCF.

- For H(e)NB interworking architecture alternative 2, the PCRF initiates the GW Control Session Termination to terminate the S9a session with the BPCF when it receives the IP-CAN session termination from the last UE connected to the H(e)NB.

For H(e)NB interworking architecture alternative 1 and 3, the H(e)NB PF initiates the GW Control Session Termination toward BPCF to terminate the S9a session when the H(e)NB deregisters from the 3GPP network.

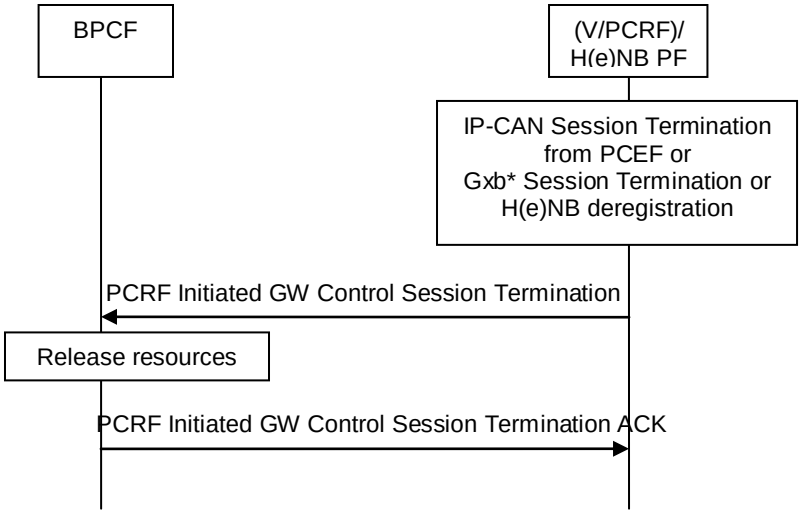


Figure 5.2.2.1.2-5: PCRF Initiated GW Control Session Termination

BPCF-Initiated Gateway Control and QoS Rules Request

In a fixed access, there will probably be limited use of this procedure. For example, the fixed accesses typically do not support UE-initiated resource requests and would also not be able to detect most of the events that are defined as event triggers in PCC. This procedure could however be applicable in case the BPCF has pre-empted some resources and wants to report a QoS rule failure to the PCRF, or when the BBF network cannot sustain the BW allocated to a particular traffic class/DSCP aggregate.

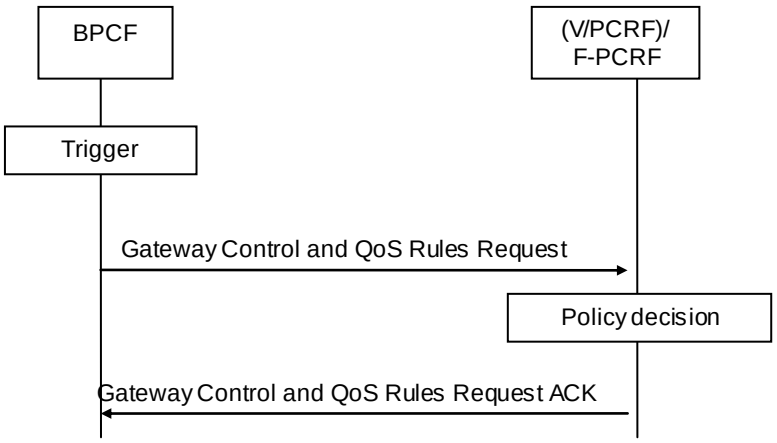


Figure 5.2.2.1.2-6: Gateway Control and QoS Rules Request

5.2.2.1.2.3 Roaming Procedures - GTP Home Routed Traffic (WLAN and H(e)NB Interworking Architecture Alternative 2 only

hPCRF Initiated GW Control Session Establishment

The S9 GW Control Session Establishment procedure is initiated by the hPCRF when the Gx session establishment/modification from the PDN GW/PCEF includes an indication that a roaming 3GPP UE connects to a H(e)NB in the BBF or WLAN UE access the network via BBF in the VPLMN. The hPCRF initiates a single S9 session for all the UEs connected to the H(e)NB when the first UE attaches to the VPLMN.

For a roaming 3GPP UE connecting to a H(e)NB in the BBF with GTP Home Routed Traffic, the hPCRF sends to the vPCRF over the S9 interface the IP tunnel information (including H(e)NB local IP address) and/or FQDN of BBF access network at which the H(e)NB is connected to.

Depending on SP policy the HPLMN may determine QoS rules by taking into account the fact that the presence of BBF access in the VPLMN.

Depending on VPLMN policy the vPCRF may modify the QoS rules it receives from the hPCRF.

The vPCRF initiates the S9a session with the BPCRF that includes the QoS information it received from the hPCRF.

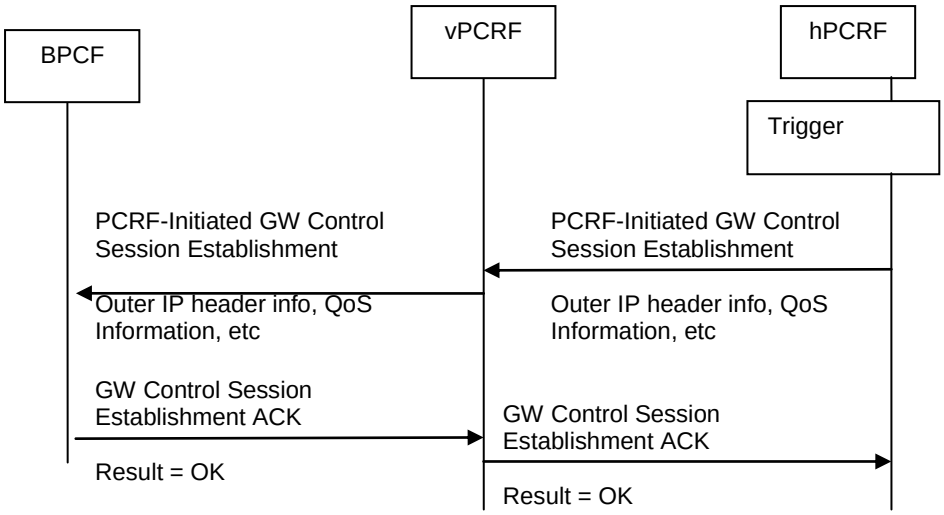


Figure 5.2.2.1.2-7: hPCRF Initiated GW Control Session Establishment

GW Control and QoS Rules provisioning (admission control request):

The hPCRF initiates the S9 GW Control and QoS Rules provisioning with the vPCRF each time the PCRF receives an IP-CAN session establishment from a subsequent UE or IP-CAN session modification/termination requests. The vPCRF initiates the S9a GW Control and QoS Rules provisioning procedure with the BPCF each time the PCRF receives an IP-CAN session establishment or IP-CAN session modification/termination requests.

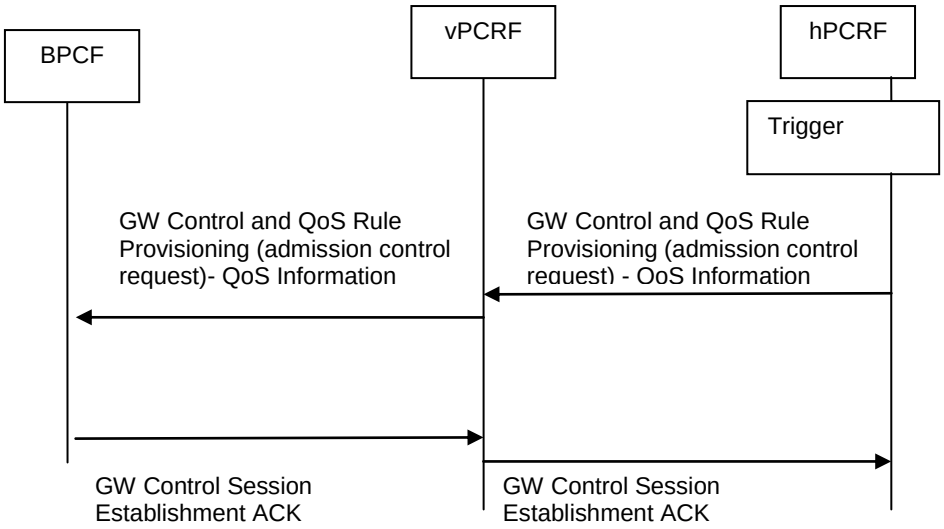


Figure 5.2.2.1.2-8: GW Control and QoS Rules provisioning

hPCRF Initiated GW Control Session Termination:

The S9 GW control session termination is triggered by the hPCRF when the last UE connected to the H(e)NB detaches from the network or the WLAN UE terminates the session. The vPCRF initiates the S9a GW control session termination procedure with the BPCF.

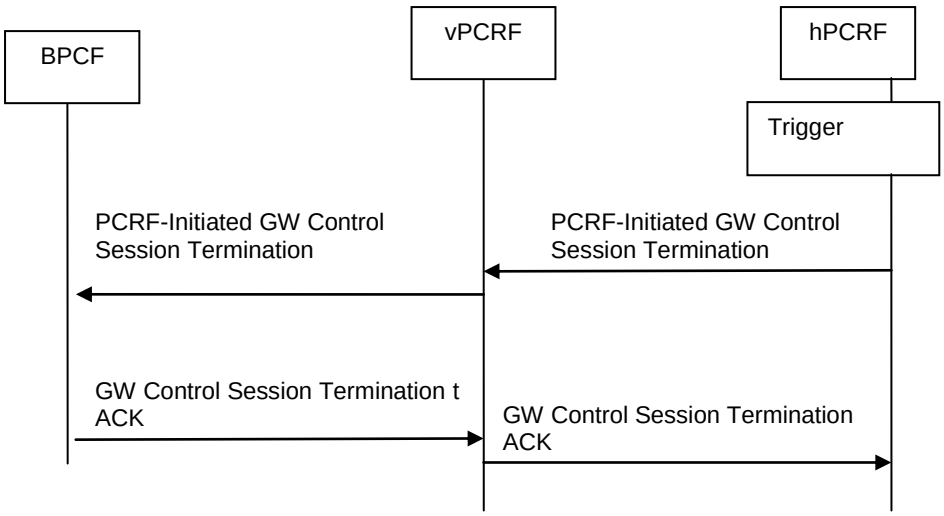


Figure 5.2.2.1.2-9: hPCRF Initiated GW Control Session Termination

5.2.2.1.3 Leg Linking and session association

For WLAN, PCRF and BPCF both need to support session binding function. When the S9a session is initiated by BPCF, PCRF must perform the session binding between the S9a session and the Gx session according to the UE Local IP address, if available, and UE identity. The PCRF must be able to perform the binding between multiple IP-CAN sessions for the same UE to the same S9a session.

When S9a session is initiated by PCRF, BPCF shall associate the R session with the S9a session.

NOTE: For PCRF-initiated S9a session case, how the BPCF performs the association of S9a and R session is out of the scope of 3GPP.

5.2.2.1.4 PCRF/BPCF Discovery and Selection

The BPCF may be served by one or more PCRF nodes in HPLMN and, in roaming scenarios, one or more PCRF nodes in the VPLMN for UE. Similarly, the PCRF may be served by one or more BPCF nodes in the fixed network.

For BPCF-initiated S9a session case, PCRF selection procedure, including vPCRF selection for roaming case, described in TS 23.203 [4] shall be used by BPCF. For a roaming scenario the BPCF is configured with the relation of HPLMN-Id reachable via a particular VPLMN-Id. The BPCF selects given a certain IMSI the correct DRA in the VPLMN. The vPCRF finds the DRA in the HPLMN based on the IMSI as described in TS 23.203 [4].

For PCRF-triggered S9a session establishment, the PCRF is configured with IP address range mappings { (IPx..IPy) -> BBF network entry point}. For WLAN scenario the PCRF selects the correct BBF network entry point based on UE Local IP address. From H(e)NB scenario the PCRF selects the correct BBF network entry point based on H(e)NB Local IP address and/or FQDN of BBF access network at which the H(e)NB is connected to. The implementation of a BBF network entry point is out-of-scope for 3GPP, but could e.g. be a BPCF or a DRA.

For WLAN and H(e)NB in Home Routed roaming case, for PCRF-triggered S9 session establishment, hPCRF finds V-DRA according to UE Local IP address, FQDN of BBF access network at which the H(e)NB is connected to and the VPLMN ID if received via Gx session, and then discovers vPCRF by V-DRA. vPCRF selects the correct BBF network entry point with the given UE local IP address and H(e)NB Local IP address and/or FQDN of BBF access network at which the H(e)NB is connected to respectively.

5.2.2.1.5 QoS interworking principles

5.2.2.1.5.1 General

This clause describes potential solution options for how to detect and classify IP packets for the purpose of QoS treatment in the BBF network.

5.2.2.1.5.2 QoS interworking principles for DSCP marking

This solution is based on DSCP marking of packets traversing the BBF network. The BBF network (e.g. BNG) makes packet classification based on the DSCP of the incoming packets.

BBF Access network

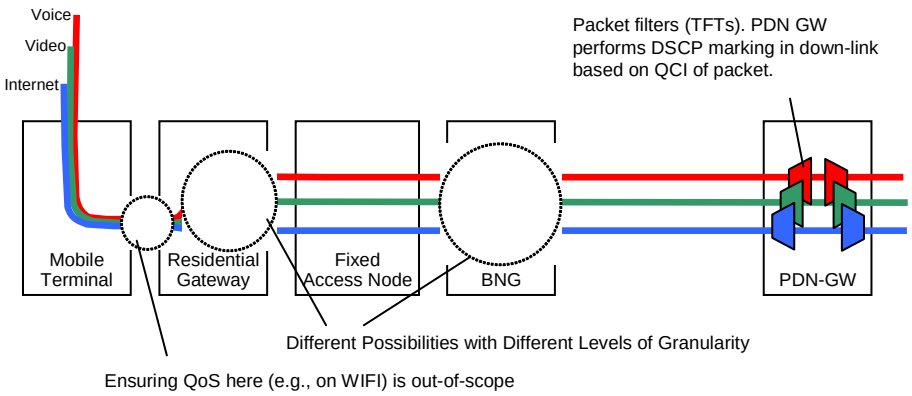
BBF access network currently supports the DSCP marking as specified in TR-092 [20] for BRAS, in TR-101 [8] for Access Nodes and Aggregation Nodes and in TR-124 Issues 2 for the RG [21].

Downlink

For the WLAN case, the PGW 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 copies that marking to the new outer header.

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

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.



NOTE 1: The figure is simplified and the intermediate transport network entities are not shown. The details of traffic handling in BBF domain is out of 3GPP scope.

Figure 5.2.2.1.5-1: Packet classification and packet forwarding treatment in a 3GPP-BBF interworking scenario.

Downlink for control plane traffic of Femto 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 copies this DSCP if it exists from the inner header to the outer header to ensure the correct QoS treatment in the tunnel before it gets into it.

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

Uplink:

For the WLAN case, 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. Reflective QoS is already used in GAN (GSM CS access tunnelled via WLAN), see TS 44.318.

NOTE 3: For IP flows initiated from the UE, uplink packets will not be marked until a marked downlink packet is received.

Editor's note: The impact of unmarked TCP-SYN uplink packets to applications is FFS.

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

- The UE needs a table of state information.
- For each incoming downlink IP packet, a lookup is made in the table. If no entry for the n-tuple of this packet exists, then a new entry is added. Otherwise, the DSCP value and the time stamp for this entry are set.
- A corresponding uplink n-tuple is made from the downlink n-tuple by swapping address (and port) destination and source.
- For each outgoing IP packet, a lookup is made in the table. If the n-tuple of the packet matches an uplink n-tuple in the table, then the DSCP value of the packet is set to the DSCP value in this entry of the table. The time stamp of this entry is set.
- Note that for tunnelled scenarios, the n-tuple in the table is the n-tuple of the inner header of the packet. In all scenarios, the DSCP value in the table is the DSCP value of the outer header of the packet. This in both downlink and uplink direction.
- Entries are removed from the table 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.

Since BBF at this point in time does not implement any dynamic policy interface between BPCF/BNG and RG, the UE 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). BBF does implement resource utilization limiters, but only on a per-line granularity. BBF might implement a number of mechanisms to protect the BBF network from a misbehaving UE (note that 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 BBF operator):

- 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 concluded from authentication (always EAP-AKA for 3GPP UEs) or from packet destination address (always ePDG/PGW 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 BBF network (e.g. in a scenario with user place confidentiality protection). The granularity may be on a per UE and DSCP basis.

NOTE: The problem of the UE taking too many uplink resources on the link between RG and BNG is the same in QoS interworking based on DSCP as on SPI - it is solely the result of lacking a dynamic policy interface to the RG.

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 also copies the marking to the outer header.

Editor's note: Use of reflective QoS by the H(e)NB will eliminate the requirement for the H(e)NB to be aware of inter operator DSCP marking agreements. Therefore the use of reflective QoS by the H(e)NB needs to be evaluated.

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, they may perform QoS treatment and QoS remapping based on DSCP value of the outer IP header.

Uplink for control plane traffic of Femto 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.

DSCP remapping

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.

Correlating admission control with DSCP marking

The BPCF performs admission control in fixed access or delegating admission control decision to other BBF nodes. Based on the admission control, the BPCF accepts or rejects the request received over S9a. The BBF operator may also want to verify that the traffic for a specific UE is not exceeding the traffic agreed by admission control that was performed 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 BBF network. Policies can be sent down by the BPCF to the BNG via the R reference interface.

Regardless of the access method used, the BPCF needs to be able to translate QCI received on S9a into the DSCP that the BNG will see. To do this, the BPCF needs to know the relation between QCIs and DSCPs for the traffic that enters the BBF domain. This allows the BBF operator to make the appropriate mapping from QCI to DSCP.

NOTE: The correlation function mentioned above is BBF-internal and therefore out-of-scope for 3GPP.

5.2.2.1.5.3 Service data flow detection based on SPI or SDF filters

In trusted scenarios where the UE connects to the EPC using S2c with no user plane confidentiality protection, the BBF access can detect service data flows inspecting the inner packets encapsulated in the DSMIPv6 tunnel, as currently specified in TS 23.402 [3] and TS 23.203 [4]. To that purpose the BBF access uses the information on the mobility protocol tunnelling header and the SDF filters that the PCRF provides to the BPCF via the S9a reference point.

In untrusted scenarios where the UE uses IPSec/SWu towards an ePDG and in trusted scenarios where the UE uses S2c with user plane confidentiality protection, the BBF access cannot detect service data flows inspecting user plane packets exchanged over the SWu and S2c reference points, since they are encrypted. In this case service data flow detection in the BBF access can be performed based on the source address and destination address of the outer IP header and the Security Parameters Index (SPI) included in the IPSec ESP header. This approach is based on the following principles:

- Different services data flows are mapped on different child IPSec Security Associations (SAs). To that purpose, if the UE is using S2c, upon reception of a PCC rule from the PCRF via the Gx reference point, the PDN GW initiates the creation of a child IPSec SA for the traffic matching the PCC rule. To make sure that the traffic exchanged on the SA is the traffic matching the PCC rule, the PDN GW uses the SDF filters included in the PCC rule to derive the traffic selectors proposed to the UE in the IKEv2 exchange. When S2b is used, it is up to the ePDG to create the child IPSec SA, based on a trigger provided by the PCRF via the Gxb* reference point (S2b-PMIP) or based on information in dedicated bearer procedures provided by the PDN GW via the S2b reference point (S2b-GTP).

NOTE: Assuming that the UE accepts the traffic selectors proposed by the PDN GW, or ePDG, with no modifications, routing of data traffic on the child SA is symmetric. Depending on operator's policies, if the UE modifies the traffic selectors proposed by the PDN GW, or ePDG, the PCC Rules Provision Procedure may be rejected.

- The SPI (Security Parameter Index) that identifies the child IPSec SA is reported back to the PCRF. This is done by the PDN GW via the Gx reference point (in case of S2c or S2b-GTP), or by the ePDG via the Gxb* reference point (S2b-PMIP).

- The PCRF provides to the BPCF via the S9a reference point the outer IP header information, the SPI and the QoS rule. The outer IP header information includes the tunnel end points, namely the UE's Care-of Address and the PDN GW address, if the UE is using S2c, or the UE's Care-of Address and ePDG address, if S2b is used.

- Based on the rules provisioned to it, the BBF access performs admission control and policy enforcement in the uplink and in the downlink direction for the traffic aggregate matching the outer IP header information and the SPI. The details of how admission control and policy enforcement are performed in the BBF access are out of 3GPP scope.

5.2.2.1.5.4 Multiple IPSec tunnel Child SAs support

RFC 4301 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.

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

5.2.2.1.5.5 Conclusion

DSCP marking is the method supported by BBF specification. The SPI/SDF-based approach is not supported by BBF specification at present time.

5.2.2.1.6 Assumptions about functionality in the BBF access network

In the above analysis, the following assumptions were made about functionality in the BBF Access Network:

- The BPCF is able to map the QoS information (QCI, bit rates, ARP) received over S9a to access-specific parameters applicable in the BBF access network
- The BBF access network (e.g. BPCF) can perform admission control based on the QoS rules received over S9a
- The BBF access network is able to support 3GPP-based access authentication and forward EAP messages between the UE and EPC..
- Triggered by the access authentication and/or local IP address assignment, the BPCF initiates establishment of the S9a session with the PCRF. This assumes that the BBF Access becomes aware of the 3GPP UE attaching.
- BPCF support for PCRF- initiated establishment of S9a session.
- Assumptions related to QoS interworking based on DSCP (for building block I only):
  - In WLAN scenarios with user plane confidentiality protection, the RG needs to honour or to translate the DSCP marking set by the UE based on pre-provisioned rules in the RG [TR-059].
  - In a Femto scenario, the RG needs to honour or translate the DSCP marking set by the H(e)NB based on pre-provisioned rules in the RG [TR-059].
- In an S2b/S2c scenario with multiple UEs behind the same NATed RG, it is assumed that the BBF is able to use UE local IP address and UDP source port number received over S9a e.g. to perform accounting or policy enforcement on a per-UE granularity.

5.2.3 Conclusion

For traffic routed via EPC, the S9a reference point re-uses procedures defined for the Gxx reference point in TS 23.203 [4]:

- One or more UEs which are attached to the same HeNB may be served by the same PCRF.
- An UE which is attached to a given HeNB may be served by different PCRFs corresponding to different APNs.
- Hence, the HeNB's serving BPCF may have one or more S9a sessions with one or more PCRFs.

In particular this implies that the PCRF provides QoS information over S9a in the form of QoS Rules as defined in TS 23.203 [4]. The BPCF translates the QoS rule as received of the S9a interface (i.e. QCI, bit rates, and ARP) into access specific QoS parameters applicable in the BBF domain (this aspect is out of scope of 3GPP).

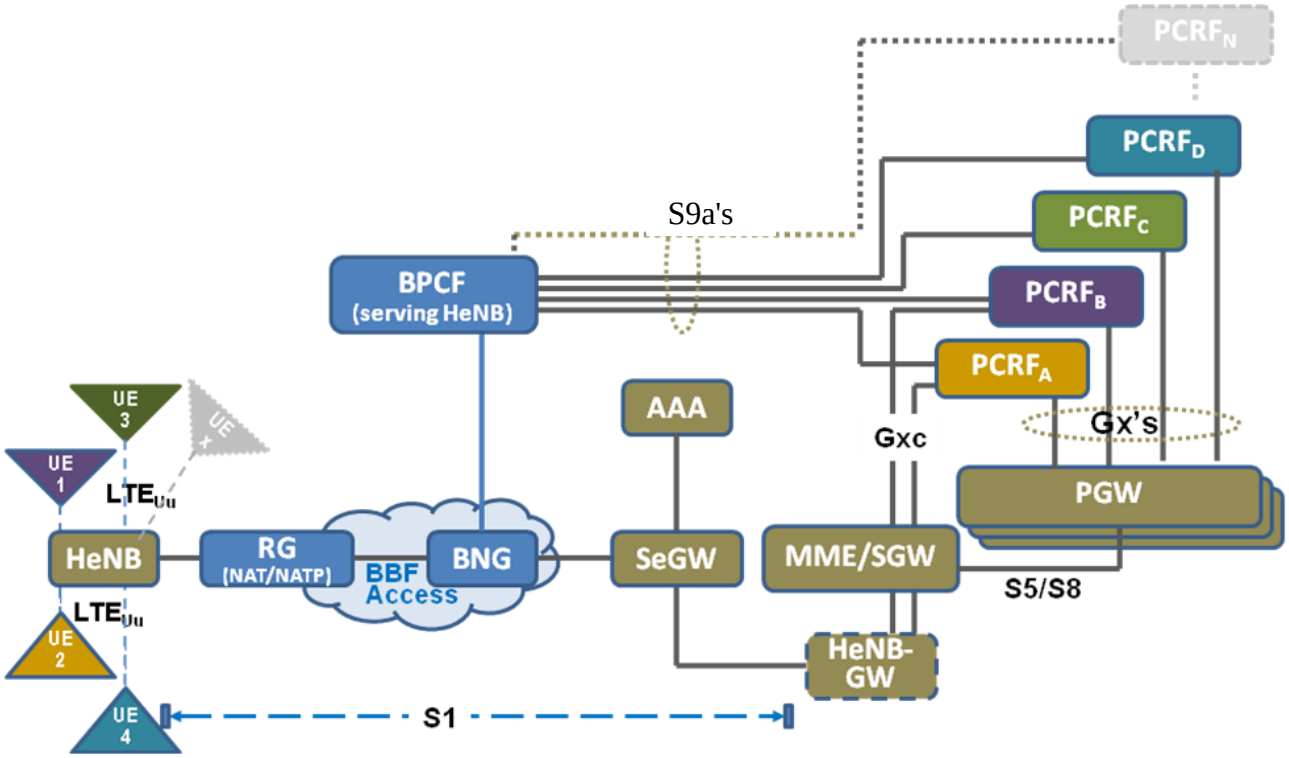


Figure 5.2.3-1: S9a relationship between UE's serving PCRF and HeNB's serving BPCF

Editor's note: The above conclusion does not make assumptions about protocol details. Stage 2 TS 23.402 [3] and TS 23.203 [4] use the same message names for Gxx and S9 with home routed traffic but they have been defined using separate Diameter applications on stage 3. How the stage 2 messages on S9a are implemented on stage 3 is out of scope for this document.

Editor's note: Enhancements to the Gxx procedures to support S9a are being identified and captured in this TR.

The existing Gxx procedures need to be enhanced with a possibility to trigger Gateway Control Session Establishment from the PCRF as described in 5.2.2.1.2.2.

For QoS interworking based on DSCP, a number of enhancements are needed:

- In scenarios where traffic is sent in an IPSec tunnel from ePDG/SeGW to the UE/H(e)NB, the ePDG/SeGW shall copy that marking to the new outer header.
- In scenarios where traffic is sent in an IPSec tunnel, the ePDG/PGW/SeGW (downlink) and UE/H(e)NB (uplink) shall map different service data flows of different DSCP values on different child IPSec Security Associations (SAs).
- For WLAN, if uplink QoS needs to be supported, the identified solution requires the UE to implement reflective QoS.
- If the UE implements reflective QoS and the BBF network needs to be protected from a misbehaving UE, BBF should implement protective measures (e.g. per-UE bandwidth limitation in the RG or in the BNG). Implementing these functions is out-of-scope for 3GPP.

5.3 Interworking between 3GPP and BBF architectures for authentication, including identities, when WLAN is used

5.3.1 Description

This item covers interworking between 3GPP and BBF architectures for authentication, including identities, on top of Release 10 baseline architecture, when the UE accesses over WLAN.

5.3.2 Solution

3GPP EPS defines several procedures for authentication of a 3GPP UE accessing over a non-3GPP access. These include:

- Access authentication procedures based on EAP-AKA and EAP-AKA'. For access authentication, EAP signalling is forwarded between BBF AAA Server and 3GPP AAA Server/proxy via the SWa and STa reference points.
- Tunnel authentication procedures for SWu based on EAP-AKA. This authentication is transparent to the BBF Access Network.
- Authentication for S2c (DSMIPv6) based on EAP-AKA. This authentication is transparent to the BBF Access Network.

Editor's note: The solutions for supporting 3GPP-based access authentication in BBF access networks are work in progress in BBF.

The basic functionality of the existing SWa and STa reference points is adequate to support BBF Access Interworking. Minor enhancements of the SWa reference point, on top of Release 10 baseline architecture, is needed to carry the permanent user identity (i.e. IMSI) in the successful response from 3GPP AAA Server to BBF AAA Server.

To support interworking with BBF access networks one scenario for deployment is that 3GPP-based access authentication is supported by the BBF access networks. This would make the BBF access aware that a 3GPP terminal is connecting via BBF access and of the user and operator identity by means of NAI and would allow the BPCF to initiate a S9a session towards the PCRF for the UE.

Another scenario for deployment is that 3GPP-based access authentication is not performed and that the BBF access is not aware of the 3GPP terminal. To support this scenario, the S9a session could be initiated from the PCRF towards the BBF access network. The S9a procedures are described in clause 5.2.

5.3.3 Conclusion

The existing release 10 baseline supports all authentication procedures needed for Building Block 1.

Minor enhancements to SWa is needed to support 3GPP-based authentication for BBF Access Interworking. Currently the only identified addition to SWa is to provide the permanent user identity (IMSI) in the reply from 3GPP AAA Server to BBF AAA Server. (Note that IMSI is already included on STa).

Editor's note: The SWa and STa references points are defined in TS 29.273 and are using the Diameter protocol. In case the BBF AAA Server only supports RADIUS some additional interworking mechanisms may be needed. This issue is FFS.

5.4 IP flow mobility support in BBF accesses

5.4.1 Description

This item covers support of IP flow mobility for interworking between 3GPP and BBF architectures.

TS 23.261 [9] defines extensions to DSMIPv6 to support IP flow mobility between 3GPP and WLAN accesses. In this specification, the HA respond the Binding acknowledge to the UE without waiting for the response from the PCRF, i.e. The flow mobility action will be finished before the admission control is performed in BBF access network.

One aspect worth noting is that TS 23.261 [9] and TS 23.203 [4] define some extensions to the PCC architecture to support IP flow mobility. In this specification, when the PCRF gets the IP flow mobility routing rule from the PCEF, the PCRF only can accept the IP flow mobility routing rule, i.e. the PCRF can't reject the IP flow mobility. This will cause the IP flows being moved without taking into account if resources are available in the target access. In the particular case of the WLAN access IP flows are moved without taking into account the result of the admission control request for the new IP flows in the BBF network.

5.4.2 Solution A

When the HA receives the IP flow mobility request from the UE, the HA shall not respond the Binding acknowledge to the UE immediately. Instead, the PCEF shall wait until the PCRF performed admission control in BBF access network to send Binding acknowledgement to the UE. If the BBF access network rejects the request, the PCRF shall reject the IP flow mobility routing rule and then the HA rejects the IP flow mobility request according to the response from the PCRF.

5.4.3 Conclusion

The existing IP flow mobility specification supports all procedures needed for IP flow mobility between 3GPP accesses and WLAN accesses located in a BBF access network. As described above in 5.4.1, when the admission control function rejects a request, the actions to be taken are not specified in the IP Flow mobility specifications which cause UE implementation dependent responses. This issue is not BBAI specific but applicable to any access systems that support admission control.

5.5 Procedures for the case when WLAN is being used

5.5.1 Procedures for untrusted WLAN with traffic routed back to the EPC with S2b

5.5.1.1 Initial Attach with PMIPv6 on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 7.2.1

This clause is related to the case when the UE powers-on in an untrusted BBF access network via PMIPv6 based S2b interface.

In the non-roaming case, PMIPv6 specification, RFC 5213, is used to setup a PMIPv6 tunnel between the ePDG and the PDN GW. It is assumed that MAG is collocated with ePDG. The IPSec tunnel between the UE and the ePDG provides a virtual point-to-point link between the UE and the MAG functionality on the ePDG.

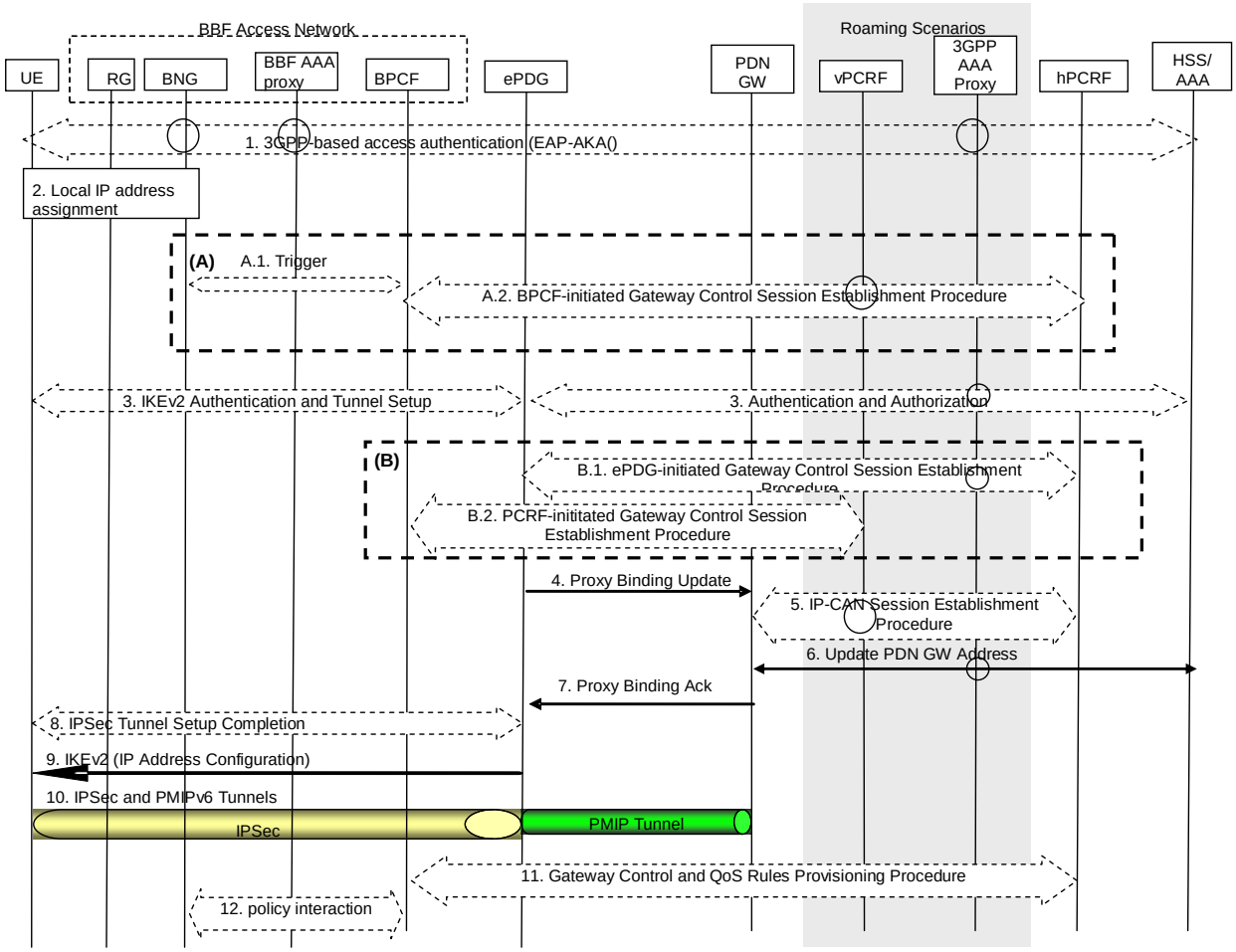


Figure 5.5.1.1-1: Initial attachment when Network-based MM mechanism are used over PMIPv6 based S2b for roaming, non-roaming and LBO

NOTE 1: Before the UE initiates the setup of an IPSec tunnel with the ePDG it configures an IP address from an untrusted non-3GPP IP access network. This address is used for sending all IKEv2 messages and as the source address on the outer header of the IPSec tunnel.

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional steps A.2, B.2 and 11 do not occur. Instead, the BBF Access Network may employ BBF local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

1. The UE may perform the 3GPP based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

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

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

A.2 If the BPCF receives the trigger in step A.1 and policy interworking with PCRF is supported, the BPCF initiates S9a session establishment. The BPCF includes the IMSI, IP-CAN type and local UE IP address in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 1-A.1 is out of scope for 3GPP specifications.

3. The description of this step is the same as for step 1 in TS 23.402 [3], clause 7.2.1

B1 In Alternative B, the ePDG initiates Gxb* session establishment with the PCRF by using Gateway Control Session establishment procedure. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC and the outer IP header information of the tunnelled traffic in the message to the PCRF (also including UDP source port number if NAT is detected).

For roaming case (both home routed and LBO), the ePDG initiates Gateway Control Session establishment procedure with the vPCRF. The ePDG contains IMSI, APN, IP-CAN type , UE IP address allocated by EPC and outer IP header information of the tunnelled traffic in the request message. When the vPCRF receives a Gateway Control Session establishment request, the vPCRF shall initiate S9 session establishment/modification procedure. The vPCRF sends a S9 session establishment request to the hPCRF with the information received over Gxb* interface excluding tunnelled traffic related info (e.g. outer IP header info of the tunnelled traffic).

B.2Triggered by the Gxb* session establishment, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF.

4-10. The description of these steps are the same as for steps 3-9 in TS 23.402 [3], clause 7.2, with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected) are also included in the Proxy Binding Update in step 4. The local UE IP address and optionally UDP source port number (if NAT is detected) are forwarded to the PCRF in step 5.

11. The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected).

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

5.5.1.1a Initial Attach with GTP on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 7.2.4.

Editor's note: Only the different procedures compare to clause 5.5.1.1 are described here.

This clause is related to the case when the UE powers-on in an untrusted BBF access network via S2b interface.

GTPv2 (see TS 29.274 [19]) is used to setup GTP tunnel(s) between the ePDG and the PDN GW. The IPSec tunnel between the UE and the ePDG provides a virtual point-to-point link between the UE and the ePDG.

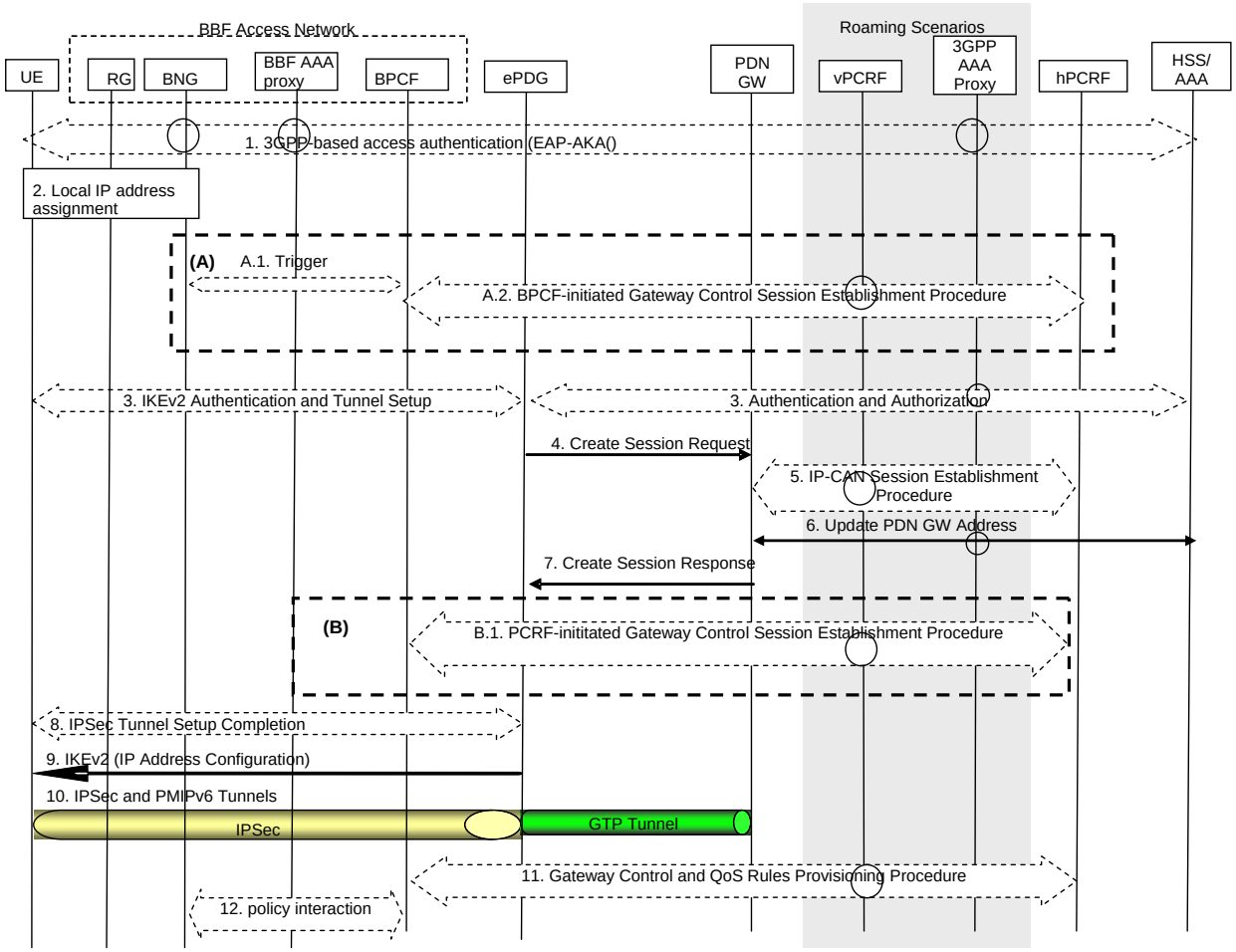


Figure 5.5.1.1a-1: Initial attachment when Network-based MM mechanism are used over GTP based S2b for roaming, non-roaming and LBO

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.

1-3. The description of these steps are the same as for step 1-3 in clause 5.5.1.1.

A.1-A.2. The description of these steps are the same as for step A.1-A.2 in clause 5.5.1.1.

4-7. The description of these steps are the same as for step A-D in TS 23.402 [3], clause 7.2.4, with following additions: the UE local IP address are also included in the Create Session Request message at step 4. The UE local IP address is forwarded to the PCRF at step 5.

B.1 Triggered by step 5, the PCRF triggers the BPCF to do Gateway Control Session establishment to establish S9a Session. The IMSI, IP-CAN type, outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF. In roaming scenarios, for home routed roaming case the hPCRF initiates Gateway Control Session establishment over S9 with the vPCRF and for LBO roaming scenarios, the vPCRF initiates Gateway Control Session establishment over S9 with the hPCRF For both home routed and LBO the vPCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session.

8-12. The description of these steps are the same as for step 8-12 in clause 5.5.1.1.

5.5.1.2 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with PMIPv6 on S2b

Non-Roaming, Home Routed Roaming and Local Breakout Case

Editor's note: This procedure is based on TS 23.402 [3], clause 7.4.1.1.

The procedure in this clause applies to Detach Procedures, initiated by UE or ePDG initiated detach procedure, and to the UE-requested PDN disconnection procedure.

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.

For multiple PDN connectivity, this detach procedure shall be repeated for each PDN connected.

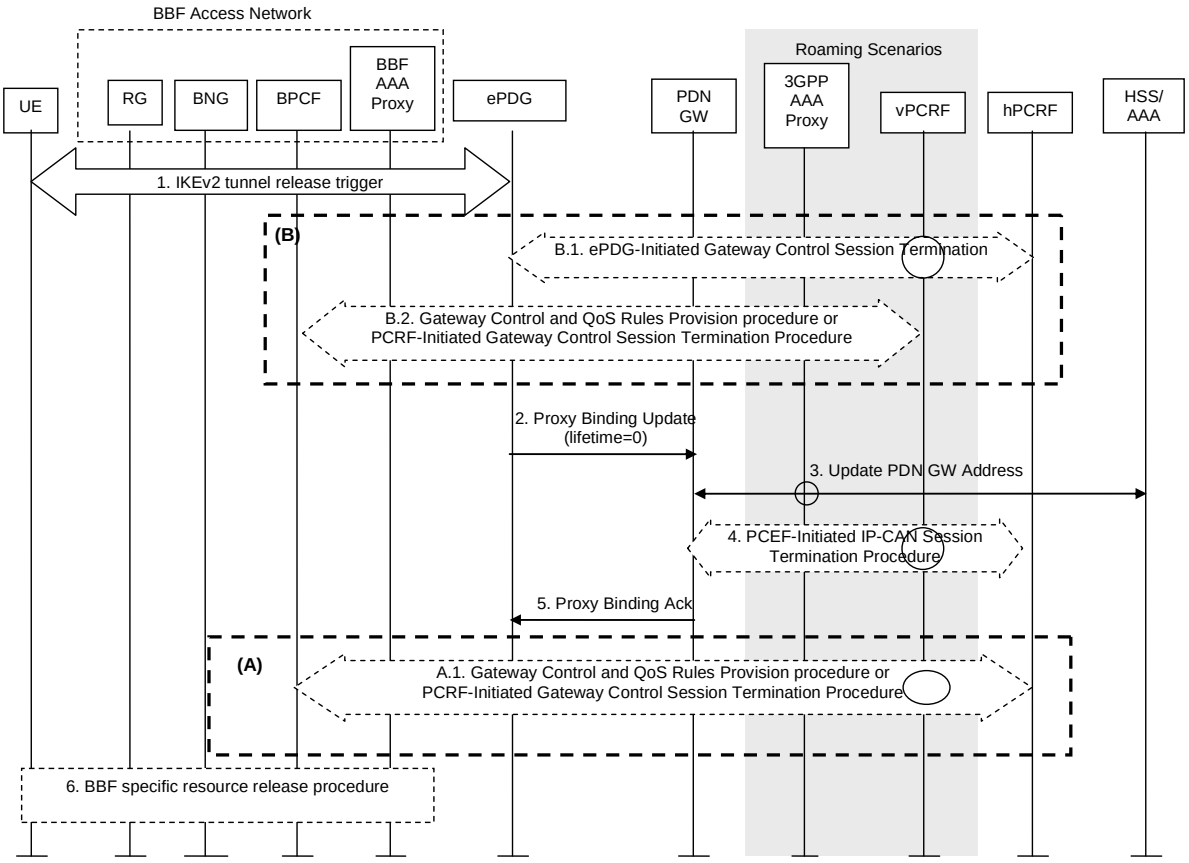


Figure 5.5.1.2-1: UE/ePDG-initiated detach procedure with PMIPv6 on S2b

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional steps A.1 and B.2 do not occur. Instead, the BBF access network may employ BBF local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are performed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

1) The description of this step is the same as for step 1 in TS 23.402 [3], clause 7.4.1.1.

B.1 Triggered by the IKEv2 tunnel release, the ePDG executes Gateway Control Session termination procedure with the PCRF.

For roaming case, the ePDG executes Gateway Control Session termination procedure with the vPCRF. Accordingly, the vPCRF initiates S9 session termination/modification with the hPCRF.

B.2 After receiving Gateway Control Session Termination from the ePDG, the PCRF (non-roaming case) or the vPCRF (roaming case) 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.

2-5) The description of these steps are the same as for steps 2-5 in TS 23.402 [3], clause 7.4.1.1

A.1 Triggered by the IP-CAN session termination in step 4, 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.

6) BBF specific resource release procedure is executed. This step is out of the scope of 3GPP.

5.5.1.2a UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with GTP on S2b

Non-Roaming, Home Routed Roaming and Local Breakout Case

Editor's note: This procedure is based on TS 23.402 [3], clause 7.4.3.1.

Editor's note: Only the different procedures compare to clause 5.5.1.2 are described here.

The procedure in this clause applies to Detach Procedures, initiated by UE or ePDG initiated detach procedure, and to the UE-requested PDN disconnection procedure.

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.

For multiple PDN connectivity, this detach procedure shall be repeated for each PDN connected.

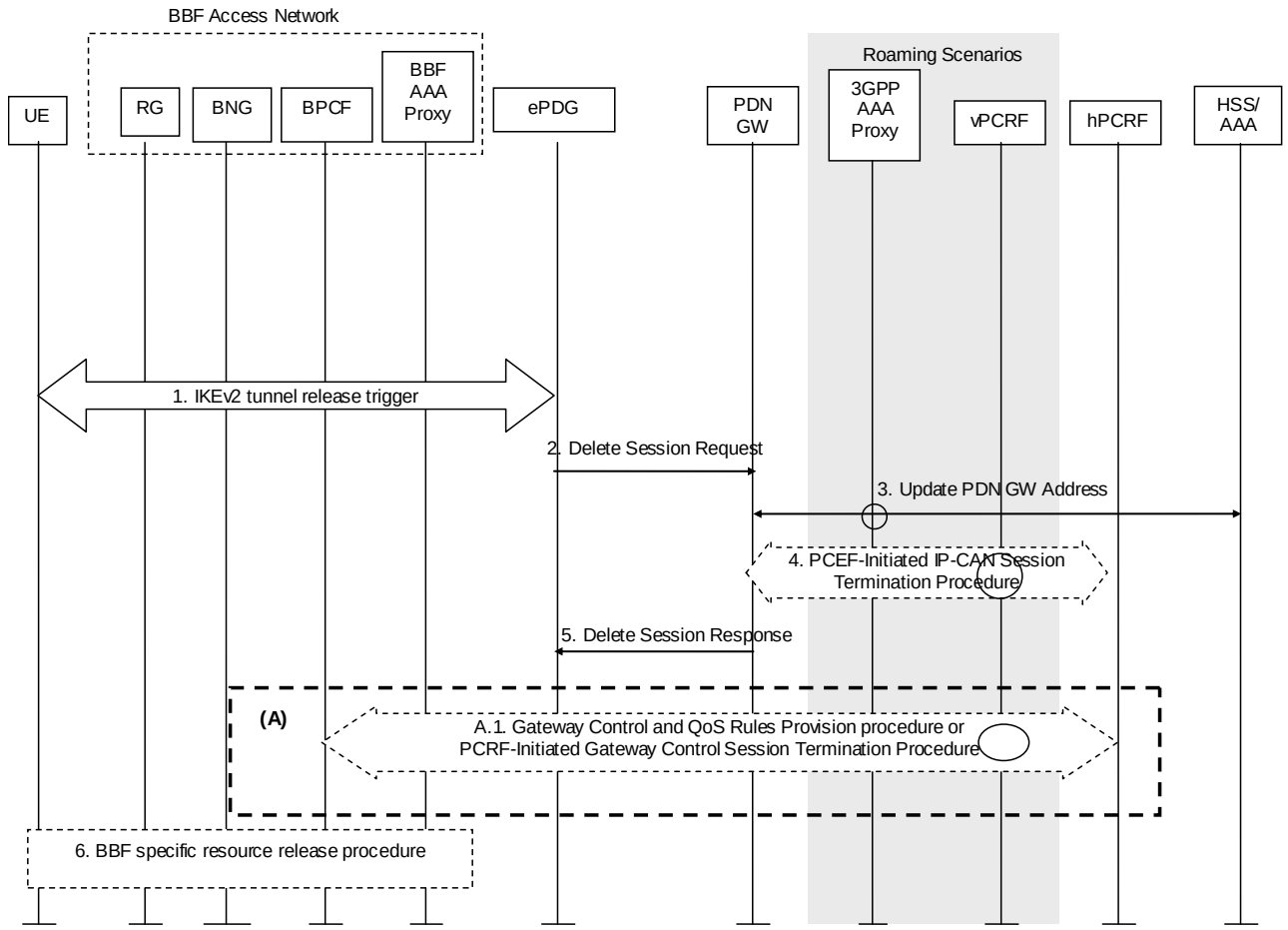


Figure 5.5.1.2a-1: UE/ePDG-initiated detach procedure with GTP based S2b

1-5) The description of these steps are the same as the steps in TS 23.402 [3], clause 7.4.3.1.

A.1) Triggered by the IP-CAN session termination in step 4, 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.

6) The description of this step is the same as for step 6 in TS 23.402 [3], clause 7.4.1.1.

5.5.1.3 HSS/AAA-initiated Detach Procedure with PMIPv6 on S2b

Non-Roaming, Home Routed Roaming and Local Breakout Case

Editor's note: This procedure is based on TS 23.402 [3], clause 7.4.2.1.

HSS/AAA-initiated detach procedure with PMIPv6 for non-roaming case is illustrated in Figure 5.5.1.3-1. The HSS can initiate the 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.

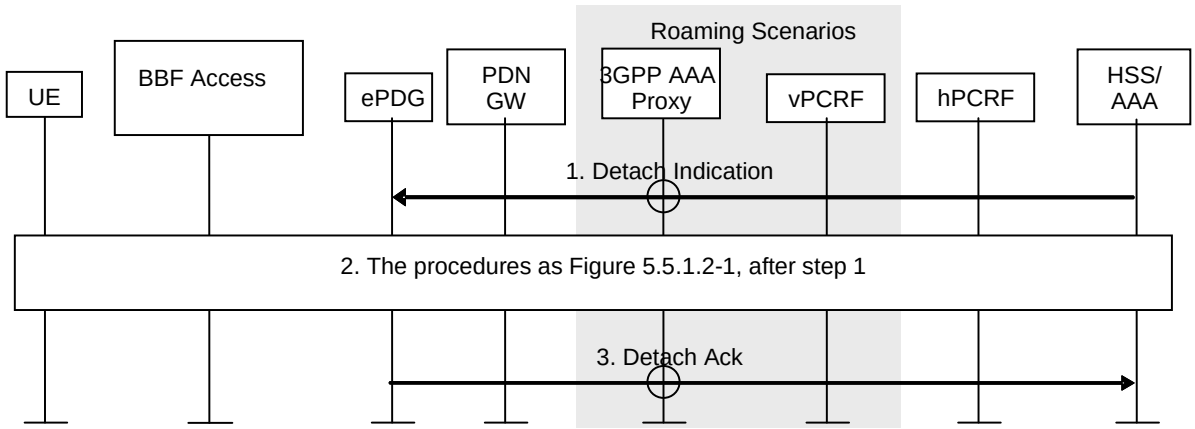


Figure 5.5.1.3-1: HSS/AAA-initiated detach procedure with PMIPv6 based S2b

NOTE 1: AAA proxy and vPCRF are only used in the case of home routed roaming and local breakout.

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 includes the procedure after step 1 in Figure 5.5.1.2-1. For multiple PDN connectivity, this step shall be repeated for each PDN Connected.

NOTE 1: The IKEv2 tunnel release is initiated by ePDG triggered by Detach Indication when last PDN connection is disconnected.

3) The description of this step is the same as for step 3 in TS 23.402 [3], clause 7.4.2.1.

NOTE 2: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIPv6 tunnels on S2b, since the ePDG is responsible for removing the PMIPv6 tunnels on S2b. The PDN GW acknowledges the receipt of the detach indication message to the HSS/AAA.

5.5.1.3a HSS/AAA-initiated Detach Procedure with GTP on S2b

Non-Roaming, Home Routed Roaming and Local Breakout Case

Editor's note: This procedure is based on TS 23.402 [3], clause 7.4.4.1.

Editor's note: Only the different procedures compare to clause 5.5.1.3 are described here.

HSS/AAA-initiated detach procedure with GTP for non-roaming case is illustrated in Figure 5.5.1.3a-1. The HSS can initiate the 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.

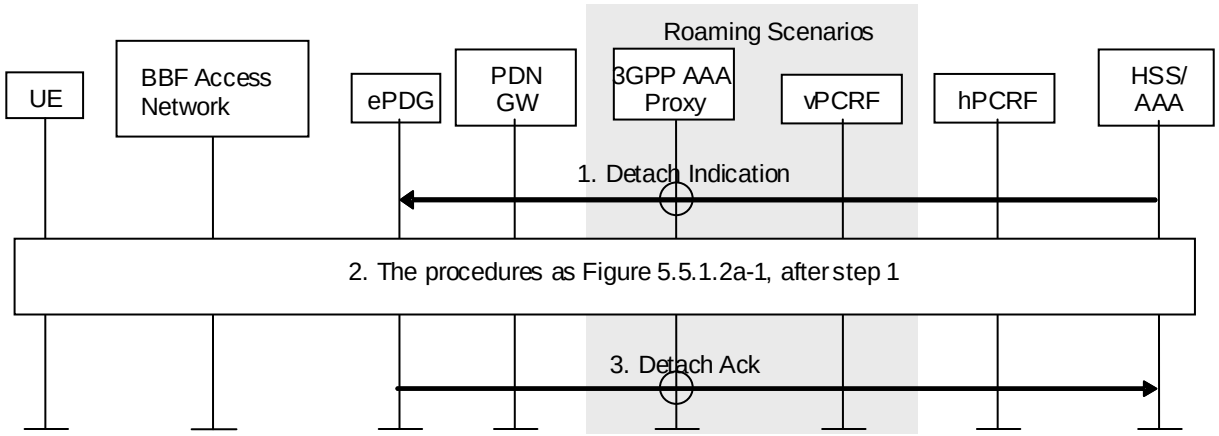


Figure 5.5.1.3-1: HSS/AAA-initiated detach procedure with GTP based S2b

1) The description of this step is the same as for step 1 in TS 23.402 [3], clause 7.4.4.1

2) This includes the procedure after step 1 in Figure 5.5.1.2a-1. For multiple PDN connectivity, this step shall be repeated for each PDN Connected.

NOTE 1: The IKEv2 tunnel release is initiated by ePDG triggered by Detach Indication when last PDN connection is disconnected.

3) The description of this step is the same as for step 3 in TS 23.402 [3], clause 7.4.4.1.

NOTE 2: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the GTP tunnels on S2b, since the ePDG is responsible for removing the GTP tunnels on S2b. The PDN GW acknowledges the receipt of the detach indication message to the HSS/AAA.

5.5.1.4 E-UTRAN to Untrusted Non-3GPP IP Access Handover with PMIPv6 on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 8.2.3.

This clause shows a call flow for a handover when a UE moves from an E-UTRAN to an untrusted non-3GPP access network. GTP or PMIPv6 is assumed to be used on the S5/S8 interface and PMIPv6 is used on the S2b interface.

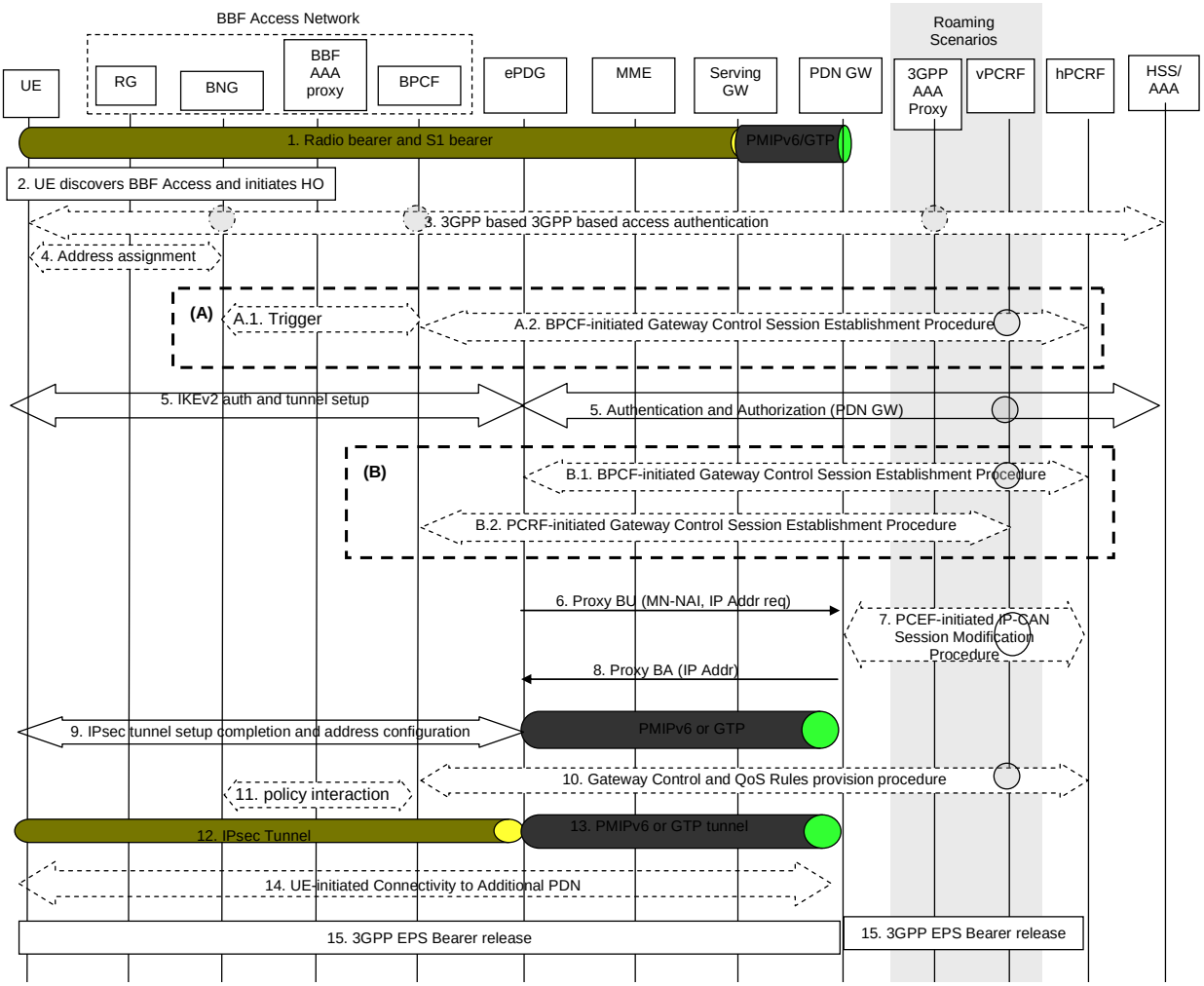


Figure 5.5.1.4-1: E-UTRAN to Untrusted Non-3GPP IP Access Handover with PMIPv6 on s2b

Both the roaming and non-roaming scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved.

For connectivity to multiple PDNs, step 14 is repeated for each PDN the UE is connected to. Step 14 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1 of TS 23.402 [3].

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise BBF access network may employ BBF local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

1-2) The description of these steps are the same as for steps 1-2 in TS 23.402 [3], clause 8.2.3.

3) The UE may perform the 3GPP-based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

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

A.1) Triggered by steps 3 and 4, the BPCF is informed about the UE accessing over BBF Access. How this is done is out of 3GPP scope.

A.2) If the BPCF receives the trigger in step A.1 and policy interworking with fixed accesses is supported, the BPCF initiates S9a session establishment. The BPCF includes the IMSI, UE IP Address and IP-CAN type in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 3-5 is out of scope for 3GPP specifications.

5) The description of this step is the same as for step 3 in TS 23.402 [3], clause 8.2.3.

B.1) The ePDG initiates Gxb* session establishment by using Gateway Control Session establishment procedure with the PCRF. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC and the outer IP header information of the tunnelled traffic in the message to the PCRF (also including UDP source port number if NAT is detected).

For roaming case, the ePDG initiates Gateway Control Session establishment procedure with the vPCRF. The ePDG contains IMSI, APN, IP-CAN type, UE IP address allocated by EPC and outer IP header information of the tunnelled traffic in the request message. When the vPCRF receives a Gateway Control Session establishment request, the vPCRF shall initiate S9 session establishment/modification procedure. The vPCRF sends a S9 session establishment request to the hPCRF with the information received over Gxb* interface excluding tunnelled traffic related info (e.g. outer IP header info of the tunnelled traffic).

B.2) Triggered by the Gxb* session establishment, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF.

6-9) The description of these steps are the same as for steps 4-7 in TS 23.402 [3], clause 8.2.3 with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected) are also included in the Proxy Binding Update in step 8. The local UE IP address and optionally UDP source port number (if NAT is detected) are forwarded to the PCRF in step 9.

10) The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF. with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected). Depending on the reply from the BPCF, the PCRF may update the PCC rules in the PCEF.

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

12-15) The description of these steps are the same as for steps 8-10 in TS 23.402 [3], clause 8.2.3.

5.5.1.4a E-UTRAN to Untrusted Non-3GPP IP Access Handover with GTP on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 8.6.2

Editor's note: Only the different procedures compare to clause 5.5.1.4 are described here.

This clause shows a call flow for a handover when a UE moves from an E-UTRAN to an untrusted non-3GPP access network. GTP or PMIPv6 is assumed to be used on the S5/S8 interface and GTP is used on the S2b interface.

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

- In the LBO case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the PDN GW in the VPLMN. The vPCRF receives the Acknowledgment from the PDN GW and forwards it to the hPCRF.

- In the non-roaming case, the vPCRF is not involved.

In case of connectivity to multiple PDNs the same behaviour as described in clause 5.5.1.4 also applies to this procedure.

The optional interaction steps between the PDN gateway and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the PDN gateway.

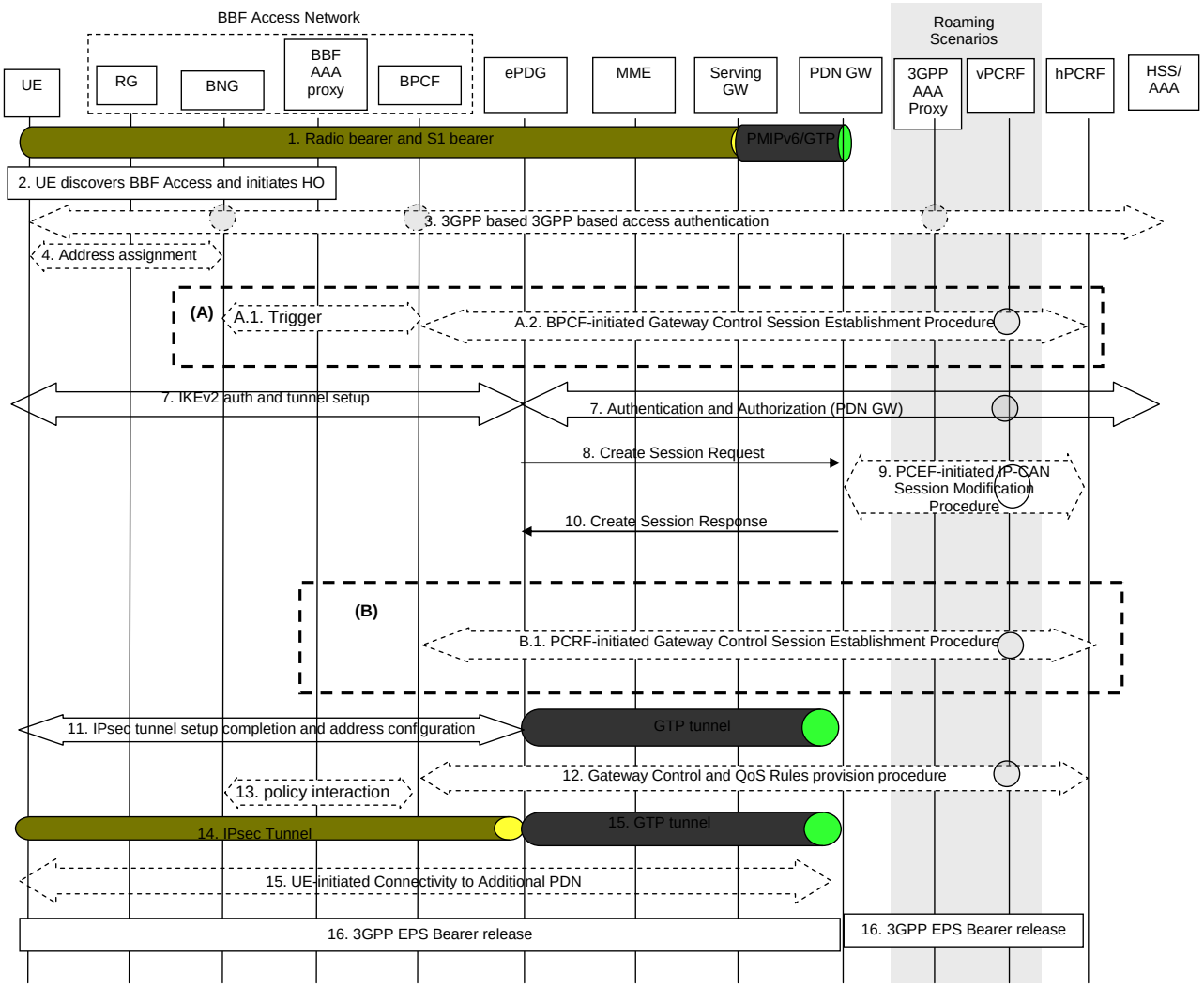


Figure 5.5.1.4-1: E-UTRAN to Untrusted Non-3GPP IP Access Handover with GTP on S2b

1-7) The description of these steps are the same as for steps 1-7 in clause 5.4.1.4.

8-10) The description of these steps are the same as for steps A-C in TS 23.402 [3], clause 8.6.2, with following additions: the UE local IP address are also included in the Create Session Request message at step 8. The UE local IP address is forwarded to the PCRF at step 9.

B.1) Triggered by step 9, the PCRF triggers the BPCF to do Gateway Control Session establishment to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF. In roaming scenarios, for home routed roaming case the hPCRF initiates Gateway Control Session establishment over S9 with the vPCRF and for LBO roaming scenarios, the vPCRF initiates Gateway Control Session establishment over S9 with the hPCRF For both home routed and LBO the vPCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session.

11-16) The description of these steps are the same as for steps 11-16 in clause 5.4.1.4.

5.5.1.5 UE-initiated Connectivity to Additional PDN with PMIPv6 or GTP on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 7.6.1.

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address/prefix for each binding.

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 GTP or PMIPv6 is used to establish connectivity with the additional PDN, the UE establishes 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 both the ePDG and the PDN GW support that feature. For PMIPv6 based S2b, when multiple PDN connections to a given APN are supported, during the establishment of a new PDN connection, the ePDG creates and sends a PDN Connection identity to the PDN GW. The PDN connection identity is unique in the scope of the UE and the APN within an ePDG, i.e. the MN-ID, the APN, and the PDN connection identity together identify a PDN connection within an ePDG. In order to be able to identify a specific established PDN connection, both the ePDG and the PDN GW shall store the PDN Connection identity. Sending the PDN connection identity is an indication that the ePDG supports multiple PDN connections to a single APN and the PDN GW shall be able to indicate if it supports multiple PDN connections to a single APN. Between the UE and the ePDG the IPSec SA associated with the PDN connection identifies the PDN connection.

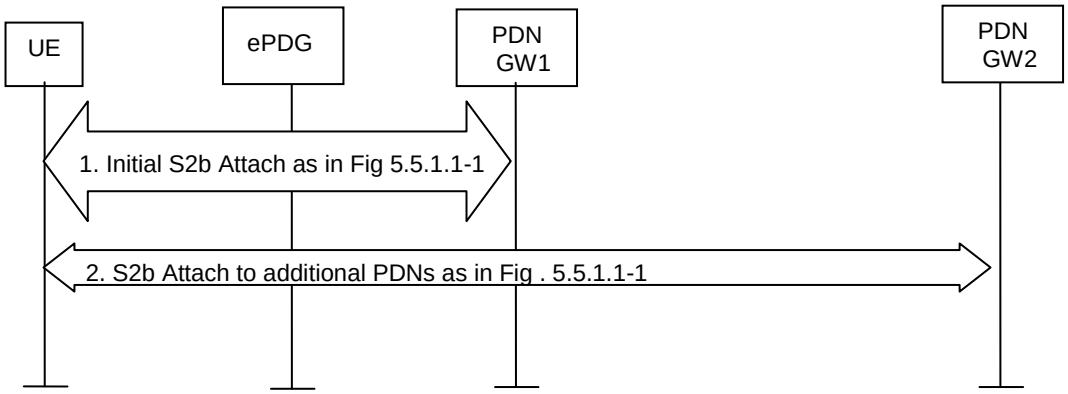


Figure 5.5.1.5-1: UE-initiated connectivity to additional PDN from Un-trusted Non-3GPP IP Access with PMIPv6 or GTP on s2b

1) The UE has performed the Initial S2b Attach procedure as defined in clause 5.5.1.1 or clause 5.5.1.1a and has an established PDN connection.

2) The UE repeats the procedure of clause 5.5.1.1, Figure 5.5.1.1-1 or clause 5.5.1.1a, Figure 5.5.1.1a-1 for each additional PDN the UE wants to connect to, with the following exceptions:

   a) Steps 1-2, A and B are only performed in the initial attach procedure and not when connecting to an additional PDN.

   b) The IKEv2 tunnel establishment procedure for each additional PDN connection is initiated with the ePDG that was selected in step 1;

   c) For network supporting multiple mobility protocols, if there was any dynamic IPMS decision in step 3, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.

5.5.1.6 Network-Initiated Dynamic PCC for S2b when accessing over BBF access

This procedure is applicable if the UE accesses over a BBF Access network.

If dynamic PCC is deployed, the procedure given in Figure 5.5.1.6-1 is used by the PCRF to provision rules to the BBF IP access and for the BBF IP 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 BBF access and the PCRF is capable to discover the BPCF for the BBF serving the UE. The access specific procedure executed in the BBF access is not within the scope of this specification.

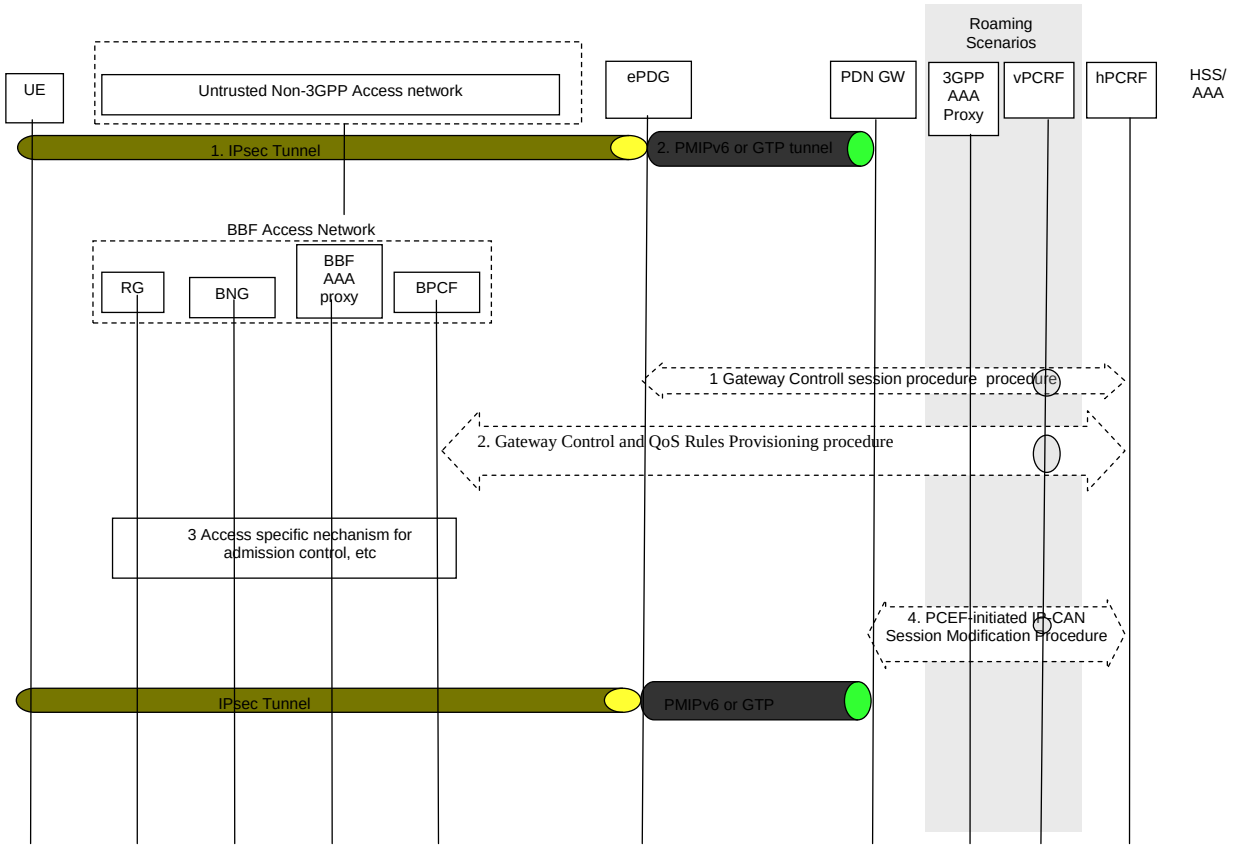


Figure 5.5.1.6-1: Network-initiated dynamic policy control procedure in untrusted BBF IP Access for S2b

This procedure concerns both the non-roaming (as Figure 5.1.2-1) and roaming case (as Figure 5.1.2-4). 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 5.1.2-5), 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 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. The PCRF initiates the Gateway Control and QoS Policy Rules Provision Procedure specified in TS 23.203 [4] by sending a message with the QoS rules to the BPCF.

2. the PCRF executes a Gateway Control and QoS Rules Provisioning procedure In roaming scenario, the hPCRF will initiate the procedure over S9 towards the vPCRF and the vPCRF in turns initiates the procedure over S9a towards the BPCF.

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

4. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [4]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules Provision procedure specified in TS 23.203 [4].

NOTE: Step 4 may occur before step 1 or performed in parallel with steps 1-3 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [4].

5.5.1.6a PGW-Initiated Dynamic PCC for GTP based S2b when accessing over BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.11.1.

This procedure is applicable if the UE accesses over a BBF Access network.

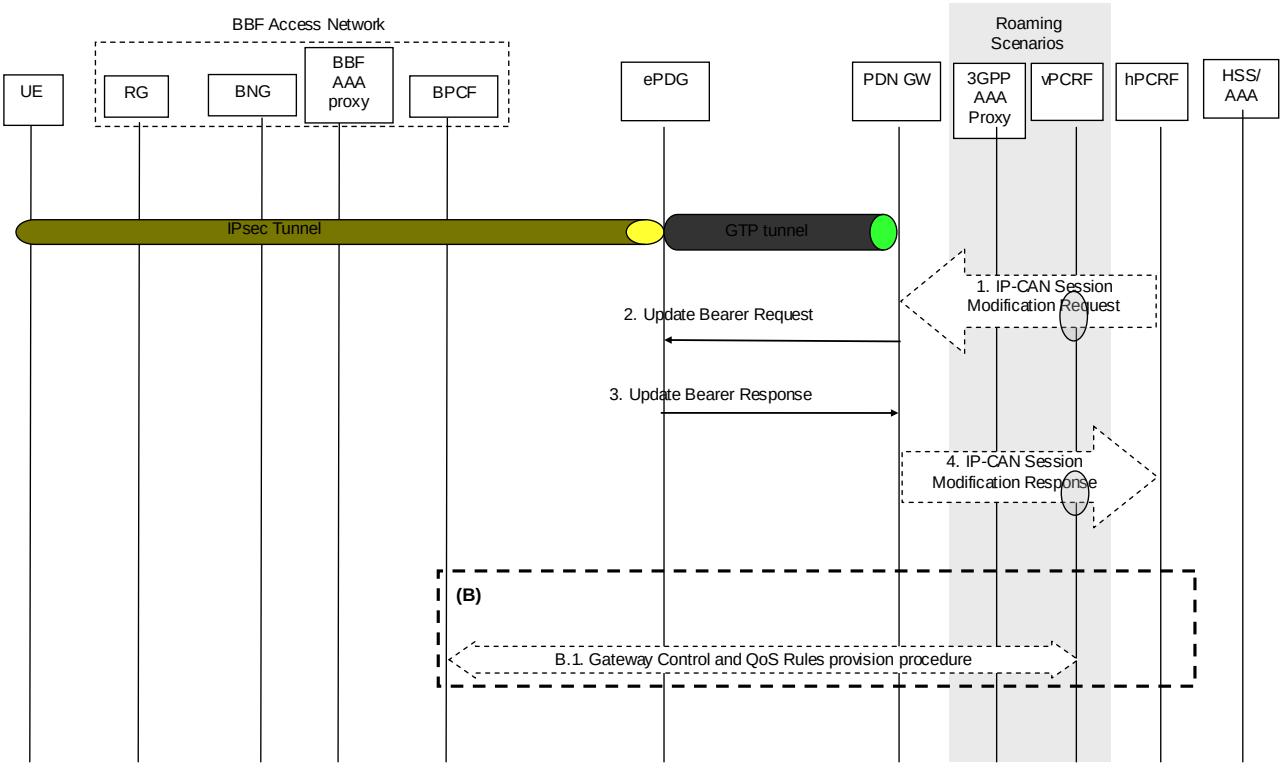


Figure 5.5.1.6a-1: PGW-initiated dynamic policy control procedure in untrusted BBF IP Access for GTP based S2b

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1-4) The description of these steps are the same as for steps 1-4 in TS 23.402 [3], clause 7.11.1.

B.1) The description of the step is the same as for steps B.2 in clause 5.5.1.6.

5.5.1.6b HSS-Initiated Subscribed QoS Modification for GTP based S2b when accessing over BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.11.2.

This procedure is applicable if the UE accesses over a BBF Access network.

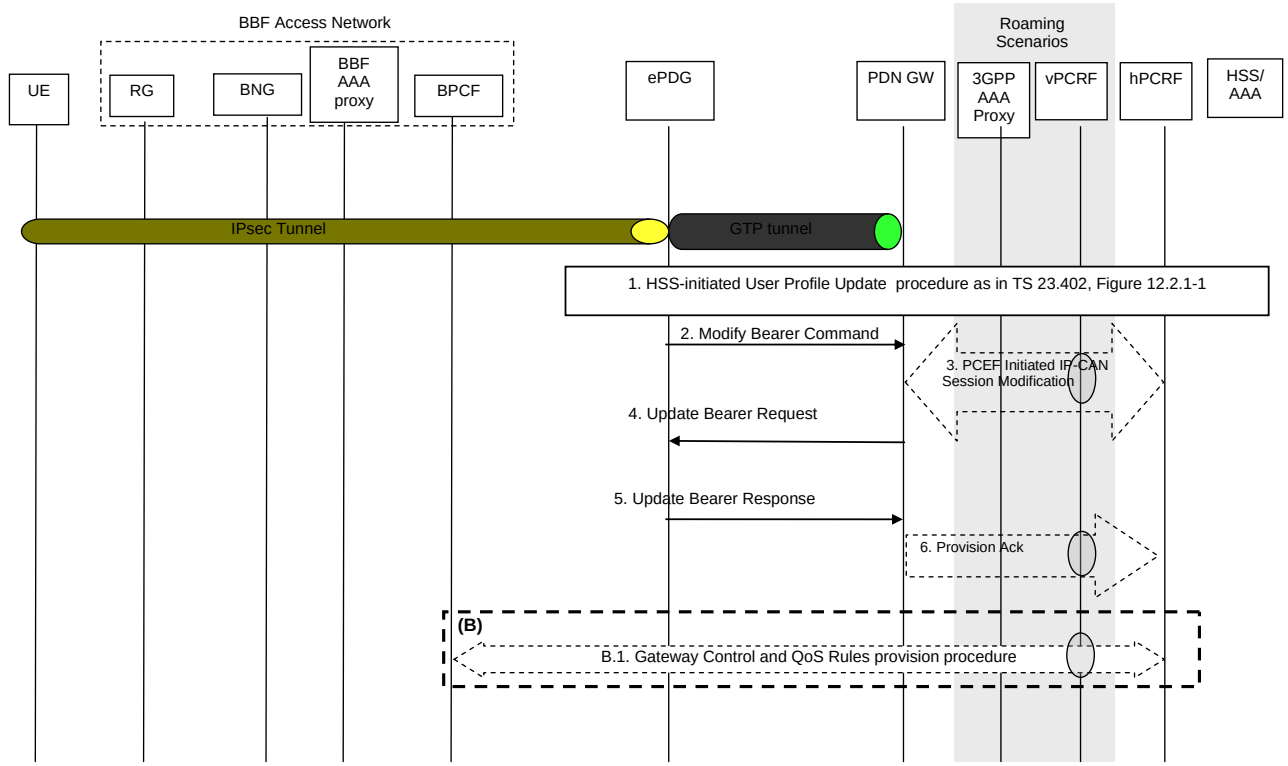


Figure 5.5.1.6a-1: HSS-Initiated Subscribed QoS Modification in untrusted BBF IP Access for GTP based S2b

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1-6) The description of these steps are the same as for steps 1-6 in TS 23.402 [3], clause 7.11.2.

B.1) The description of the step is the same as for steps B.2 in clause 5.5.1.6.

5.5.1.7 PDN GW initiated Resource Allocation Deactivation with S2b PMIPv6 when accessing over BBF Access Network

Editor's note: This procedure is new compared to TS 23.402 [3].

This procedure is applicable if the UE accesses over a BBF Access network.

This procedure is performed to release all the resources associated with the PDN address, for example, due to IP-CAN session modification requests from the PCRF or due to handover Non-3GPP to 3GPP. When it is performed for an handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

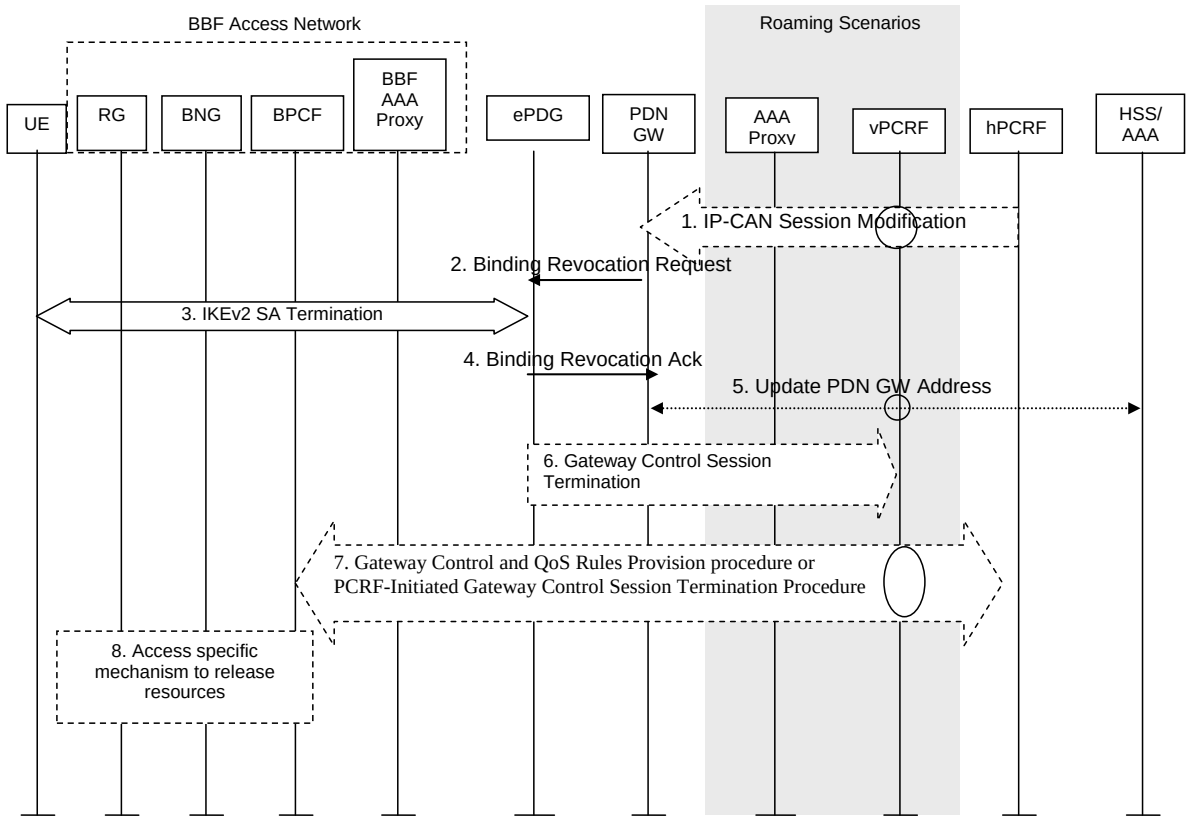


Figure 5.5.1.7-1: PDN GW Initiated Binding Revocation with PMIPv6 on s2b

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP IP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages 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 in figure 5.5.17-1 only occur if dynamic policy provisioning is deployed. Otherwise policy BBF access network may employ BBF local policies

1. If dynamic PCC is deployed, the PDN GW initiated Resource Allocation Deactivation procedure may for example be triggered due to 'IP-CAN session Modification procedure', as defined in TS 23.203 [4]. In this case, the resources associated with the PDN connection in the PDN GW are released.

   The PDN GW initiated Resource Allocation Deactivation can also be triggered during handovers from Non-3GPP to 3GPP.

2. The PDN GW sends a Binding Revocation Indication message to ePDG as defined in draft-ietf-mext-binding-revocation [35].

3. The ePDG releases the IPSec tunnel.

4. The trusted non-3GPP IP access returns a Binding Revocation Acknowledgement message to the PDN GW.

5. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the AAA Server/HSS to remove the PDN GW identity information and APN corresponding to the UE's PDN Connection. This information is de-registered from the HSS as described in clause 12.

6. Triggered by the IPSec tunnel termination, the ePDG terminates the Gxb* session. This step only applies in case Gxb* was used to trigger initiation of the S9a session from PCRF.

NOTE: Step 6 may occur before or after steps 7-8. Step 6 does not trigger step 7.

7. Based on the updated PCC rules 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. In roaming scenario, the hPCRF will initiate the procedure over S9 towards the vPCRF and the vPCRF in turns initiates the procedure over S9a towards the BPCF.

8. The resources may be released in the BBF access, according to an access specific release mechanism.

5.5.1.7a PDN GW initiated Resource Allocation Deactivation with S2b GTP when accessing over BBF Access Network

Editor's note: This procedure is based on TS 23.402 [3], clause 7.9.2.

This procedure can be used to deactivate a dedicated bearer or deactivate all bearers belonging to a PDN address, for example, due to IP-CAN session modification requests from the PCRF or due to handover from Non-3GPP to 3GPP access. If the default bearer belonging to a PDN connection is deactivated, the PDN GW deactivates all bearers belonging to the PDN connection.

When it is performed for an handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

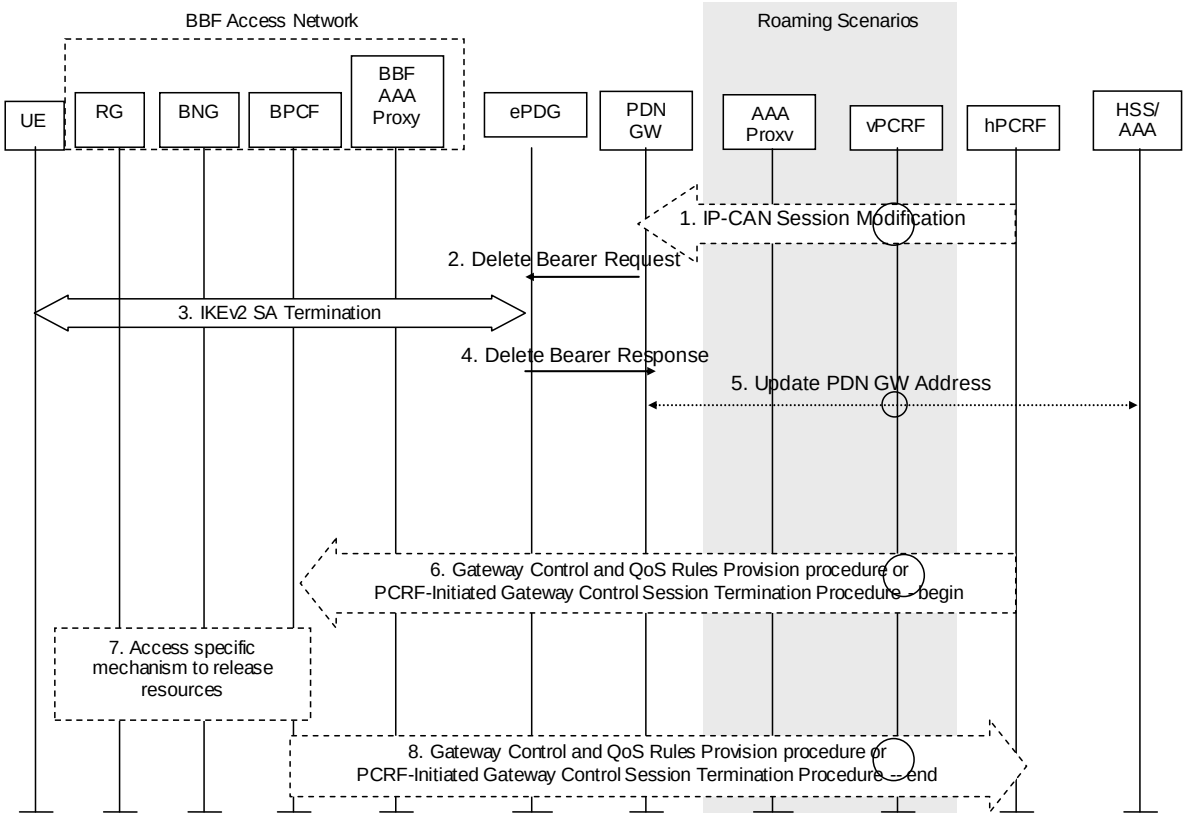


Figure 5.5.1.7a-1: PDN GW Initiated Binding Revocation with S2b GTP

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP IP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages 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 in figure 5.5.17a-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1-5) The description of these steps are the same as for steps 1-5 in TS 23.402 [3], clause 7.9.2.

6-8) The description of these steps are the same as for steps 7-9 in clause 5.5.1.7.

5.5.1.8 Handover without ePDG relocation for PMIPv6 based S2b

The procedure described in this clause is informative.

This clause is related to the case when the UE handover from one untrusted non-3GPP access to BBF access network, when PMIPv6 based S2b is used.

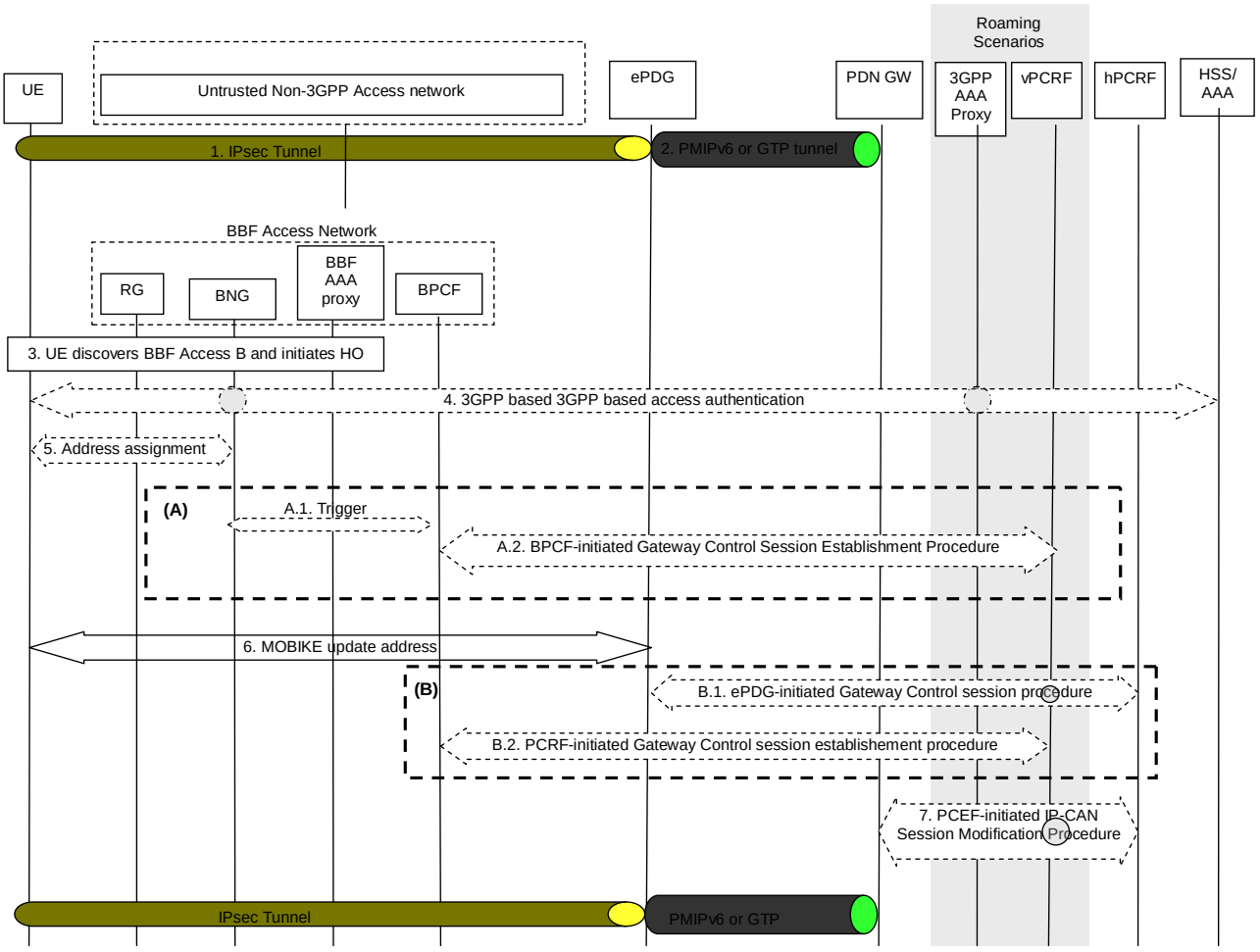


Figure 5.5.1.8-1: Handover without ePDG relocation for PMIPv6 based S2b

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

The following steps are performed:

1~2. The UE is connected from one untrusted non-3GPP access to ePDG via the IPSec tunnel and a PMIPv6 tunnel is established between the PDN GW and ePDG.

3. UE discovers BBF network and initiates handover procedure.

   Step 4-5 are same to the attach procedure step 1-2 in figure 5.5.1.1-1.

A.1 - A.2. These steps are the same as in the attach procedure step A.1 - A.2 in figure 5.5.1.1-1.

6. MOBIKE update address message exchange (in both directions, initiated by UE). And optionally, MOBIKE address verification, initiated by ePDG, is send to UE as described in MOBIKE [18].

B.1. The ePDG initiates Gxb* session establishment or modification, if Gxb* has established, with the PCRF. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC and the outer IP header information of the tunnelled traffic in the message to the PCRF.

B.2. Triggered by the Gxb* session establishment or modification, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF.

7. PCRF may initiate IP-CAN session modification by PCC provision procedure.

5.5.1.8a Handover without ePDG relocation for GTP based S2b

Editor's note: Only the different procedures compare to clause 5.5.1.8 are described here.

The procedure described in this clause is informative.

This clause is related to the case when the UE handover from one untrusted non-3GPP access to BBF access network, when GTP based S2b is used.

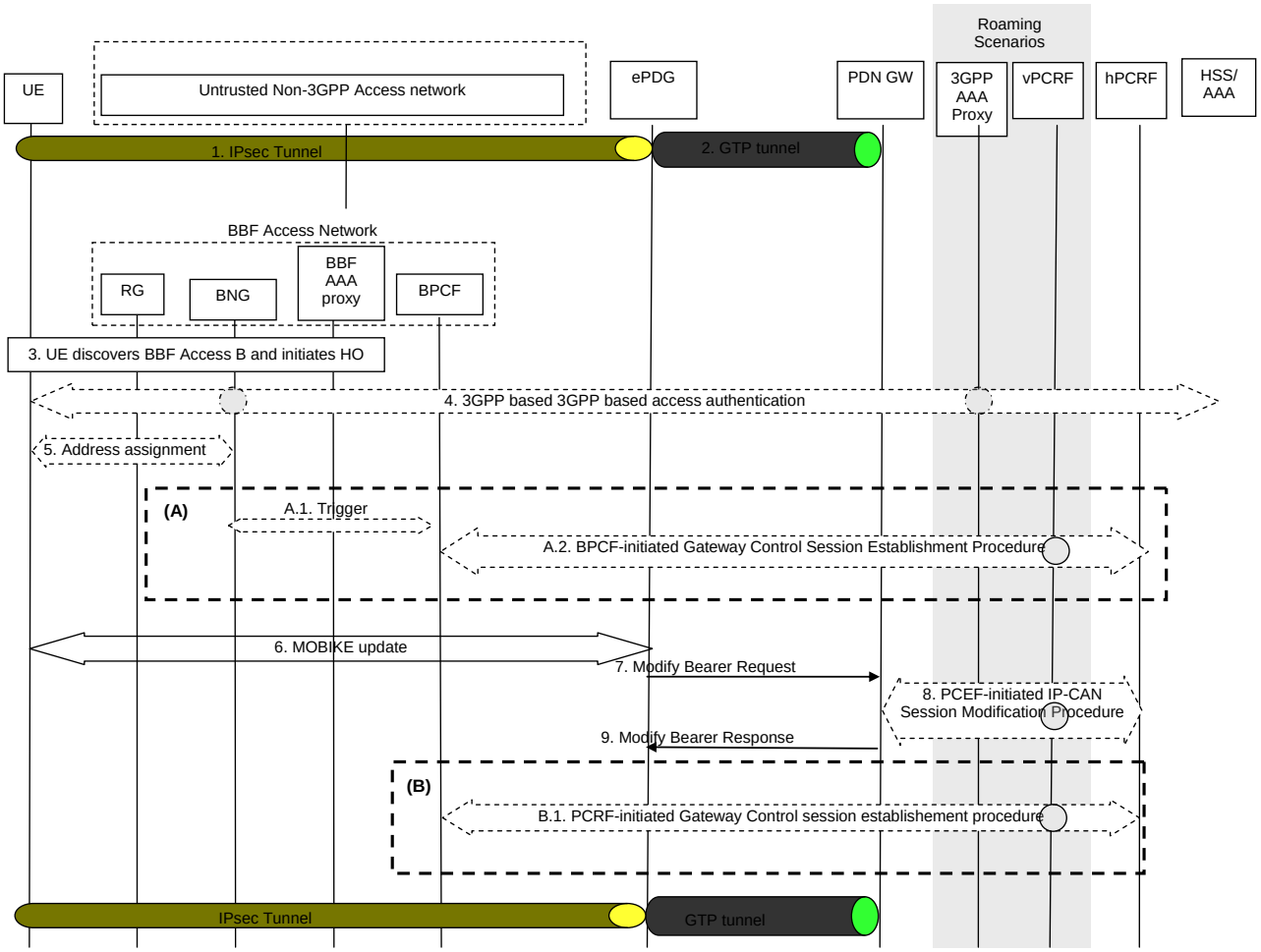


Figure 5.5.1.8a-1: Handover without ePDG relocation for GTP based S2b

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

The following steps are performed:

1~2. The UE is connected from one untrusted non-3GPP access to ePDG via the IPSec tunnel and a GTP tunnel is established between the PDN GW and ePDG.

3. UE discovers BBF network and initiates handover procedure.

Step 4-5 are same to the attach procedure step 1-2 in figure 5.5.1.1a-1.

A.1 - A.2. These steps are the same as in the attach procedure step A.1 – A.2 in figure 5.5.1.1a-1.

6. IKEv2 update message exchange (in both directions, initiated by UE). And optionally, MOBIKE address verification, initiated by ePDG, is send to UE as described in MOBIKE [18].

7. ePDG sends Modify bearer request message with the new UE local IP address to PGW.

8. PGW initiates IP-CAN session modification procedure.

9. PGW responses with Modify Bearer Response message to ePDG.

B.1. Triggered by IP-CAN session modification procedure, the PCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF. In roaming scenarios, for home routed roaming case the hPCRF initiates Gateway Control Session establishment over S9 with the vPCRF and for LBO roaming scenarios, the vPCRF initiates Gateway Control Session establishment over S9 with the hPCRF. For both home routed and LBO the vPCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session.

5.5.1.9 IPSec tunnel modified within the same untrusted BBF WLAN IP Accesses with PMIPv6 based S2b

This clause is related to the case when the UE initiates IPSec tunnel update procedure, which may be as a result of that UE IP address for IPSec tunnel changed, for example IP address is expired and new IP address is allocated to UE.

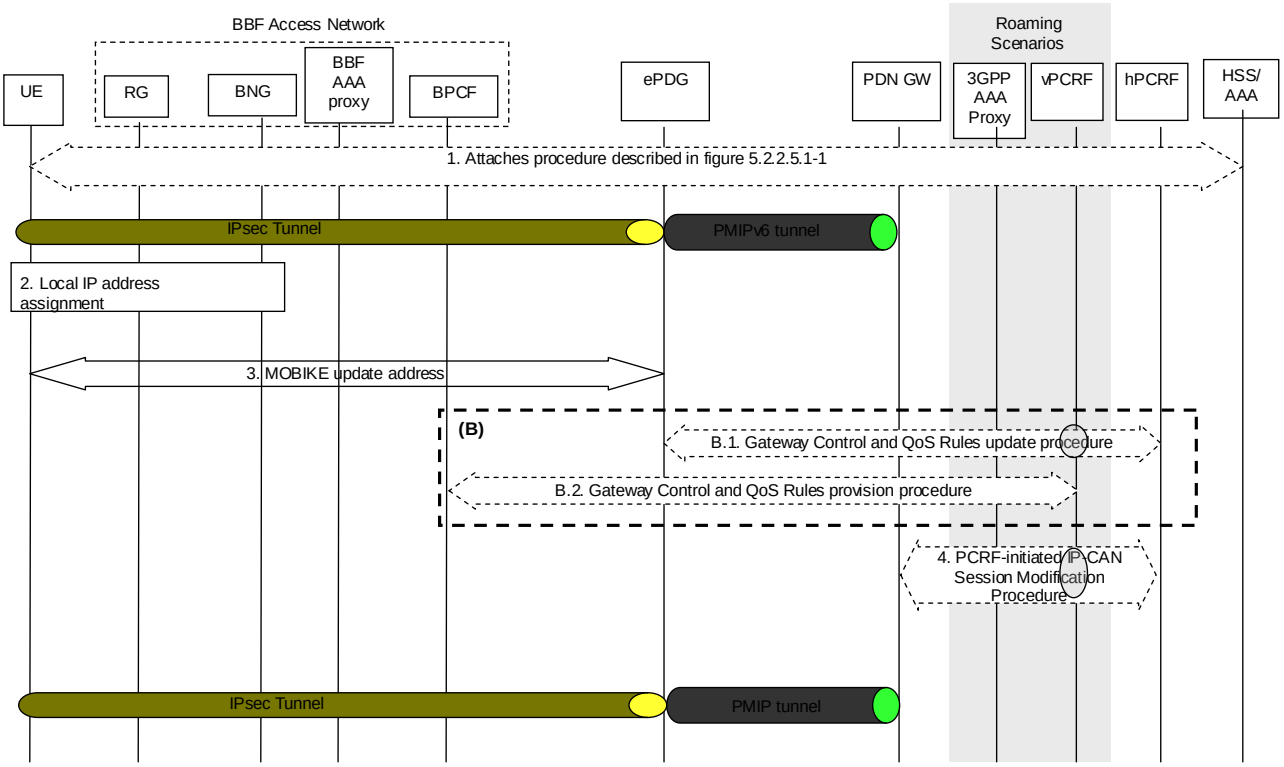


Figure 5.5.1.9-1. IPSec tunnel modified without ePDG relocation for PMIPv6 based S2b

The steps shown in (A) and (B) are mutually exclusive in this procedure, i.e. either steps A.1-A.2 are executed or steps B.1-B.2. Details regarding when to use alternative A or alternative B to trigger S9a session establishment are described in clause 5.2.2.1.2.

1. UE attaches to EPC from BBF access network via ePDG, as described in figure 5.5.1.1-1. The IPSec tunnel is established between ePDG and UE; the PMIPv6 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@ 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].

B.1. The ePDG initiates Gxb* session modification with the PCRF. The ePDG includes the updated outer IP header information of the tunnelled traffic in the message to the PCRF (also including UDP source port number if NAT is detected).

B.2. Triggered by the Gxb* session modification, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session modification with the BPCF to update S9a Session. The updated outer IP header information for tunnel traffic is included in the request message which sending to the BPCF.

4. PCRF may initiate IP-CAN session modification by PCC provision procedure.

5.5.1.9a IPSec tunnel modified within the same untrusted BBF WLAN IP Accesses with GTP based S2b

This clause is related to the case when the UE initiates IPSec tunnel update procedure, which may be as a result of that UE IP address for IPSec tunnel changed, for example IP address is expired and new IP address is allocated to UE.

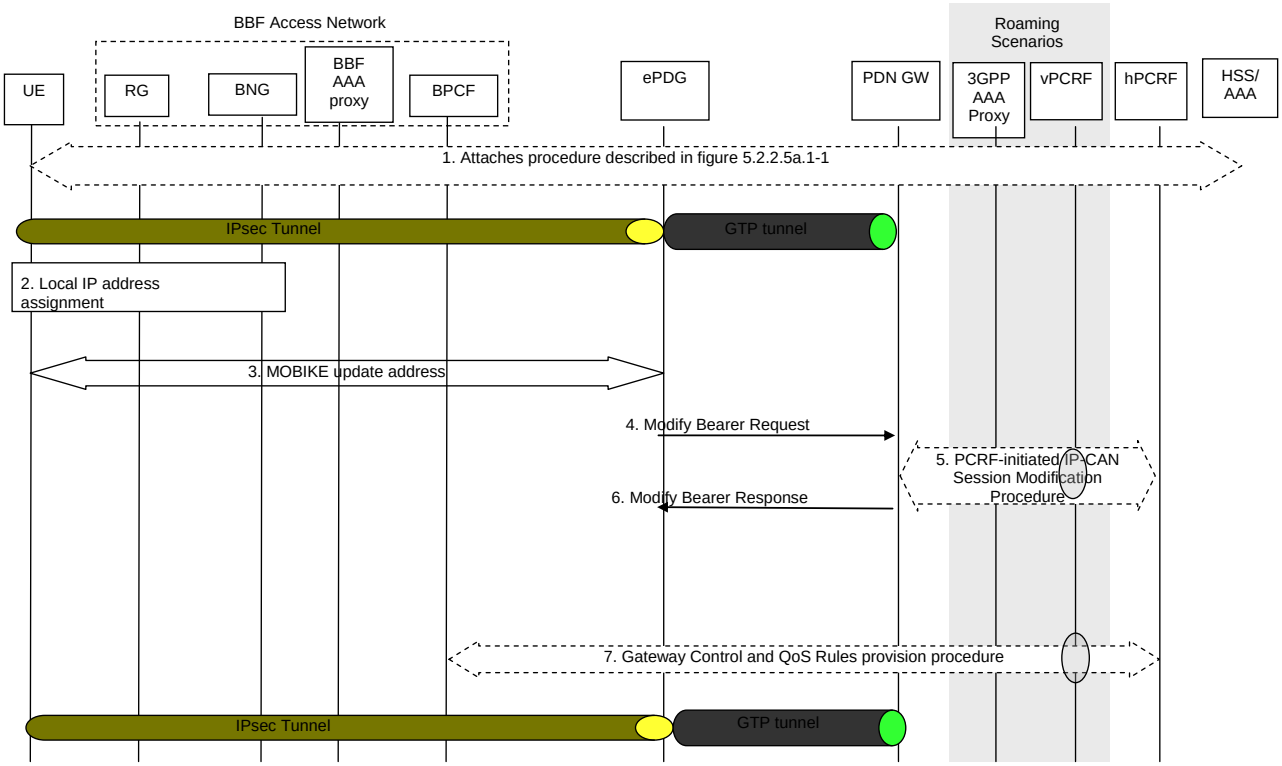


Figure 5.5.1.9-1. IPSec tunnel modified without ePDG relocation for GTP based S2b

1. UE attaches to EPC from BBF access network via ePDG, as described in figure 5.5.1.1a-1. The IPSec tunnel is established between ePDG and UE; the GTP tunnel is established between the PDN GW and ePDG.

2-3. The description of these steps are the same as for steps 2-3 in clause 5.5.1.9a.

4-7. The description of these steps are the same as for steps 4-8, B in clause 5.5.1.8a.

5.5.1.10a Dedicated bearer activation with GTP on S2b

Editor's note: This procedure is based on TS 23.402 [3], clause 7.10.

This clause shows a call flow for Dedicated S2b bearer activation. GTP is assumed to be used on the S2b interface.

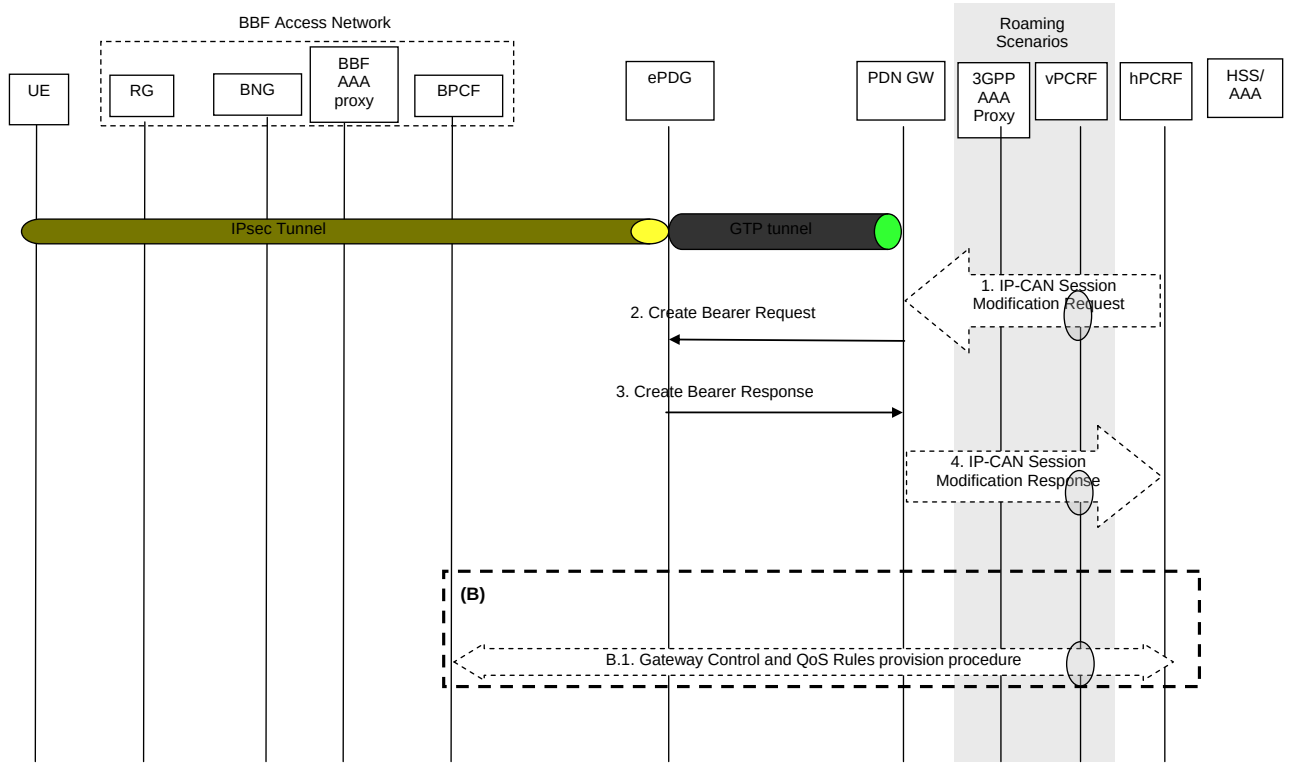


Figure 5.5.1.x-1. Dedicated S2b bearer activation for GTP based S2b

The steps shown in (A) and (B) are mutually exclusive in this procedure, i.e. either steps A.1-A.2 are executed or steps B.1-B.2. Details regarding when to use alternative A or alternative B to trigger S9a session establishment are described in clause 5.2.2.1.2.

1-4. The description of these steps are the same as for steps 1-4 in TS 23.402 [3], clause 7.10.

B.1. Triggered by step 1, the PCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF. In roaming scenarios, for home routed roaming case the hPCRF initiates Gateway Control Session establishment over S9 with the vPCRF and for LBO roaming scenarios, the vPCRF initiates Gateway Control Session establishment over S9 with the hPCRF. For both home routed and LBO the vPCRF initiates Gateway Control Session establishment with the BPCF to establish S9a Session.

5.5.2 Procedures for trusted BBF WLAN with traffic routed to the EPC with S2c

5.5.2.1 Initial Attach with DSMIPv6 on S2c to trusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 6.3.

This clause is related to the case when the UE attaches to a BBF access which is considered trusted. In this case only S2c procedures can be used in Building Block 1.

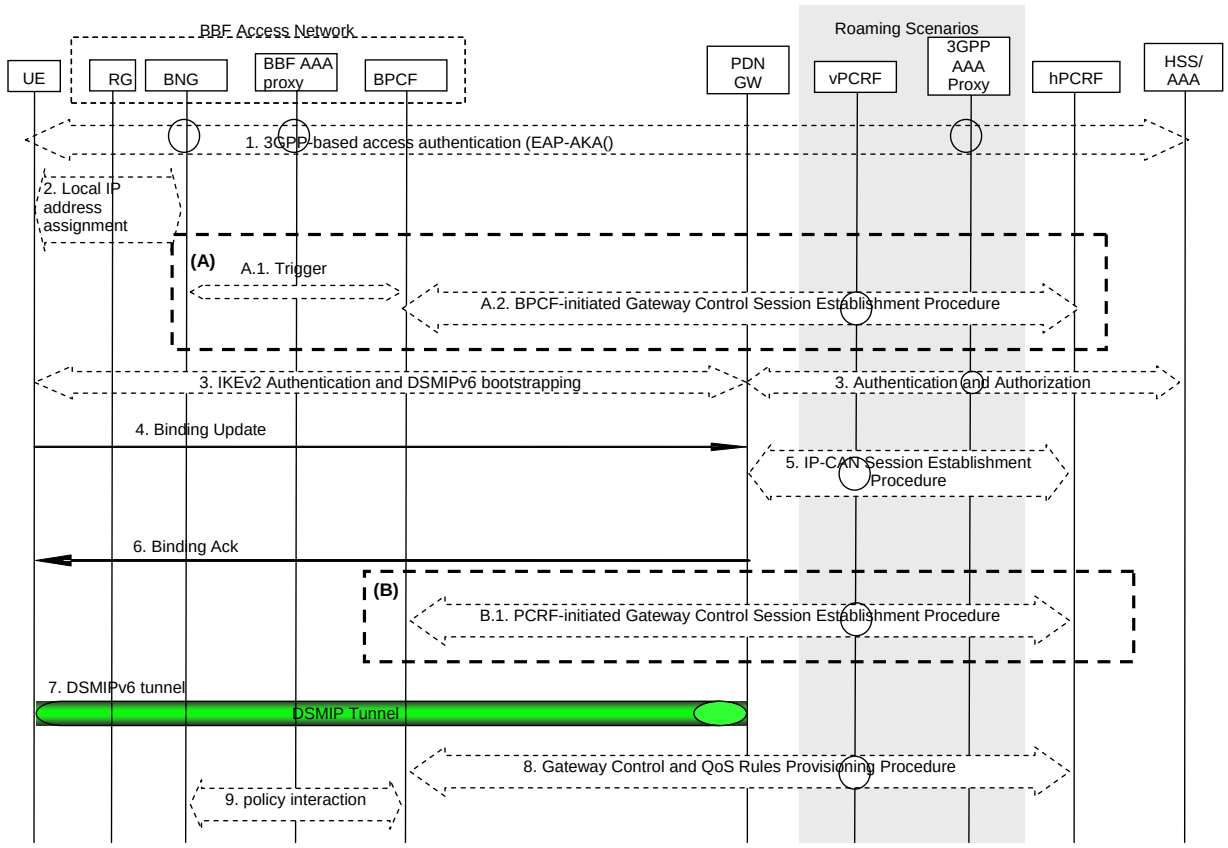


Figure 5.5.2.1-1: Initial attachment with DSMIPv6 when S2c is used for roaming, non-roaming and LBO

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional steps A.2, B.1 and 8 do not occur. Instead, the BBF Access Network may employ BBF Local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

1. The UE may perform the 3GPP based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

2. The UE receives a local IP address from the BBF Access Network which is used as CoA in S2c signalling. How this is done is out of 3GPP scope, but it may involve IP address assignment by an RG or a BNG.

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

A.2. If the BPCF receives the trigger in step A.1 and policy interworking with PCRF is supported, the BPCF initiates S9a session establishment. The BPCF includes the UE identity, and IP-CAN type in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 1-A.1 is out of scope for 3GPP specifications.

3-6. The description of these steps are the same as for steps 4-7 in TS 23.402 [3], clause 6.3 with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected) are forwarded to the PCRF in step 7.

B.1. Triggered by the IP-CAN Session establishment from the PDN GW, the PCRF initiate the S9a session establishment with the BPCF. The Care of Address, IP-CAN type, QoS information, and optionally the IMSI, needs to be included in the request message which sending to the BPCF.

7. The DSMIPv6 tunnel is established and the UE initiated its services.

8. The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF. with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected).

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

5.5.2.2 UE-initiated Detach Procedure and UE-Requested PDN Disconnection with DSMIPv6 on S2c in trusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 6.5.2.

The procedure in this clause applies to Detach Procedures, 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.

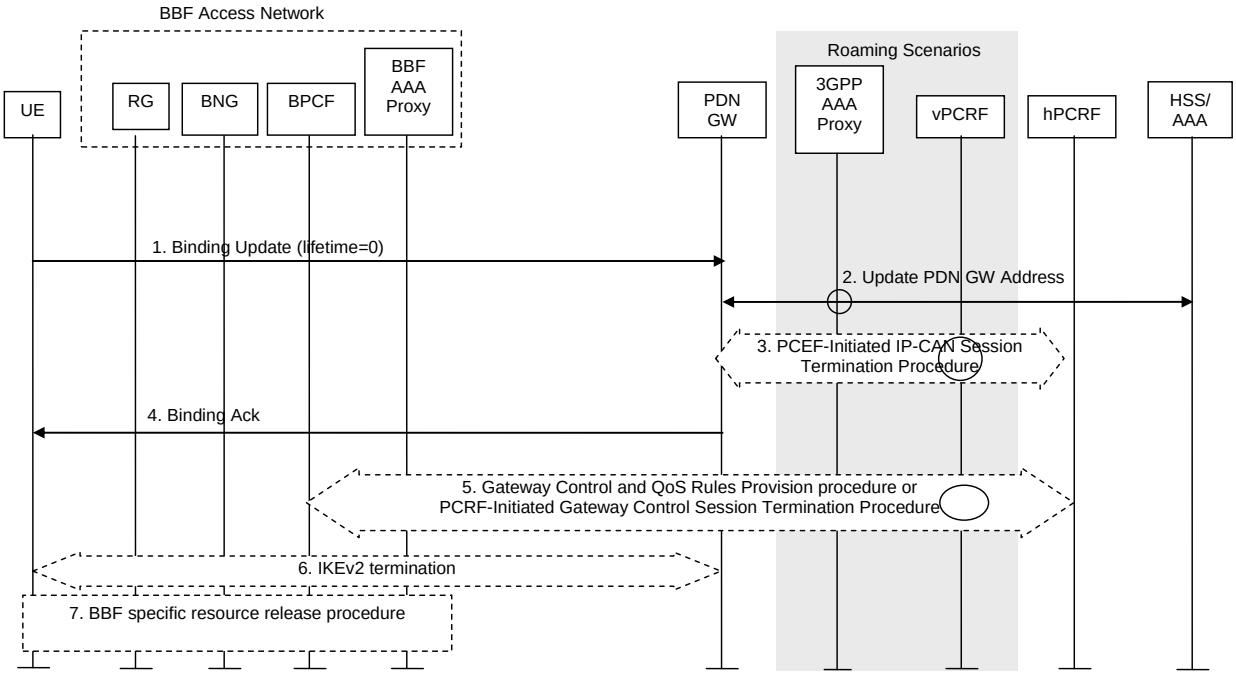


Figure5.5.2.2-1: UE-initiated detach procedure with DSMIPv6 on s2c

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional step 5 does not occur. Instead, the BBF access network may employ BBF local policies.

1-4. The description of these steps are the same as for steps 1-5 in TS 23.402 [3], clause 6.5.2.

5. Triggered by the IP-CAN session termination in step 3, 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.

6. The description of this step is the same as for step 6 in TS 23.402 [3], clause 6.5.2.

7. BBF specific resource release procedure is executed. This step is out of the scope of 3GPP.

5.5.2.3 HSS-initiated Detach Procedure with DSMIPv6 on S2c in trusted BBF access

Editor's note This procedure is based on TS 23.402 [3], clause 6.5.3.

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

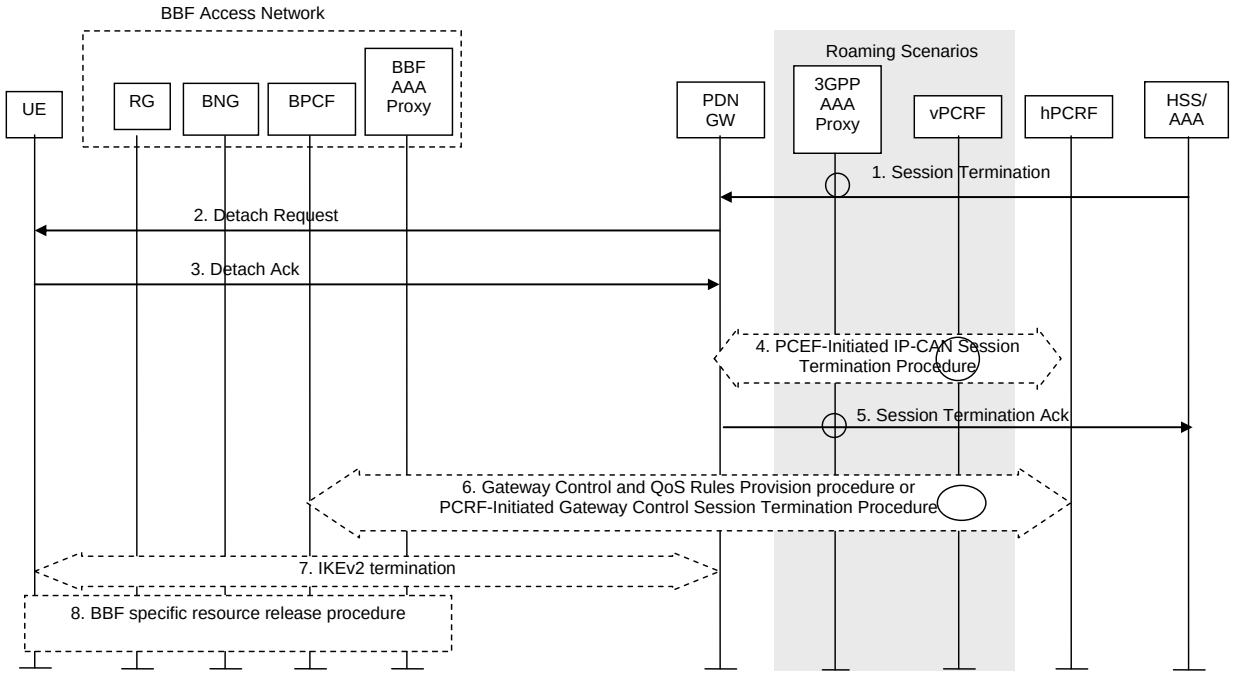


Figure5.5.2.3-1: HSS-initiated detach procedure with DSMIPv6 on s2c

1-5. The description of these steps are the same as for steps 1-5 in TS 23.402 [3], clause 6.5.3.

6. Triggered by the IP-CAN session termination in step 4, 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.

7. The description of this step is the same as for step 6 in TS 23.402 [3], clause 6.5.3.

8. BBF specific resource release procedure is executed. This step is out of the scope of 3GPP.

5.5.2.4 PDN GW-initiated PDN disconnection Procedure with DSMIPv6 on S2c in trusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 6.5.4.

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

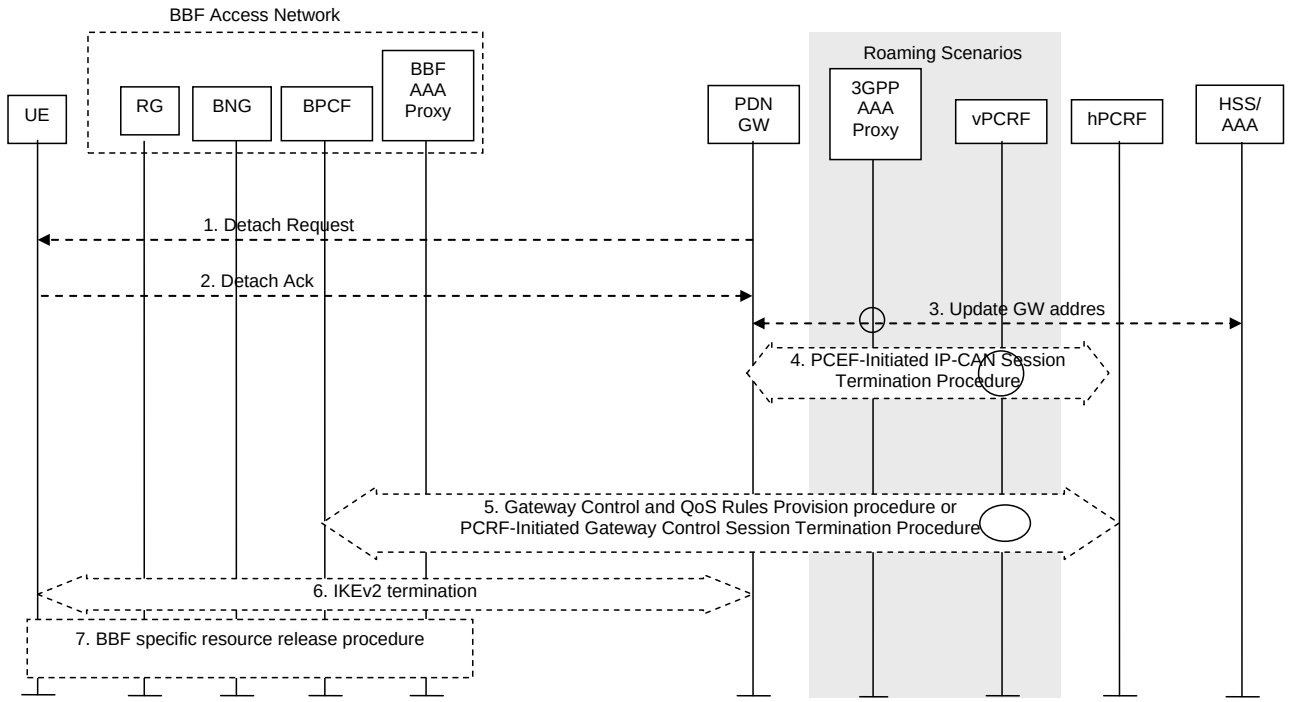


Figure 5.5.2.4-1: PDN GW-initiated PDN disconnection procedure with DSMIPv6

1-4. The description of these steps are the same as for steps 1-4 in TS 23.402 [3], clause 6.5.4.

5. Triggered by the IP-CAN session termination in step 4, 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.

6. The description of this step is the same as for step 6 in TS 23.402 [3], clause 6.5.4.

7. BBF specific resource release procedure is executed. This step is out of the scope of 3GPP.

5.5.2.5 E-UTRAN to Trusted BBF access Handover with DSMIPv6 on S2c

Editor's note: This procedure is based on TS 23.402 [3], clause 8.4.2.

This clause shows a call flow for a handover when a UE moves from an E-UTRAN to an trusted BBF access network.

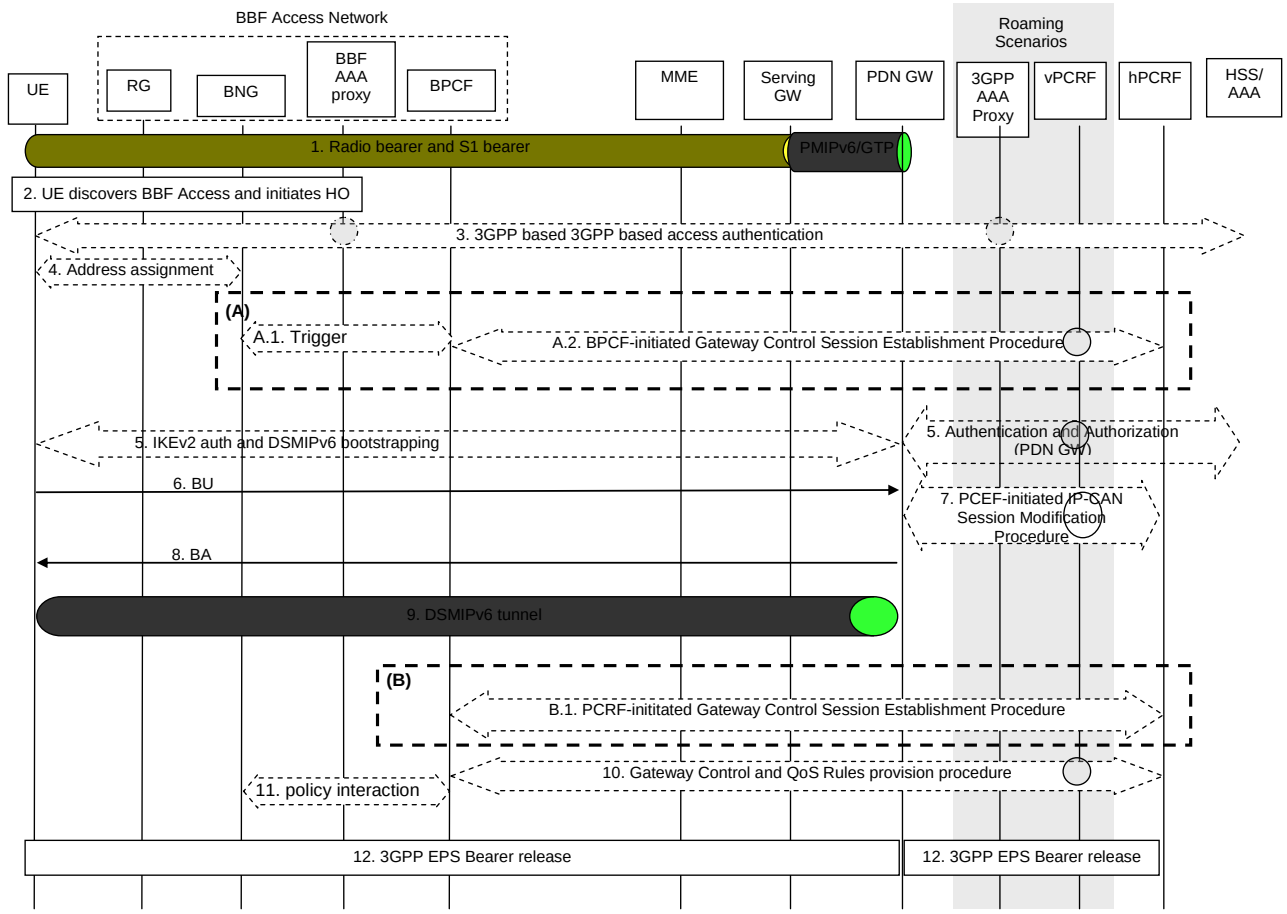


Figure 5.5.2.5-1: E-UTRAN to Trusted BBF Access Handover with DSMIPv6 on s2c

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

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise BBF access network may employ BBF local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

For connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and BBF access before the handover of PDN connections to trusted BBF access is triggered, steps 2 to A.2 shall be skipped. However whether step A.1 is executed is out of the scope of 3GPP and it is BBF specific.

- If the UE is connected only to 3GPP access before the handover of the PDN connection to trusted BBF access is triggered, steps 2 to A.2 shall be performed. However whether step A.1 is executed is out of the scope of 3GPP and it is BBF specific.

- Steps 6 to 12 shall be repeated for each PDN connection that is being transferred from 3GPP access. If not performed in 3GPP access prior to the handover, step 5 shall also repeated for each PDN connection that is being transferred from 3GPP access. The step B.1 shall be executed only if the S9a Gateway Control Session is not already established, i.e. if step A.2 has not been performed or only when the first PDN connection is established.

1-2. The description of these steps are the same as for steps 1-2 in TS 23.402 [3], clause 8.4.2.

3. The UE may perform the 3GPP-based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

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

A.1) Triggered by steps 3 and 4, the BPCF is informed about the UE accessing over BBF Access. How this is done is out of 3GPP scope.

A.2) If the BPCF receives the trigger in step A.1 and policy interworking with fixed accesses is supported, the BPCF initiates S9a session establishment. The BPCF includes the UE Identity and IP-CAN type in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 3-A.1 is out of scope for 3GPP specifications.

5-9. The description of these steps are the same as for steps 6-11 in TS 23.402 [3], c clause 8.4.2, excluding step 10. The local UE IP address and optionally UDP source port number (if NAT is detected) are forwarded to the PCRF in step 7.

B.1) Triggered by the IP-CAN Session establishment from the PDN GW, the PCRF initiate the S9a session establishment with the BPCF. The Care of Address, IP-CAN type, QoS information, and optionally the IMSI, needs to be included in the request message which sending to the BPCF.

10. The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF. with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected). Depending on the reply from the BPCF, the PCRF may update the PCC rules in the PCEF

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

12. The description of this step is the same as for step 12 in TS 23.402 [3], clause 8.4.2.

5.5.2.6 Network-Initiated Dynamic PCC for DSMIPV6 on S2c when accessing trusted BBF access

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

If dynamic PCC is deployed, the procedure given in Figure 5.5.2.6 is used by the PCRF to provision rules to the BBF IP access and for the BBF IP 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 BBF access and the PCRF is capable to discover the BPCF for the BBF serving the UE. The access specific procedure executed in the BBF access is not within the scope of this specification.

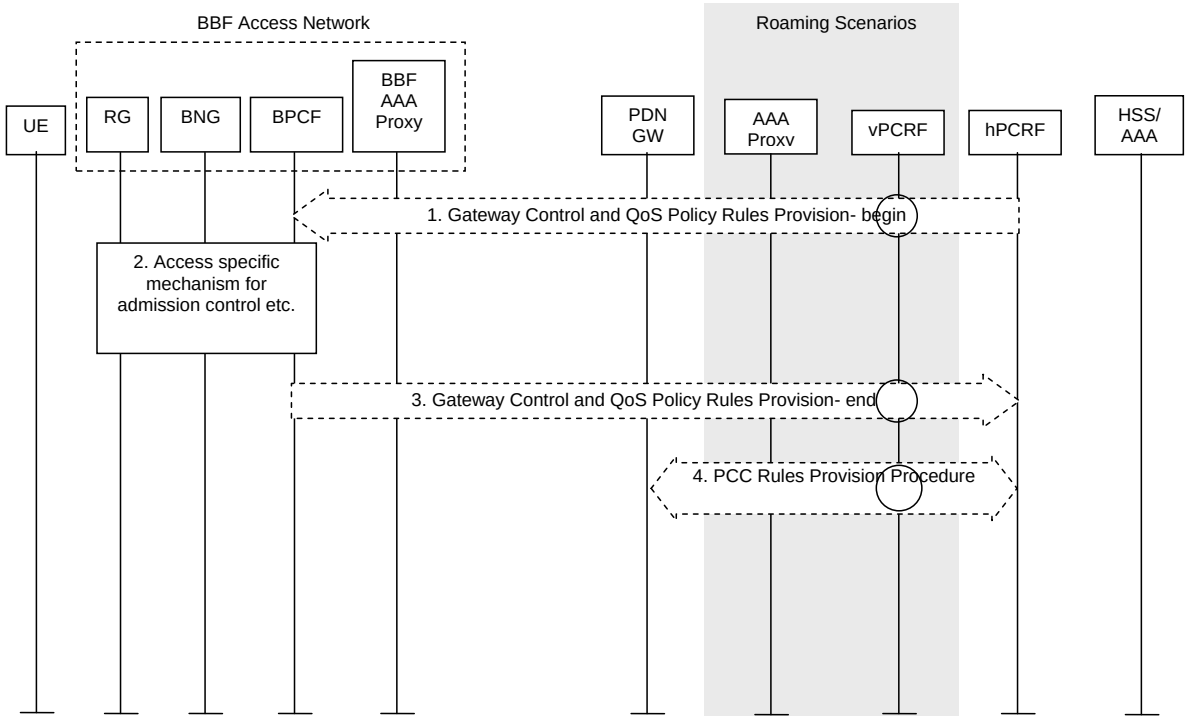


Figure 5.5.2.6-1: Network-initiated dynamic policy control procedure in Trusted BBF IP Access for DSMIPv6 on S2c

This procedure concerns both the non-roaming (as Figure 5.1.2-2) and roaming case (as Figure 5.1.2-5). 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 5.1.2-8), 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 only occur if dynamic policy provisioning is deployed. Otherwise BBF access network may employ BBF local policies.

1. The PCRF initiates the Gateway Control and QoS Policy Rules Provision Procedure specified in TS 23.203 [4] by sending a message with the QoS rules to the BPCF.

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

3. The BPCF responds to the PCRF indicating the result of the request received in Step 1 and thus completing the GW Control and QoS Rules Provision procedure started in step 1.

4. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [4]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules Provision procedure specified in TS 23.203 [4].

NOTE: Step 4 may occur before step 1 or performed in parallel with steps 1-3 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [4].

5.5.2.7 UE-Initiated Connectivity to Additional PDN with DSMIPv6 on S2c over trusted BBF 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.

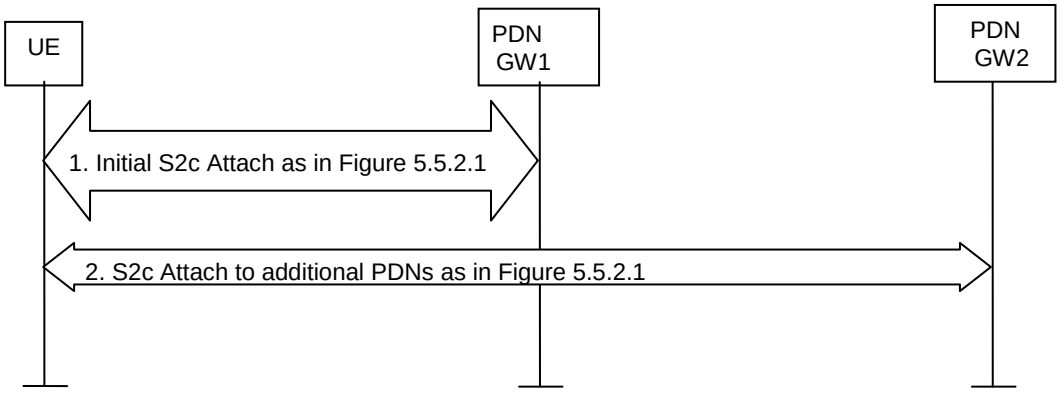


Figure 5.5.2.7-1: UE-Initiated connectivity to additional PDN from Trusted Non-3GPP IP Access with DSMIPv6 on S2c

1. The UE has performed the Initial S2c attach procedure as defined in clause 5.5.2.1 and has an established PDN connection.

2. The UE repeats the procedure steps 6-12 in clause 5.5.2.1 for each additional PDN the UE wants to connect to.

5.5.3 Procedures for untrusted BBF WLAN with traffic routed to the EPC with S2c

5.5.3.1 Initial Attach with DSMIPv6 on S2c to untrusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.3.

This clause is related to the case when the UE attaches to a BBF access which is considered untrusted. In this case only S2c procedures can be used.

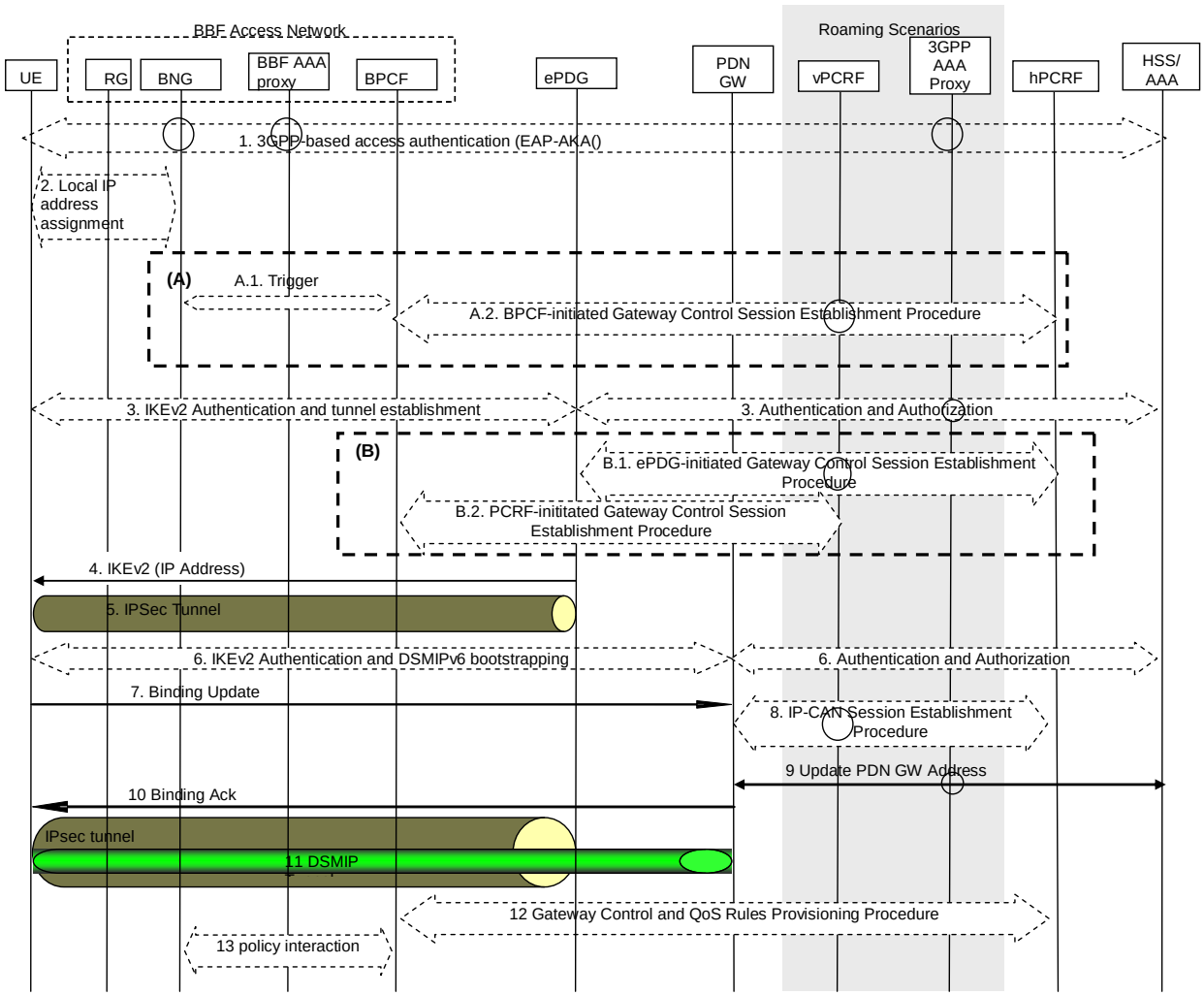


Figure 5.5.3.1-1: Initial attachment when S2c is used for roaming, non-roaming and LBO

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional steps 4 and 13 do not occur. Instead, the BBF Access Network may employ static configured policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

1. The UE may perform the 3GPP based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

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

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

A.2) If the BPCF receives the trigger in step 3 and policy interworking with PCRF is supported, the BPCF initiates S9a session establishment. The BPCF includes the UE identity, and IP-CAN type in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 1-3 is out of scope for 3GPP specifications.

3. The description of this step is the same as for steps 1 in TS 23.402 [3], clause 7.3.

B1) The ePDG initiates Gxb* session establishment by using Gateway Control Session establishment procedure with the PCRF. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC and the outer IP header information of the tunnelled traffic in the message to the PCRF (also including UDP source port number if NAT is detected).

For roaming case, the ePDG initiates Gateway Control Session establishment procedure with the vPCRF. The ePDG contains IMSI, APN, IP-CAN type, UE IP address allocated by EPC and outer IP header information of the tunnelled traffic in the request message. When the vPCRF receives a Gateway Control Session establishment request, the vPCRF shall initiate S9 session establishment/modification procedure. The vPCRF sends a S9 session establishment request to the hPCRF with the information received over Gxb* interface excluding tunnelled traffic related info (e.g. outer IP header info of the tunnelled traffic).

B.2) Triggered by the Gxb* session establishment, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF.

4-11. The description of these steps are the same as for steps 2-8 in TS 23.402 [3], clause 7.3.

12. The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF. with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected).

13. The BPCF may interact with the BNG, e.g. to download policies. This step is out of 3GPP scope.

5.5.3.2 UE-initiated Detach Procedure and UE-Requested PDN Disconnection with DSMIPv6 on S2c in untrusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.5.2.

The procedure in this clause applies to Detach Procedures, 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.

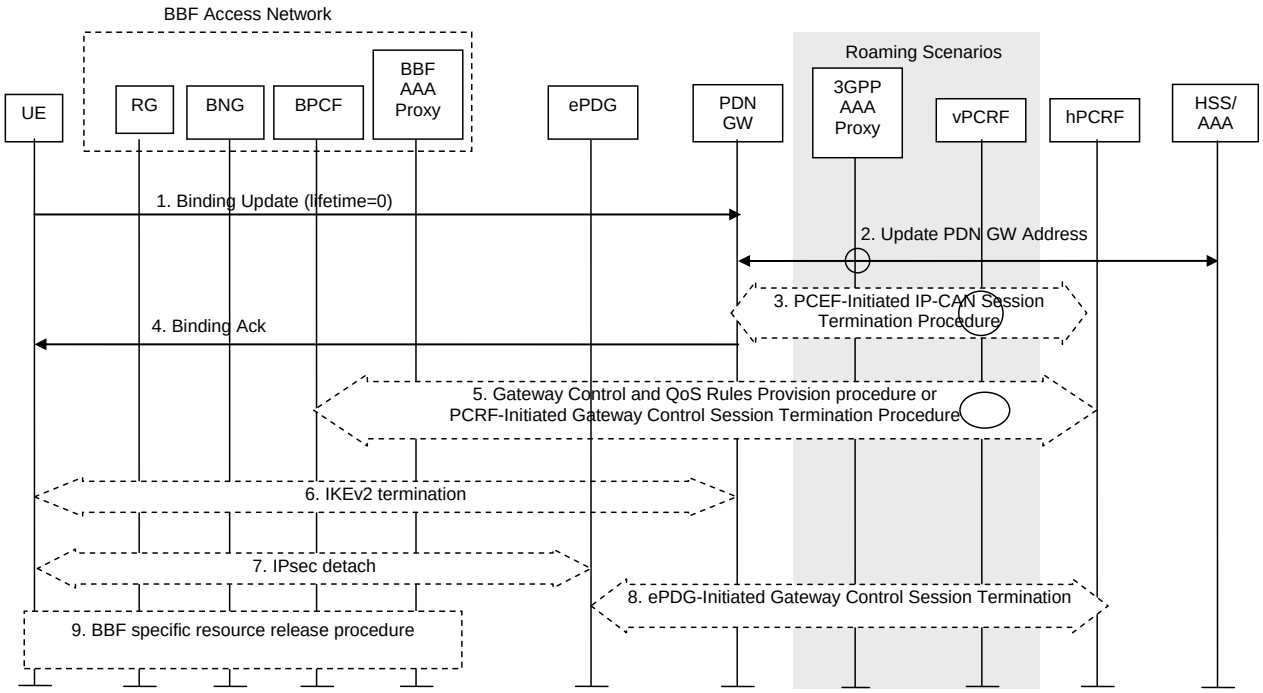


Figure 5.5.3.2-1: UE-initiated detach procedure with DSMIPv6 on S2c

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 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.

If dynamic policy provisioning over S9a is not deployed, the optional step 5 does not occur. Instead, the BBF access network may employ BBF local policies.

1-4) The description of these steps are the same as for steps 1-4 in TS 23.402 [3], clause 7.5.2.

5) Triggered by the IP-CAN session termination in step 3, 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.

6-7) The description of this step is the same as for step 5-6 in TS 23.402 [3], clause 7.5.2.

8) Triggered by the IKEv2 tunnel release, the ePDG executes the Gateway Control Session termination procedure with the PCRF. This step is only applicable in alternative B.

9) The description of this step is the same as for step 7 in TS 23.402 [3], clause 7.5.2.

5.5.3.3 HSS-initiated Detach Procedure with DSMIPv6 on S2c in untrusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.5.3.

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

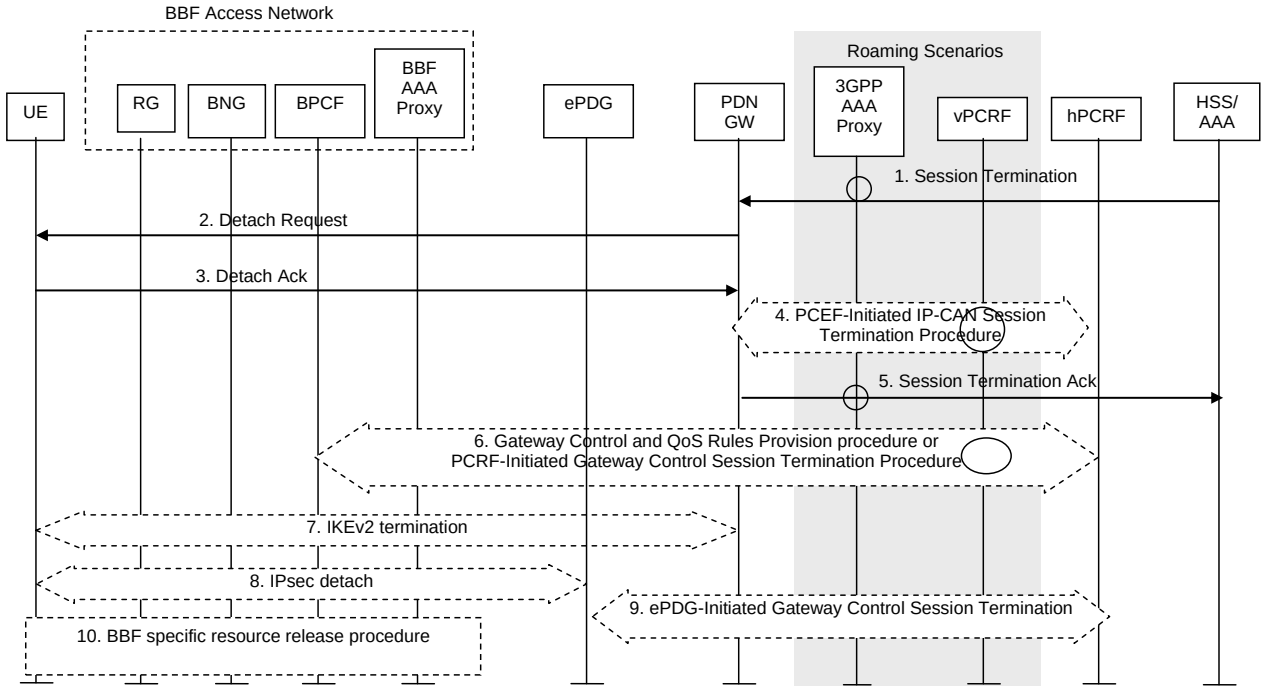


Figure 5.5.3.3-1: HSS-initiated detach procedure with DSMIPv6 on s2c

If dynamic policy provisioning over S9a is not deployed, the optional step 6 does not occur. Instead, the BBF access network may employ BBF local policies.

1-5) The description of these steps are the same as for steps 1-5 in TS 23.402 [3], clause 7.5.3.

6) Triggered by the IP-CAN session termination in step 4, 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.

7-8) The description of this step is the same as for step 6-7 in TS 23.402 [3], clause 7.5.3.

9) Triggered by the IKEv2 tunnel release, the ePDG executes the Gateway Control Session termination procedure with the PCRF. This step is only applicable in alternative B.

10) The description of this step is the same as for step 7 in TS 23.402 [3], clause 7.5.3.

5.5.3.4 PDN GW-initiated PDN disconnection Procedure with DSMIPv6 on S2c in untrusted BBF access

Editor's note: This procedure is based on TS 23.402 [3], clause 7.5.4.

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

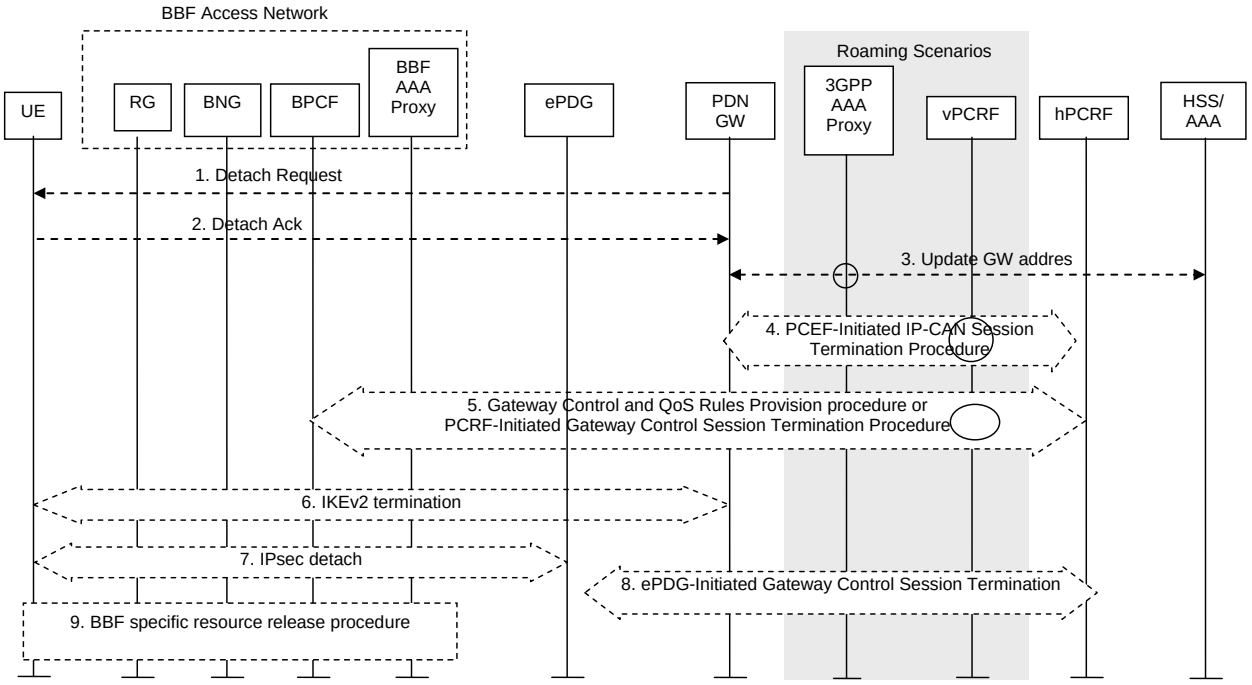


Figure 5.5.3.4-1: PDN GW-initiated PDN disconnection procedure with DSMIPv6 on s2c

If dynamic policy provisioning over S9a is not deployed, the optional step 5 does not occur. Instead, the BBF access network may employ BBF local policies.

1-4. The description of these steps are the same as for steps 1-4 in TS 23.402 [3], clause 7.5.4.

5. Triggered by the IP-CAN session termination in step 4, 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.

6-7. The description of this step is the same as for step 6-7 in TS 23.402 [3], clause 7.5.4.

8. Triggered by the IKEv2 tunnel release, the ePDG executes the Gateway Control Session termination procedure with the PCRF. This step is only applicable in alternative B.

9. The description of this step is the same as for step 7 in TS 23.402 [3], clause 7.5.4.

5.5.3.5 E-UTRAN to untrusted BBF access Handover with DSMIPv6 on S2c

Editor's note: This procedure is based on TS 23.402 [3], clause 8.4.3.

This clause shows a call flow for a handover when a UE moves from an E-UTRAN to an untrusted BBF access network.

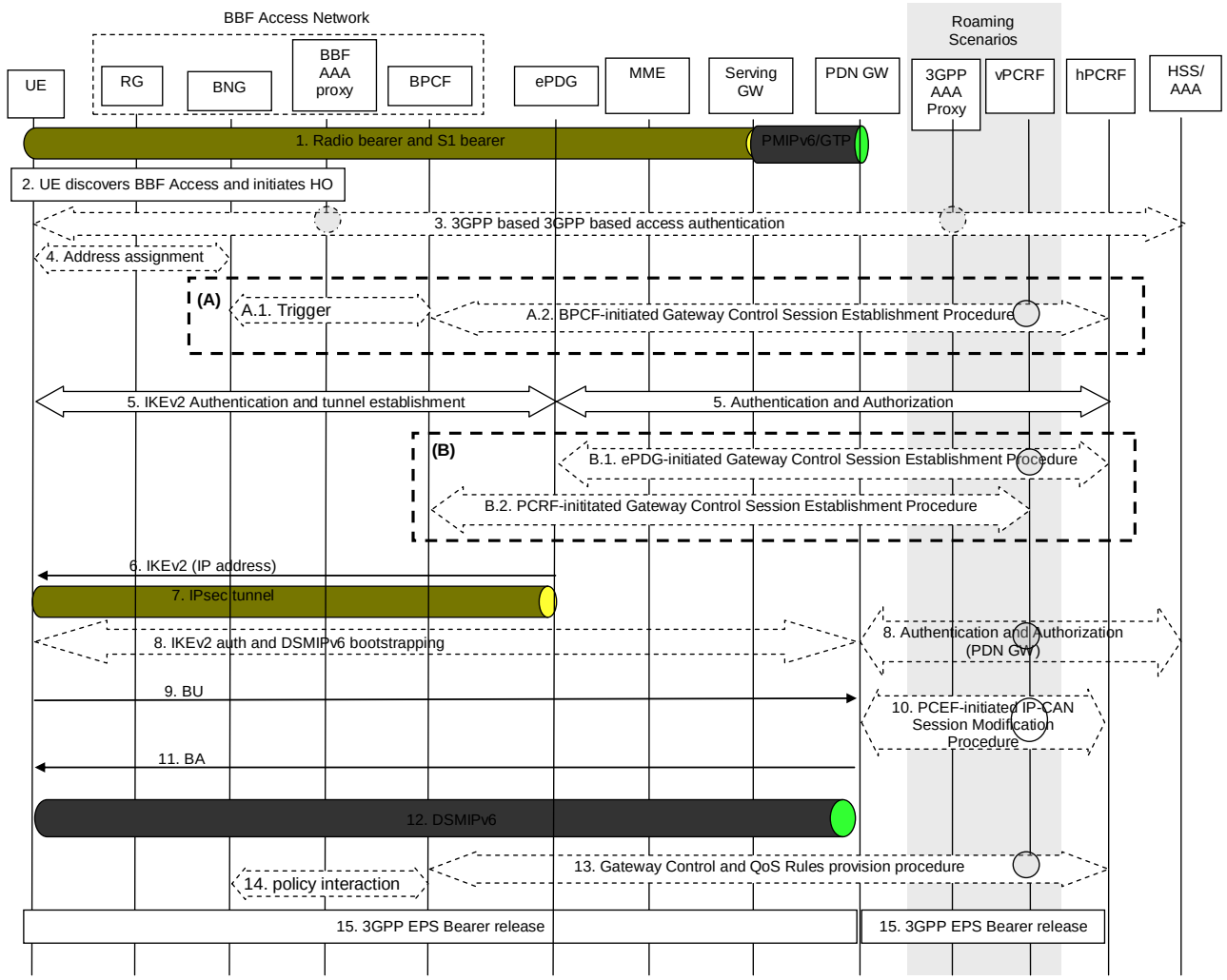


Figure 5.5.3.5-1: E-UTRAN to untrusted BBF Access Handover with DSMIPv6 on s2c

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

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise BBF access network may employ BBF local policies.

Depending on scenario, either the steps shown in (A) or the steps in (B) are preformed. Details for S9a session establishment and when (A) or (B) is used for S9a session establishment are described in clause 5.2.2.1.2.

For connectivity to multiple PDN the following applies:

- If the UE is connected to both 3GPP access and BBF access before the handover of PDN connections to untrusted BBF access is triggered, steps 2 to 5 shall be skipped. However whether step A.1 is executed is out of the scope of 3GPP and it is BBF specific.

- If the UE is connected only to 3GPP access before the handover of PDN connections to untrusted BBF access is triggered, steps 2 to 4 shall be performed. However whether step A.1 is executed is out of the scope of 3GPP and it is BBF specific.

- Steps 8 to 14 shall be repeated for each PDN connection that is being transferred from 3GPP access. If not performed in 3GPP access prior to the handover, Step 6 shall also be repeated for each PDN connection that is being transferred from 3GPP access. The step B.1 shall be executed only if the S9a Gateway Control Session is not already established, i.e. if step A.2 has not been performed or only when the first PDN connection is established or transferred to BBF access.

1-2. The description of these steps are the same as for steps 1-2 in TS 23.402 [3], clause 8.4.3.

3. The UE may perform the 3GPP-based (EAP) access authentication procedure involving the BBF access network. As part of this step, the permanent user identity (IMSI) is provided from the 3GPP AAA Server to the BBF access network.

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

A.1) Triggered by steps 3 and 4, the BPCF is informed about the UE accessing over BBF Access. How this is done is out of 3GPP scope.

A.2) If the BPCF receives the trigger in step A.1 and policy interworking with fixed accesses is supported, the BPCF initiates S9a session establishment. The BPCF includes the UE Identity, UE IP address and IP-CAN type in the message to the PCRF. The details of how the BPCF is notified about the UE connecting in steps 3-A.1 is out of scope for 3GPP specifications.

5. The description of this step is the same as for steps 3 in TS 23.402 [3], clause 8.4.3.

B.1) The ePDG initiates Gxb* session establishment by using Gateway Control Session establishment procedure with the PCRF. The ePDG includes the IMSI, APN, IP-CAN type, UE IP address allocated by EPC and the outer IP header information of the tunnelled traffic in the message to the PCRF (also including UDP source port number if NAT is detected).

For roaming case, the ePDG initiates Gateway Control Session establishment procedure with the vPCRF. The ePDG contains IMSI, APN, IP-CAN type, UE IP address allocated by EPC and outer IP header information of the tunnelled traffic in the request message. When the vPCRF receives a Gateway Control Session establishment request, the vPCRF shall initiate S9 session establishment/modification procedure. The vPCRF sends a S9 session establishment request to the hPCRF with the information received over Gxb* interface excluding tunnelled traffic related info (e.g. outer IP header info of the tunnelled traffic).

B.2) Triggered by the Gxb* session establishment, the PCRF (non-roaming case) or the vPCRF (roaming case) initiates Gateway Control Session establishment with the BPCF to establish S9a Session. The IMSI, IP-CAN type, and outer IP header information for tunnel traffic needs to be included in the request message which sending to the BPCF.

6-12. The description of these steps are the same as for steps 4-10 in TS 23.402 [3], clause 8.4.3.

13. The Gateway Control and QoS Rules provision procedure may be initiated by the PCRF towards the BPCF. with the following additions: The local UE IP address and optionally UDP source port number (if NAT is detected). Depending on the reply from the BPCF, the PCRF may update the PCC rules in the PCEF.

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

15. The description of this step is the same as for step 11 in TS 23.402 [3], clause 8.4.3.

5.5.3.6 Network-Initiated Dynamic PCC for S2c when accessing untrusted BBF access

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

If dynamic PCC is deployed, the procedure given in figure 5.5.2 is used by the PCRF to provision rules to the BBF IP access and for the BBF IP 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 3GPP EPC The access specific procedure executed in the BBF access is not within the scope of this specification.

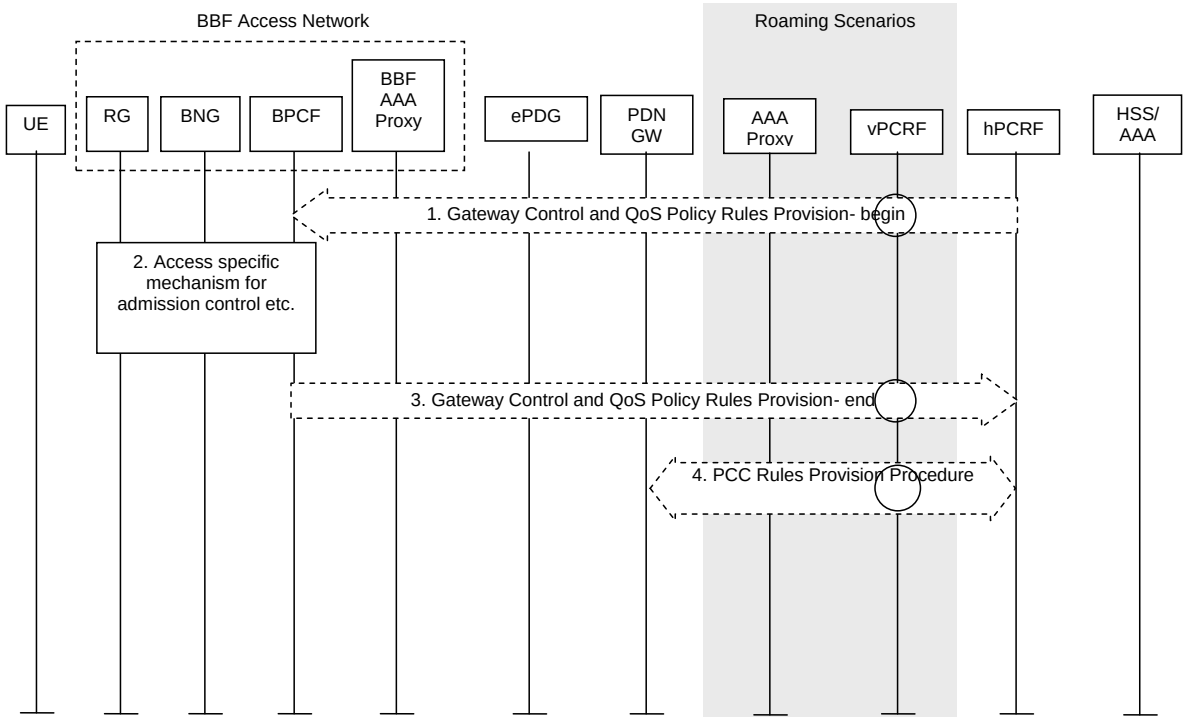


Figure 5.5.3.6-1: Network-initiated dynamic policy control procedure in un-trusted BBF IP Access for DSMIPv6 on S2c

This procedure concerns both the non-roaming (as figure 5.1.2-2) and roaming case (as figure 5.1.2-5). 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 5.1.2-8), 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 only occur if dynamic policy provisioning is deployed. Otherwise BBF access network may employ BBF local policies.

1. The PCRF initiates the Gateway Control and QoS Policy Rules Provision Procedure specified in TS 23.203 [4] by sending a message with the QoS rules to the BPCF.

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

3. The BPCF responds to the PCRF indicating the result of the request received in Step 1 and thus completing the GW Control and QoS Rules Provision procedure started in step 1.

4. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [4]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of a PCC Rules Provision procedure specified in TS 23.203 [4].

NOTE: Step 4 may occur before step 1 or performed in parallel with steps 1-3 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [4].

5.5.3.7 UE-Initiated Connectivity to Additional PDN with DSMIPv6 on S2c over untrusted BBF 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.

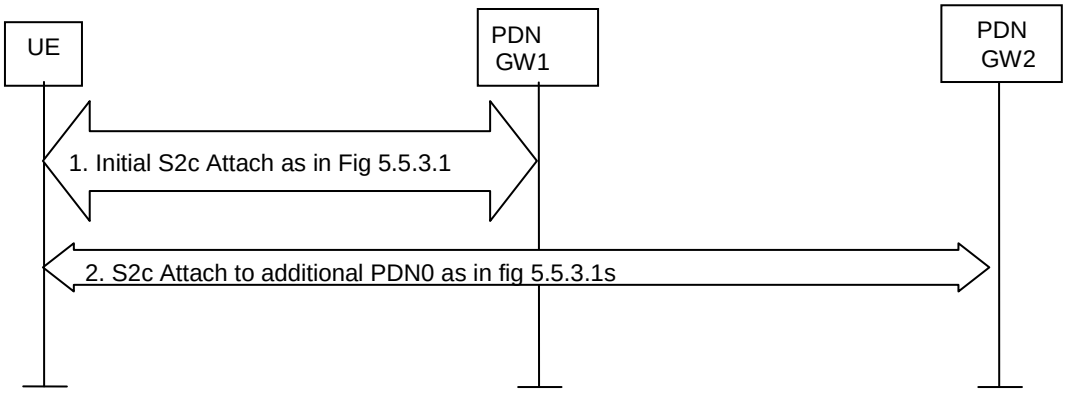


Figure 5.5.3.7-1: UE-Initiated connectivity to additional PDN from untrusted Non-3GPP IP Access with DSMIPv6 on S2c

1) The UE has performed the Initial S2c attach procedure as defined in clause 5.5.3.1 and has an established PDN connection.

2) The UE repeats the procedure steps 6-12 of clause 5.5.3.1, figure 5.5.3.1-1 (BPCF-initiated S9a session establishment) or steps 7-12 in (BPCF-initiated S9a session establishment) or figure 5.5.3.1-1 of clause 5.5.3.1-1 (PCRF-initiated S9a session establishment) 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 3, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.

5.6 H(e)NB interworking architecture alternative 1

5.6.1 Procedures

Editor's note: The message names and protocol specific are not finalised.

NOTE: In the procedure in the following if HeNB GW is not deployed, the communication is between on H(e)NB Policy Function and MME.

5.6.1.1 H(e)NB power on

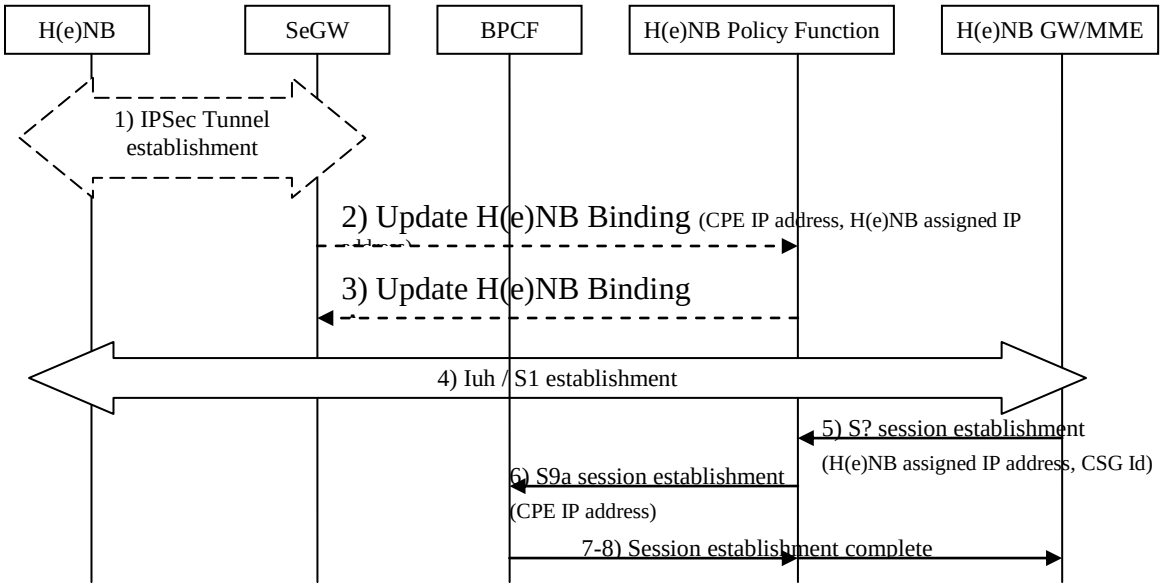


Figure 5.6.1.1-1: Update H(e)NB Binding on H(e)NB power on

1. If configured, H(e)NB establishes an IPSec connection towards the SeGW.
2. The SeGW, if present, informs the H(e)NB policy function of the binding between the CPE IP address CPE (outer IP address) and the IP address assigned to the H(e)NB (inner IP address).
3. The H(e)NB Policy Function accepts the updated information.
4. The H(e)NB establishes the S1 or Iuh connection to the H(e)NB GW or MME as per normal procedures.
5. The H(e)NB GW / MME establishes an S? session to the H(e)NB policy function including information about the H(e)NB such as CSG ID, IP address assigned to the H(e)NB.
6. The H(e)NB policy function identifies the IP address associated with the fixed access over which the H(e)NB is communicating based on information received during step 2. The H(e)NB policy function establishes an S9a session towards the BPCF using the IP address of the fixed access. Policies applied may, for example, be associated with control plane signalling or management traffic for the H(e)NB.
7. The BPCF responds to the request.
8. The H(e)NB policy function responds to the H(e)NB GW / MME.

NOTE 1: If the CPE is acting as a bridge device, BBF procedures may be applied for IP-CAN session establishment for the H(e)NB when it is first connected to the CPE. Once IPSec establishment is complete, the BPCF binds this to the subsequent request from the H(e)NB policy function.

NOTE 2: H(e)NB Policy Function admission control functionality need not be applied in this procedure.

5.6.1.2 UE initial attach and Idle-to-Active transition whilst on H(e)NB

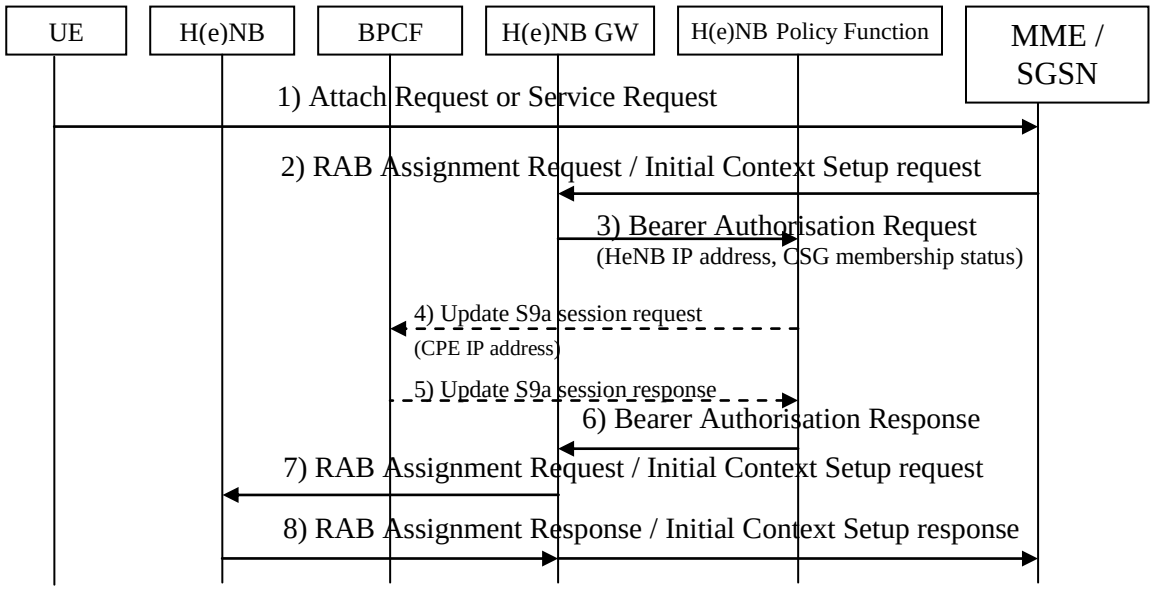


Figure 5.6.1.2-1: UE initial attach to a H(e)NB

NOTE: This flow does not include all the steps associated with Attach Procedure or UE triggered Service Request from TS 23.401 [2] and TS 23.060 [22].

1. The UE performs either an initial attach or Service Request for idle-to-active transition.
2. The MME / SGSN sends a RAB Assignment Request or Initial Context Setup Request message towards the H(e)NB.
3. On reception of the RAB Assignment Request or Initial Context Setup Request message at the H(e)NB GW, the H(e)NB GW requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the H(e)NB and the CSG membership status of the UE.
4. The H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at H(e)NB power on.
5. The BPCF acknowledges the changes to the session.
6. The H(e)NB policy function responds with the outcome of the authorisation request.
7. Based on the authorisation decision, the H(e)NB GW continues or rejects the RAB assignment / Initial Context setup.

8). The remainder of the attach / service request procedure completes.

5.6.1.3 Idle mode mobility onto H(e)NB

No specific procedures in this scenario. Resource authorisation only needs to be performed when a bearer is to be established.

5.6.1.4 Bearer Activation / Modification / Deactivation

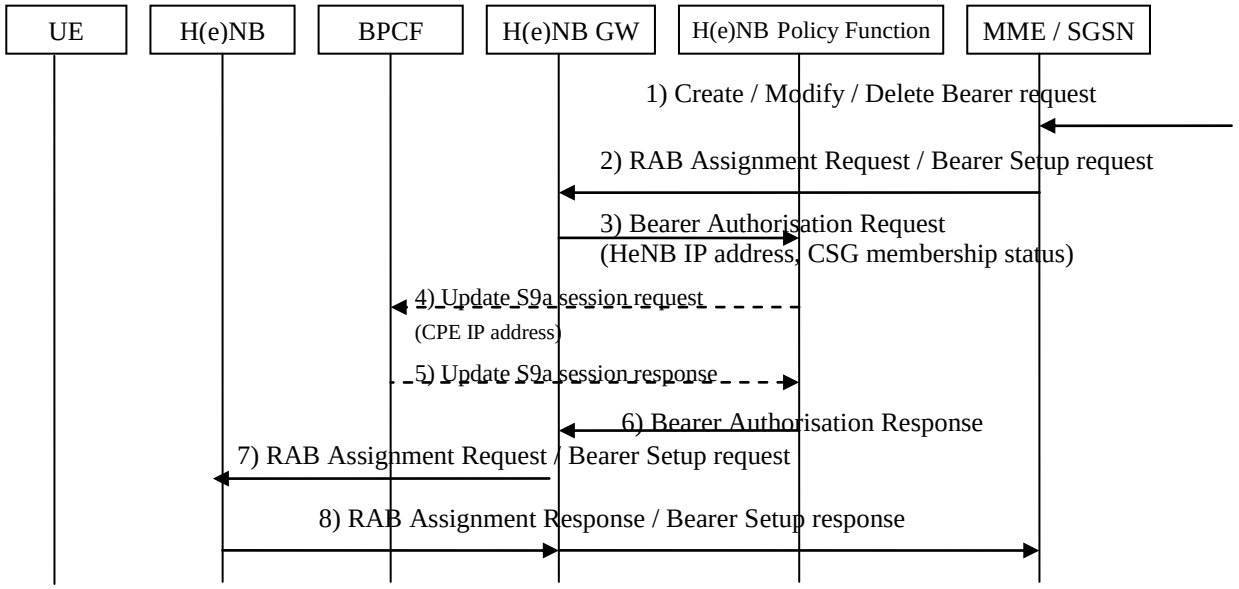


Figure 5.6.1.4-1: Bearer establishment / modification / deactivation on a H(e)NB

NOTE 1: This flow does not include all the steps associated with Bearer establishment / modification / deactivation procedures from TS 23.401 [2] and TS 23.060 [22].

1. The MME / SGSN receives a Create / Modify / Delete Bearer Request message from EPC.
2. The MME / SGSN sends a RAB Assignment Request or Bearer Setup Request message towards the H(e)NB.
3. On reception of the RAB Assignment Request or Bearer Setup Request message at the H(e)NB GW, the H(e)NB GW requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the H(e)NB and the CSG membership status of the UE.
4. The H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at H(e)NB power on.
5. The BPCF acknowledges the changes to the session.
6. The H(e)NB policy function responds with the outcome of the authorisation request.
7. Based on the authorisation decision, the H(e)NB GW continues or rejects the RAB assignment / Bearer setup.

NOTE 2: For deactivation procedures, the H(e)NB GW can continue with the deactivation even when a rejection comes back from the H(e)NB Policy Function.

8. The remainder of the bearer establishment / modification / deactivation procedure completes.

5.6.1.5 Inter H(e)NB mobility

5.6.1.5.1 To different H(e)NB GW

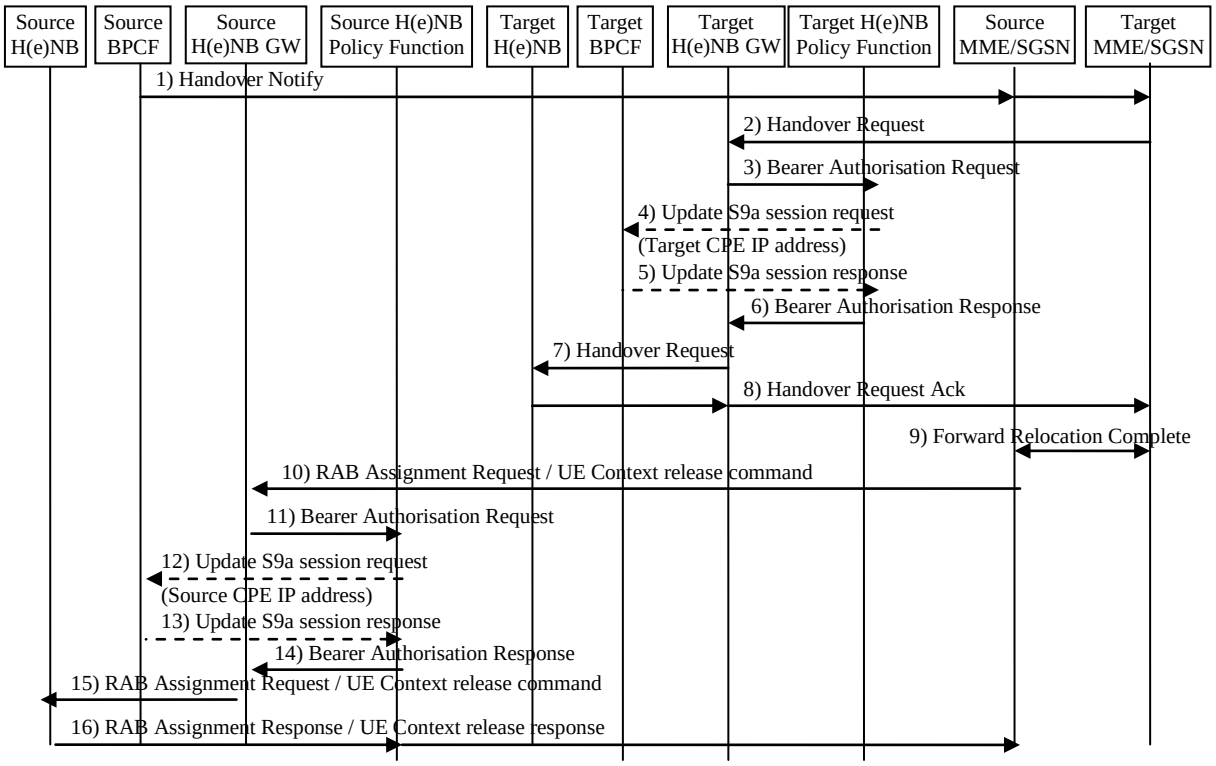


Figure 5.6.1.5.1-1: Mobility from H(e)NB to another H(e)NB associated with another H(e)NB GW

NOTE 1: This flow does not include all the steps associated with S1-based handover / SRNS relocation procedure from TS 23.401 [2].

1. The source H(e)NB sends a Handover Notify towards the target MME / SGSN via the source MME/SGSN.
2. Handover procedures continue according to TS 23.401 [2] / TS 23.060 [22]. The target MME / SGSN sends a Handover Request to the target H(e)NB.
3. On reception of the Handover Request message at the target H(e)NB GW, the target H(e)NB GW requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the target H(e)NB and the CSG membership status of the UE.
4. The target H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at target H(e)NB power on.
5. The BPCF acknowledges the changes to the session.
6. Based on the authorisation decision, the H(e)NB GW continues, modifies or rejects the Handover request. The modification is limited to removing bearers that were not authorised.
7. The H(e)NB policy function responds with the outcome of the authorisation request.
8. The target H(e)NB acknowledges the Handover Request.
9. Handover procedures proceed as per TS 23.401 [2] / TS 23.060 [22]. The source MME / SGSN receives Forward Relocation Complete message.
10. The source MME deletes the UE context in the H(e)NB by sending a UE Context Release request towards the H(e)NB.

11. On reception of the RAB Assignment Request or UE Context Release Request message at the H(e)NB GW, the H(e)NB GW requests authorisation for the bearer(s) that are being released.

12. The H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at source H(e)NB power on.

13. The BPCF acknowledges the changes to the session.

14. The H(e)NB policy function responds with the outcome of the authorisation request.

15. The H(e)NB GW continues with the RAB assignment / UE Context release.

NOTE 2: The H(e)NB GW need not wait for the response from the H(e)NB Policy function before completing the RAB assignment / UE context release to the H(e)NB.

16. The remainder of the Handover procedure completes.

5.6.1.6 Mobility to macro network

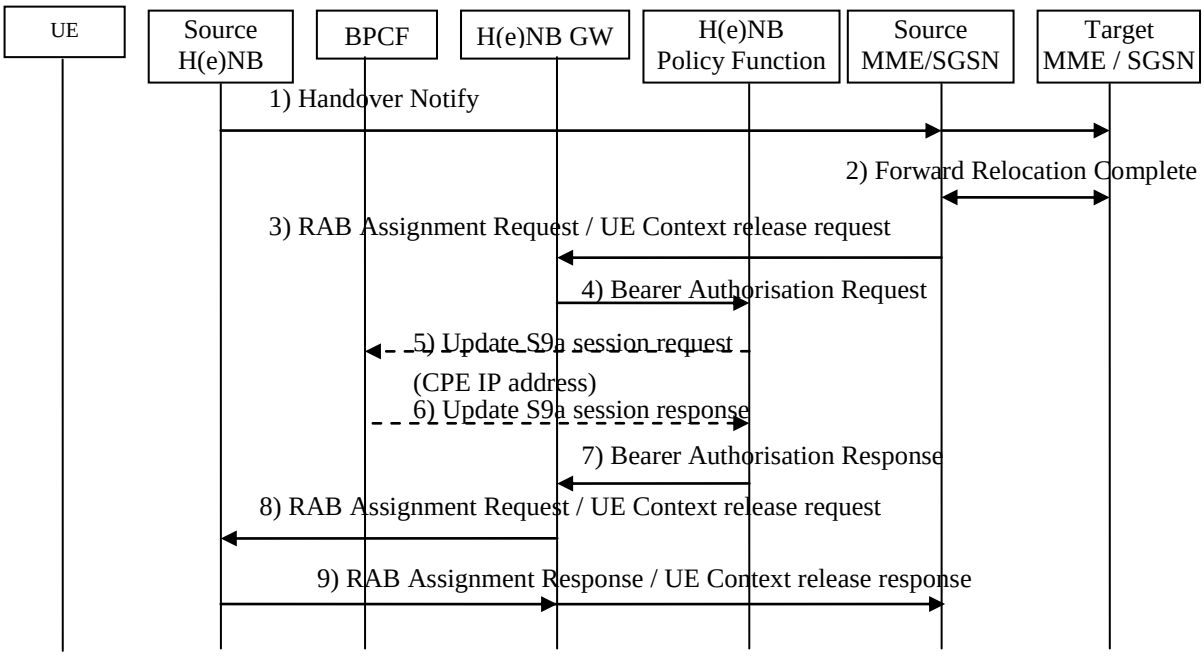


Figure 5.6.1.6-1: Mobility from H(e)NB to macro (example with CN node relocation)

NOTE 1: This flow does not include all the steps associated with S1-based Handover / SRNS Relocation procedure from TS 23.401 [2].

1. The source H(e)NB sends a Handover Notify towards the target MME / SGSN via the source MME/SGSN.

2. Handover procedures continue according to TS 23.401 [2]. The source MME / SGSN receives Forward Relocation Complete message.

3. The source MME deletes the UE context in the H(e)NB by sending a UE Context Release request towards the H(e)NB.

4. On reception of the RAB Assignment Request or UE Context Release Request message at the H(e)NB GW, the H(e)NB GW requests authorisation for the bearer(s) that are being released.

5. The H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at H(e)NB power on.

6. The BPCF acknowledges the changes to the session.

7. The H(e)NB policy function responds with the outcome of the authorisation request.

8. The H(e)NB GW continues with the RAB assignment / UE Context release.

NOTE 2: The H(e)NB GW need not wait for the response from the H(e)NB Policy function before completing the RAB assignment / UE context release to the H(e)NB.

9. The remainder of the Handover procedure completes.

5.6.1.7 UE Attach without HeNB GW

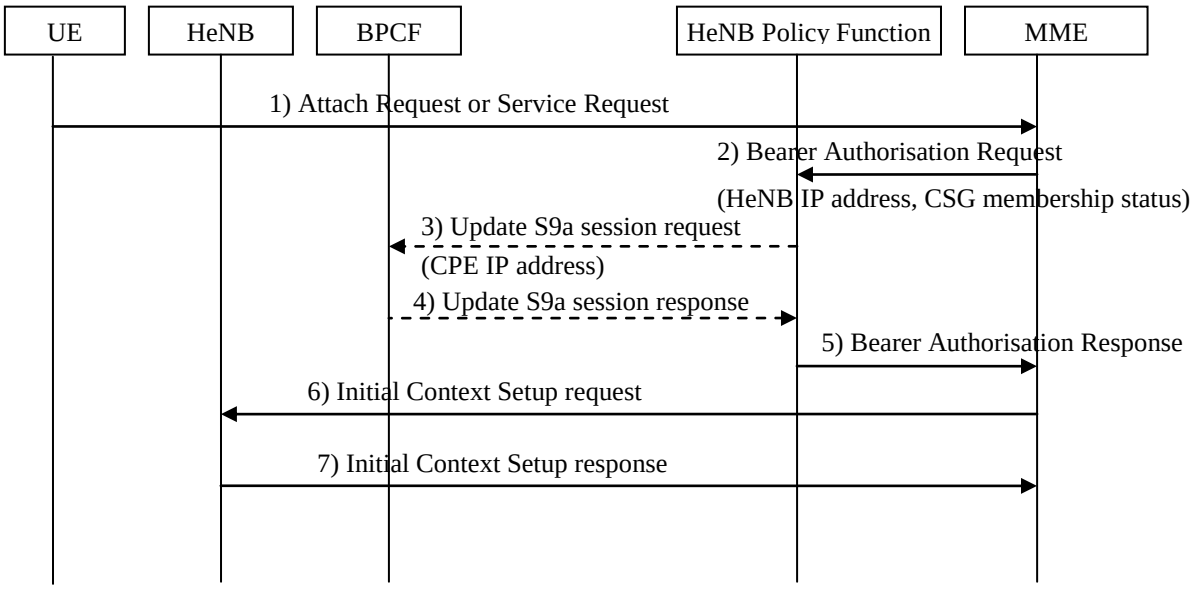


Figure 5.6.1.7-1: UE initial attach to a HeNB without HeNB GW

NOTE: This flow does not include all the steps associated with Attach Procedure or UE triggered Service Request from TS 23.401 [2].

1. The UE performs either an initial attach or Service Request for idle-to-active transition.

2. In parallel to step 2, the MME requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the HeNB and the CSG membership status of the UE.

3. The HeNB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at HeNB power on.

4. The BPCF acknowledges the changes to the session.

5. The HeNB policy function responds with the outcome of the authorisation request.

6. Based on the bearer authorisation response from the HeNB Policy Function, the MME forwards the Initial Context Setup Request message towards the HeNB.

7. The remainder of the attach / service request procedure completes. This occurs independently of steps 2-5.

5.6.1.8 CS call establishment

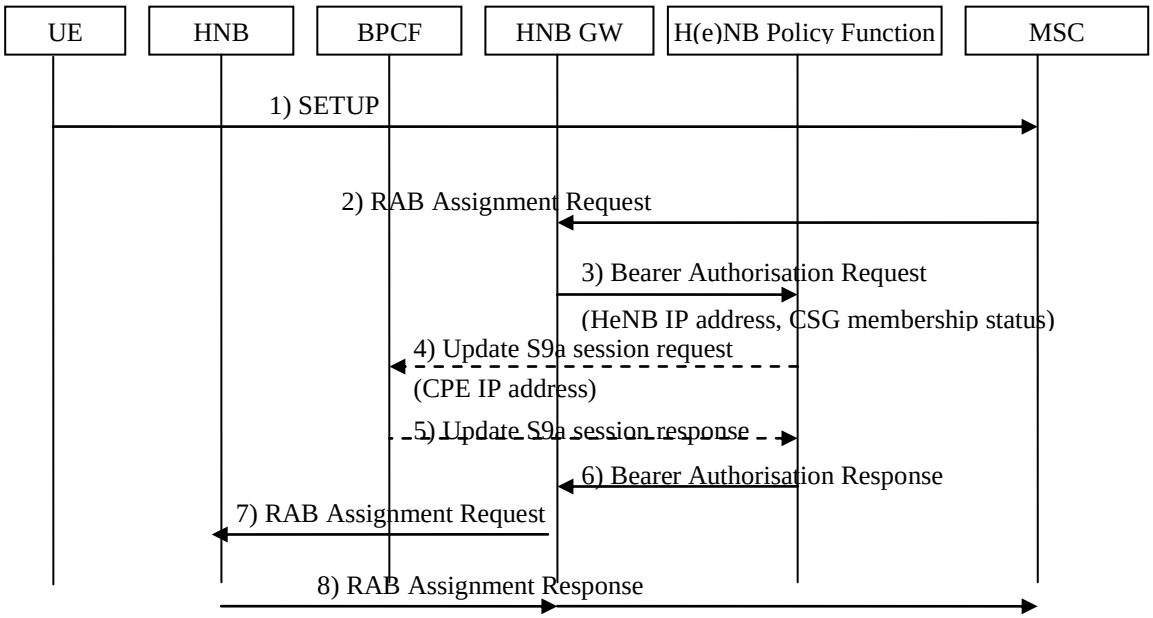


Figure 5.6.1.8-1: CS call establishment

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

1. The UE initiates call setup using a SETUP message.
2. The MSC sends a RAB Assignment Request message towards the HNB.
3. In parallel to step 2, the HNB GW requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the HNB and the CSG membership status of the UE.
4. The HNB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at HNB power on.
5. The BPCF acknowledges the changes to the session.
6. The HNB policy function responds with the outcome of the authorisation request.
7. Based on the authorisation decision, the H(e)NB GW continues or rejects the RAB assignment / Initial Context setup.
8. The remainder of the call setup procedure completes.

5.6.1.9 UE detach and Active-to-Idle transition whilst on H(e)NB

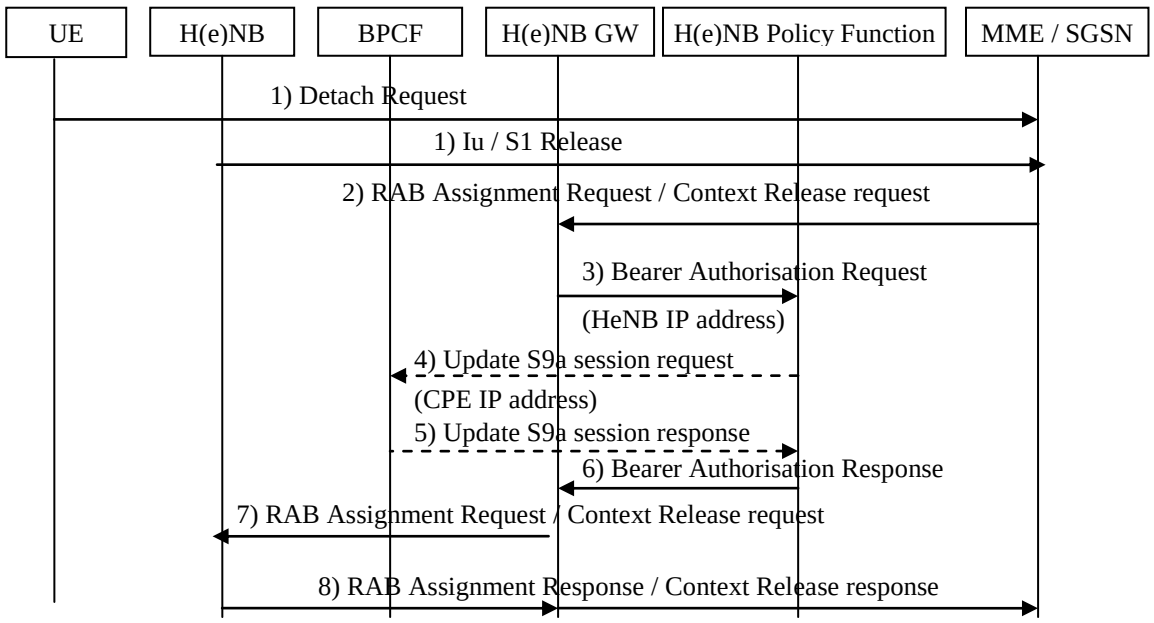


Figure 5.6.1.9-1: UE detach or Active-to-Idle transition on a H(e)NB

NOTE 1: This flow does not include all the steps associated with Detach Procedure or Iu/S1 Release from TS 23.401 [2] and TS 23.060 [22].

1. The UE performs either a detach or the HNB performs initiates an Iu release for active-to-idle transition.
2. The MME / SGSN sends a RAB Assignment Request or Initial Context Setup Request message towards the H(e)NB.
3. On reception of the RAB Assignment Request or Context Release Request message at the H(e)NB GW, the H(e)NB GW requests authorisation for the bearer(s) that form part of the original request including the IP address assigned to the H(e)NB.
4. The H(e)NB policy function decides what action to take and may update the S9a session as a result of the decision. This reuses the S9a session established at H(e)NB power on.
5. The BPCF acknowledges the changes to the session.
6. The H(e)NB policy function responds with the outcome of the authorisation request.
7. The H(e)NB GW continues with the RAB assignment / UE Context release.

NOTE 2: The H(e)NB GW need not wait for the response from the H(e)NB GW before continuing the release procedures.

8. The remainder of the detach / release procedure completes.

5.6.1.10 H(e)NB policy function initiated bearer Deactivation

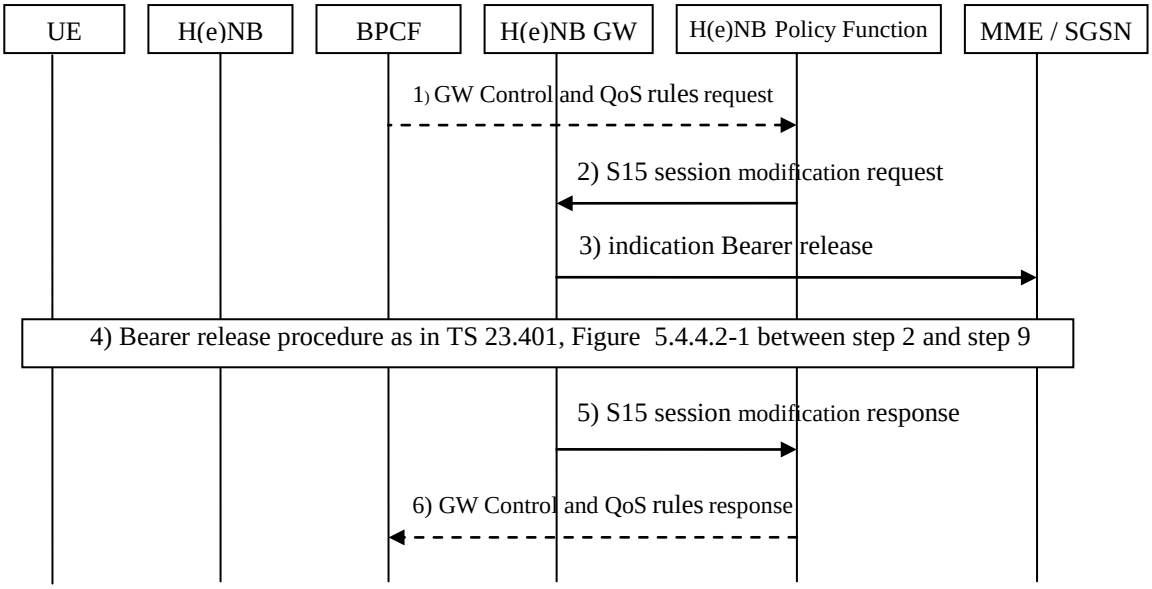


Figure 5.6.1.10-1: H(e)NB policy function initiated bearer Deactivation

This procedure is performed when the H(e)NB policy function initiated a bearer deactivation based on triggered by a request to decrease or release authorized resource for the H(e)NB or local decision. In case of the request to reduce the authorized resource the H(e)NB policy function may decide to trigger bearer deactivation due to limited resources.

1. The BPCF send a S9a GW Control and QoS rules request to H(e)NB policy function to modify the authorized resource for H(e)NB due to local reasons (e.g. due to pre-emption in BBF network).

2. The H(e)NB policy function decides to trigger bearer deactivation due to resource limitation and send S15 session modification request to H(e)NB GW. This request indicates which bearer shall be released.

3. The H(e)NB GW send an indication of bearer release to the MME. This indication is same to the step 1 in TS 23.401 [2], Figure 5.4.4.2-1.

4. Then MME initiated dedicated bearer deactivation procedure, the step 2 to step 9 in TS 23.401 [2], Figure 5.4.4.2-1, is invoked.

5. The H(e)NB GW acknowledges the request.

6. The H(e)NB policy function acknowledges the request.

NOTE 1: H(e)NB policy function may make local decision to trigger bearer deactivation procedure. In this case, step 1 and step 6 are optional.

NOTE 2: The events that trigger BPCF initiated S9a session modification procedure are out of 3GPP scope.

5.7 H(e)NB interworking architecture alternative 2

5.7.1 General

5.7.2 TS 23.401 procedures

5.7.2.1 E-UTRAN Initial Attach

NOTE: Enhancements to the Initial Attach procedure rest on the assumption that the HeNB sends the tunnel information and the FQDN of the BPCF to the MME in UE associated S1 signalling (refer to the definition of Initial UE Message message in TS 36.413)

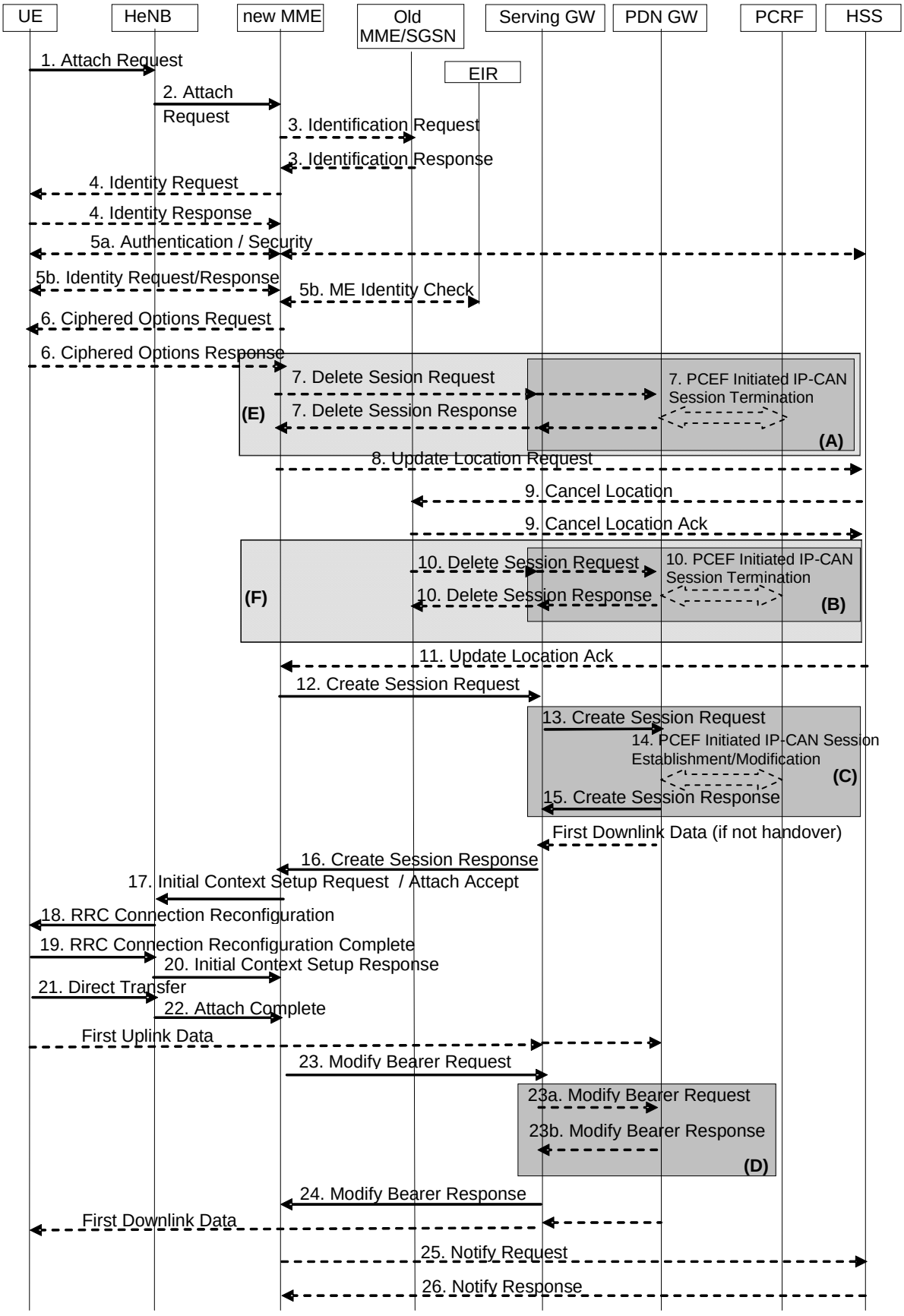


Figure 5.7.2.1-1: Attach procedure

This procedure is the same as described in TS 23.401 [2], clause 5.3.2.1, with modifications to the following steps:

2. The HeNB includes in the Initial UE Message message the outer IP address of the IPSec tunnel, referred to as "Tunnel- Info", and the FQDN of the BPCF in the BBF access network.

12. This step is the same as step 12 in TS 23.401 [2], with the addition that the MME also includes HeNB Tunnel-Info and FQDN of BPCF in the Create Session Request sent to the Serving GW.

14. This step is the same as step 14 in TS 23.401 [2], with the addition that the PDN GW also includes HeNB Tunnel-Info and FQDN of BPCF (when the HeNB connects to the BBF access network) is provided from the PDN GW to the PCRF if received in previous messages.

5.7.2.2 UE requested PDN connectivity

NOTE: Enhancements to the UE requested PDN connectivity procedure rest on the assumption that the HeNB sends the tunnel information and the FQDN of the BPCF to the MME in UE-associated S1 signalling (refer to the definition of Uplink NAS Transport message in TS 36.413).

The UE requested PDN connectivity procedure for an E-UTRAN is depicted in figure 5.10.2-1. The procedure allows the UE to request for connectivity to a PDN including allocation of a default bearer. The PDN connectivity procedure may trigger one or multiple Dedicated Bearer Establishment procedures to establish dedicated EPS bearer(s) for that UE.

An emergency attached UE shall not initiate any PDN Connectivity Request procedure. A normal attached UE shall request a PDN connection for emergency services when Emergency Service is required and an emergency PDN connection is not already active.

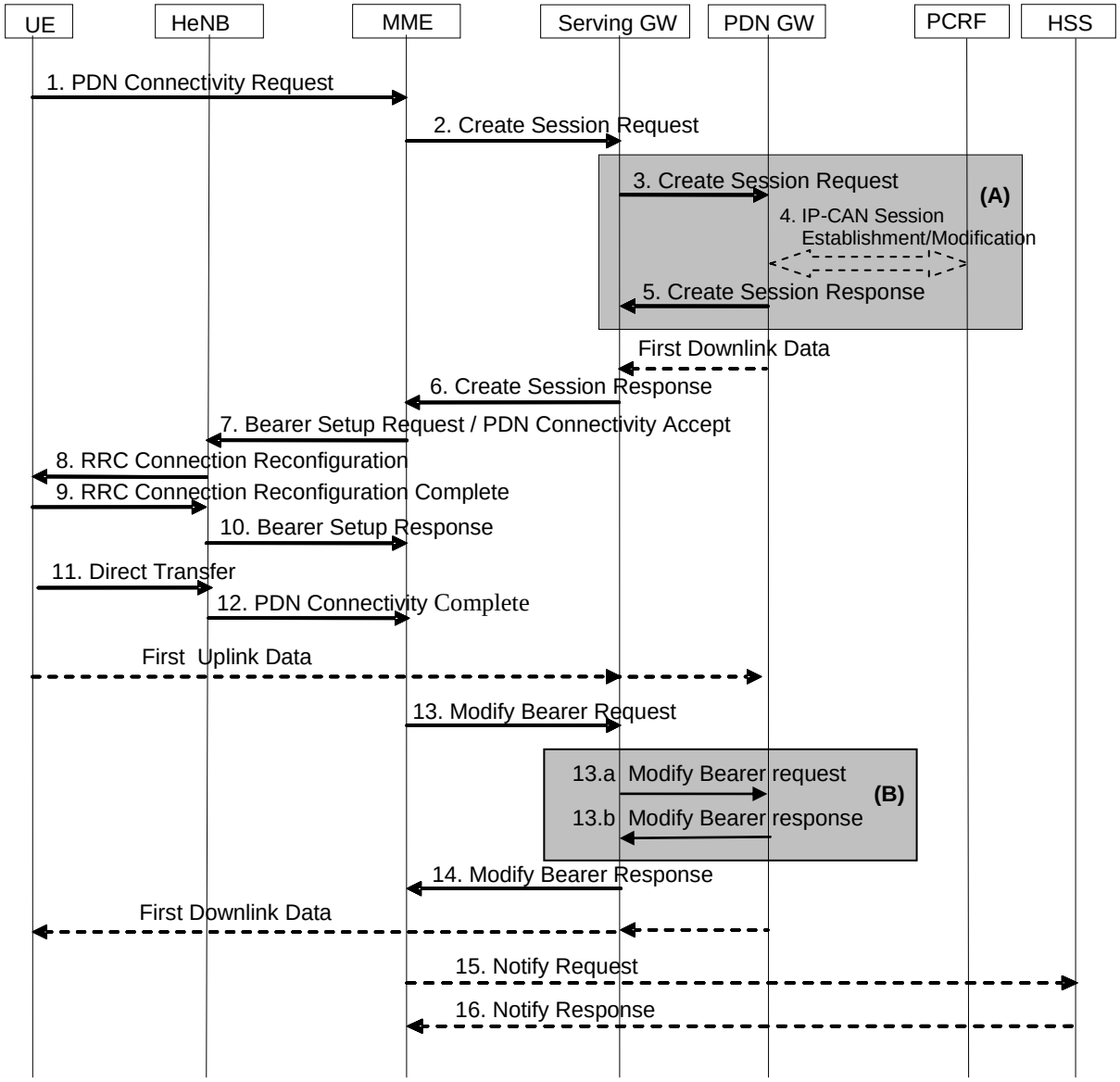


Figure 5.7.2.2-1: UE requested PDN connectivity

This procedure is the same as described in TS 23.401 [2], clause 5.10.2, with modifications to the following steps:

1. The HeNB includes in the Uplink NAS Transport message the outer IP address of the IPSec tunnel, referred to as "Tunnel- Info", and the FQDN of the BPCF in the BBF access network.

2. This step is the same as step 2 in TS 23.401 [2], with the addition that the MME also includes HeNB Tunnel-Info and FQDN of BPCF in the Create Session Request sent to the Serving GW.

4. This step is the same as step 4 in TS 23.401 [2], with the addition that the PDN GW also includes HeNB Tunnel-Info and FQDN of BPCF is provided from the PDN GW to the PCRF if received in previous messages.

5.7.3 TS 23.402 Procedures

5.7.3.1 Initial E-UTRAN Attach with PMIP-based S5 or S8

This clause is related to the case when the UE powers-on in the LTE network with PMIP-based S5 or S8 interface and includes the case of roamers from a GTP network into a PMIPv6 network when PMIP-based S5 is used to connect the Serving GW and the PDN GW of the visited PLMN. Proxy Mobile IP version 6 is used on S5 or S8 interface. It is assumed that the MAG is collocated with the Serving GW for the PMIPv6 procedure between the Serving GW and the PDN GW.

When only GTP-based S5 or S8 connections are established for roamers from a GTP network into a PMIPv6 network the procedure as described in TS 23.401 [2] applies.

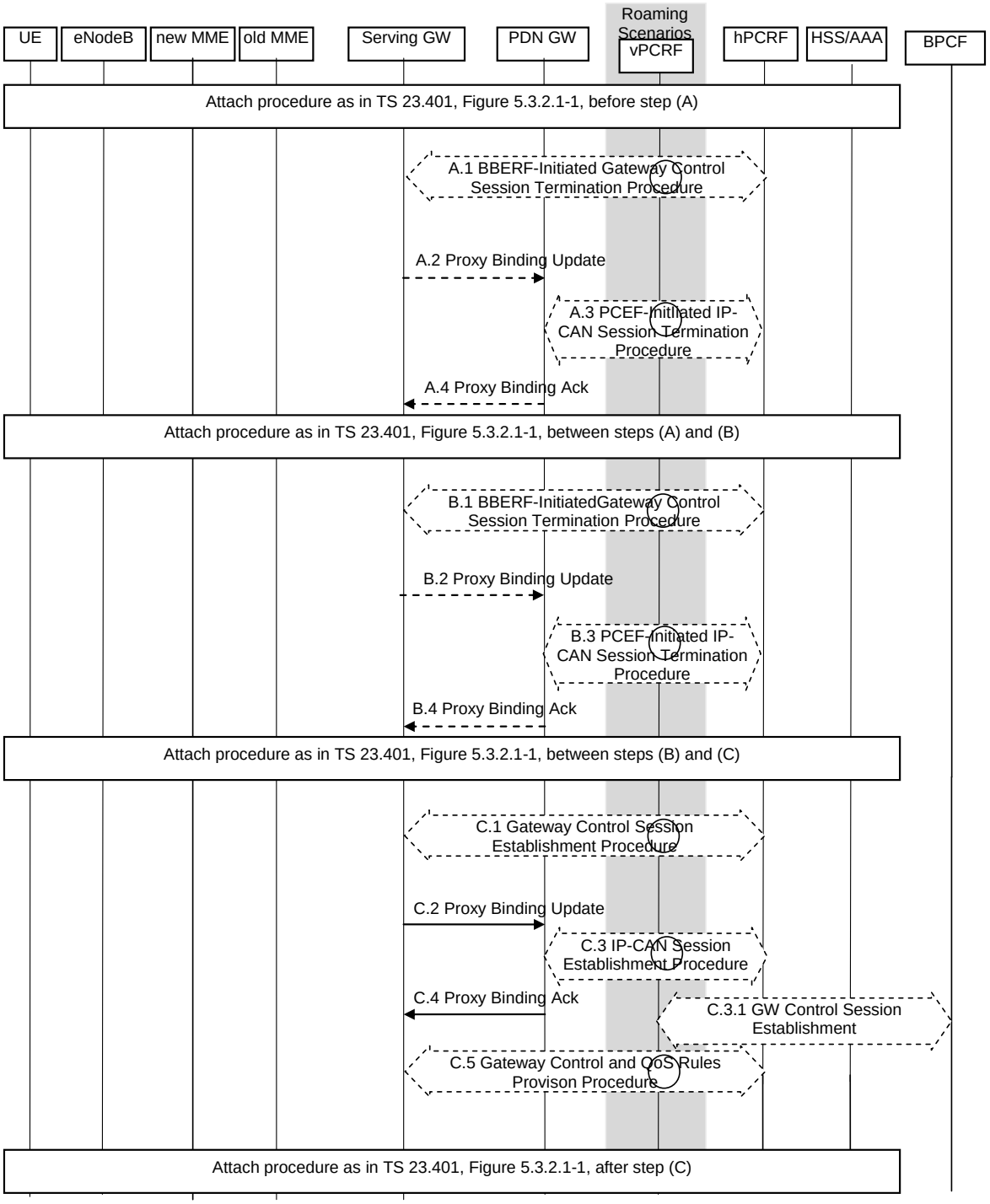


Figure 5.7.3.1-1 (TS 23.402 [3] 5.2-1): Initial E-UTRAN attach with PMIP-based S5 or S8

The signalling sequence relies on the MME to send the IPSec Tunnel Information using the Create Session Request message per attach procedure of TS 23.401 [2], clause 5.3.2.1, figure 5.3.2.1-1.

Editor's note: It is FFS how the MME obtains the IP@ of the IPSec tunnel.

C.1) The Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF that includes the HeNB Tunnel-Info and FQDN of BPCF (when the HeNB connects to the BBF access network).

C.2) The Serving GW sends a Proxy Binding.

C.3) The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF.

C.3.1) The PCRF initiates the GW Session Establishment Procedure with the BPCF that includes the HeNB Tunnel Info, QoS Rule with the QoS information (QCI, GBR, MBR and ARP).

Editor's note: It is FFS how the PCRF discovers the BPCF.

C.4) The PDN GW responds with a PMIPv6 Binding Acknowledgement.

C.5) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure.

After steps C.1-C.5 the procedure continues as it is defined in clause 5.3.2 in TS 23.401 [2] with the exception that the steps in block D are not performed.

5.7.3.2 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).

In case of detach, all the bearers at the Serving GW are terminated. Further, the IP-CAN session for the UE in the PDN GW is also terminated.

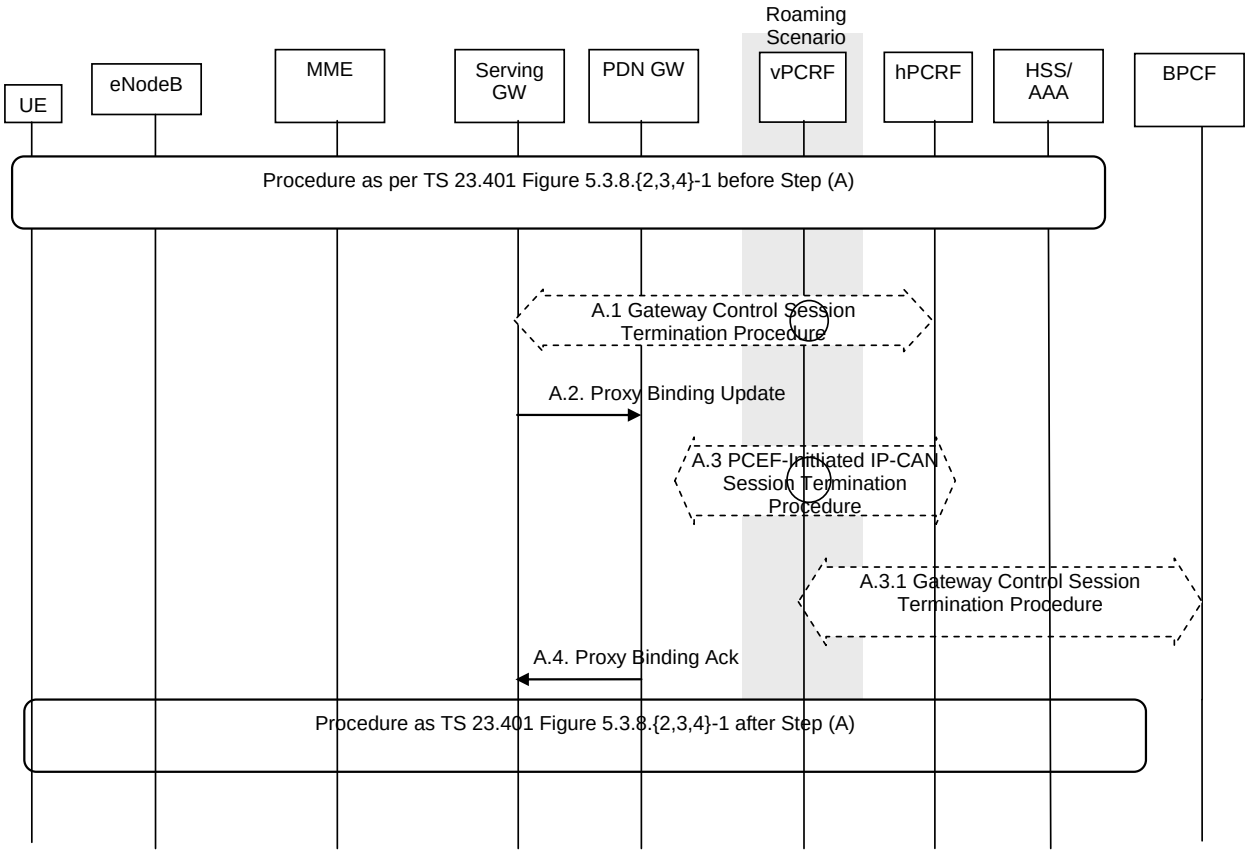


Figure 5.7.3.2-1 (TS 23.402 [3] 5.3-1): E-UTRAN Detach Procedure for PMIP-based S5/S8

A.1) The Serving GW initiates the Gateway Control Session Termination.

A.2) The Serving GW sends a Proxy Binding Update.

A.3) The PDN GW initiates the PCEF-Initiated IP-CAN Session Termination.

A.3.1) The PCRF initiates the GW Control Session termination when the last Gx IP-CAN session bound to an S9a session is terminated (i.e. the UE detaches from the network).

A.4) The PDN GW responds to the Serving GW with the result of the PDN connection release with Proxy Binding Update Acknowledgement.

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

The procedure given in Figure 5.6.1.3-1 applies to all dedicated resource allocation operations for E-UTRAN which are triggered by PCRF, with the only exception of MME-initiated Dedicated Bearer Deactivation procedure which is covered in TS 23.402 [3] clause 5.4.5.3 The procedures initiated by the S-GW in the E-UTRAN differ for each case.

The procedure described in Figure 5.6.1.3-1 shows only the steps, due to PMIP based S5/S8, that are different from the GTP variant of the procedure given in TS 23.401 [2].

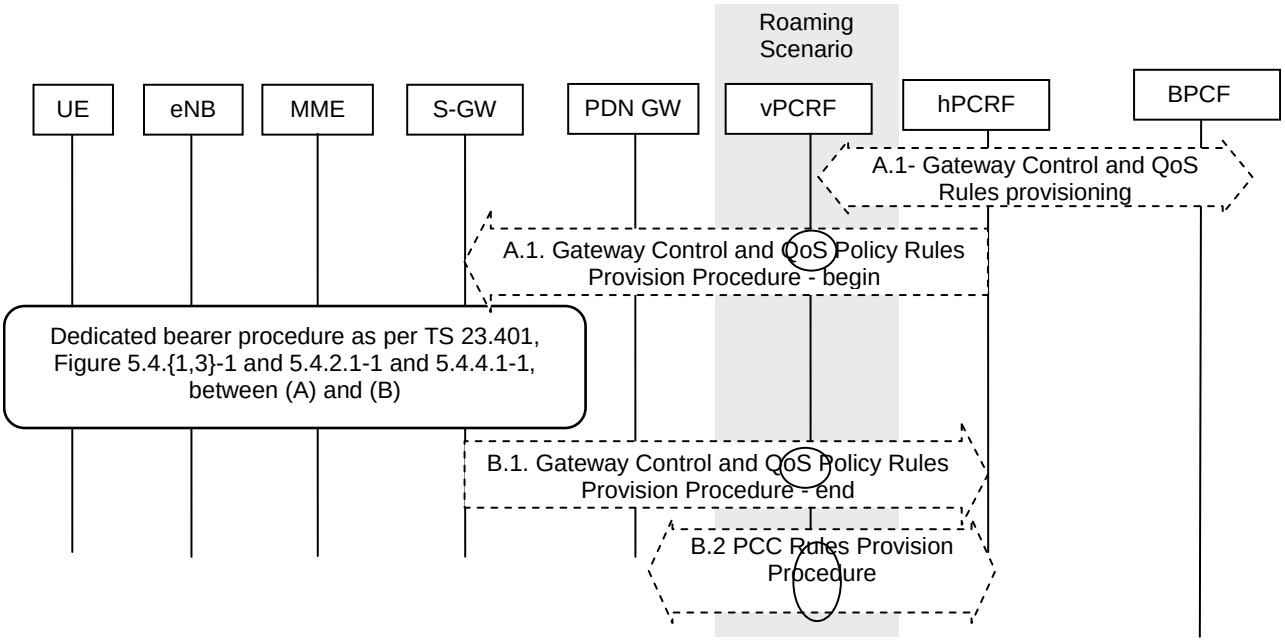


Figure 5.7.3.3-1 (5.4.1-1): Dedicated Resource Allocation Procedure, UE in Active Mode

NOTE 1: Step A1 below is executed after step 1 (IP-CAN Session Modification sent from the PCRF to the PDN GW) according to TS 23.401 [2], clause 5.4.1, and figure 5.4.1-1: Dedicated Bearer Activation Procedure. The new step A.1- shall precede step 1 of TS 23.401 [2], figure 5.4.1-1 in order to determine whether the BPCF will admit the new bearer.

A.1-) The h/PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to determine whether the BPCF will allocate resources for a new SDF/s. The message includes the QoS rule and QoS Information (QCI, ARP, GBR, MBR) IEs.

A.1) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [4] by sending a message with the QoS rules and Event Trigger information to the S-GW.

Steps between A.1 and B.1 are described in TS 23.401 [2], clauses 5.4.{1, 2.1, 3, 4.1}.

B.1) The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could.

B.2) The PCRF initiates the PCC Rules Provision Procedure.

5.7.3.4 Intra-LTE TAU and Inter-eNodeB (macro to HeNB) Handover with Serving GW Relocation

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.

In case of a Serving GW relocation, the target Serving GW must establish a Gateway Control Session with the PCRF to perform policy controlled functions such as Bearer-Binding. The source Serving GW relinquishes its Gateway Control Session with the PCRF in step B.

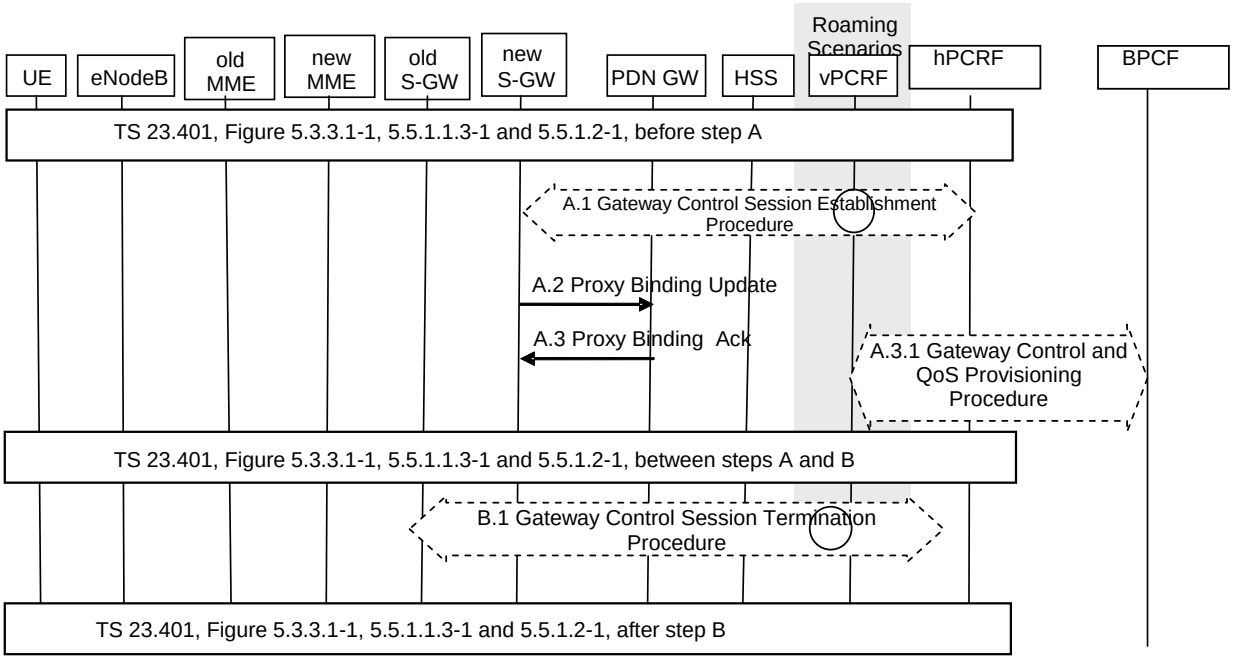


Figure 5.7.3.4 -1 (TS 23.402 [3], 5.7.1-1): Intra-LTE and Inter-eNodeB (macro to HeNB) Handover with Serving GW Relocation

A.1) The Target Serving GW initiates the Gateway Control Session Establishment Procedure.

A.2) The new Serving GW performs a PMIPv6 Proxy Binding.

A.3) The PDN GW acknowledges the Binding

A.3.1) The v/PCRF initiates the GW Control and QoS Provisioning procedure with the BPCF to determine whether the BPCF will whether the BPCF will allocate resources for a new SDF/s. The message includes the QoS rule and QoS Information (QCI, ARP, GBR, MBR) IEs.

Steps between A.3 and B.1 are described in TS 23.401 [2], clauses 5.3.3.1 and 5.5.1.

B.1) The old Serving GW initiates the Gateway Control Session Termination Procedure.

5.8 H(e)NB interworking architecture alternative 3

5.8.1 General

5.8.2 Procedures

5.8.2.1 Procedures for the case when H(e)NB is being used and traffic is routed back to the EPC

5.8.2.1.1 S9a Session Establishment Procedure

The procedure in this clause applies to S9a Session Establishment Procedure, initiated by the H(e)NB Policy Function during the H(e)NB Registration Procedure.

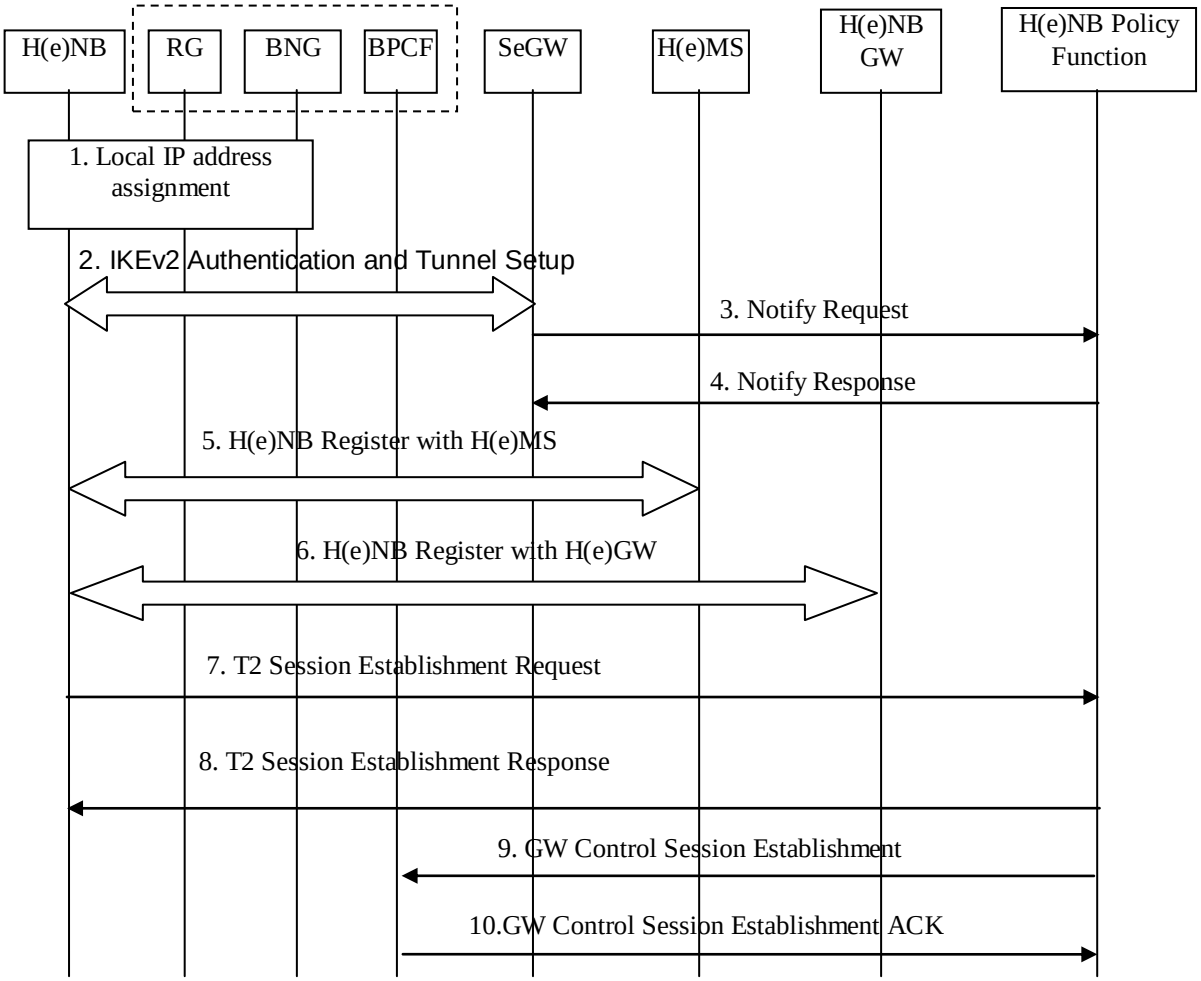


Figure 5.8.2.1.1-1: S9a Session Establishment Procedure

1. When the H(e)NB powers on, it receives a local IP address from the BBF 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 local IP address will be the outer IP address of the IPSec tunnel between the H(e)NB and the SeGW.

2. The IKEv2 tunnel establishment procedure is started by the H(e)NB. The H(e)NB may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The SeGW IP address to which the H(e)NB needs to form IPSec tunnel is discovered via DNS query as specified in clause 5.1 in TS 32.583 and TS 32.593. A secure connection is established between the H(e)NB and Security Gateway. The SeGW assigns an IP address to the H(e)NB as the inner IP address of the IPSec tunnel.

3. The SeGW sends the Notify Request message to the H(e)NB Policy Function, which contains the IPSec Tunnel information (e.g. the outer IP address, the inner IP address, etc.).

4. The H(e)NB Policy Function shall store the IPSec Tunnel information and sends a Notify Response message to the SeGW.

5. The H(e)NB initiates the Registration to H(e)MS Procedure as specified in clause 5.2.1 in TS 32.583 and in clause 5.1.3 in TS 32.593.

NOTE: Step 5 may happen before step 2.

6. The H(e)NB initiates the Registration to H(e)NB-GW, which is already defined in TS 25.467 [12] clause 5.2.2 and in TS 36.413 clause 8.7.3.

7. The H(e)NB initiates the T2 session establishment with H(e)NB Policy Function. The H(e)NB sends the H(e)NB ID and H(e)NB IP address (i.e. IPSec inner IP address) to the H(e)NB Policy Function. The H(e)NB Policy Function binds the T2 Session with the IPSec tunnel information sent by SeGW in step 3 by matching the H(e)NB IP address (i.e. IPSec inner IP address).

8. The H(e)NB Policy Function sends T2 session establishment response to the H(e)NB.

9. Triggered by step 7, the H(e)NB Policy Function initiates establishment of an S9asession by sending GW Control Session Establishment(IPSec Tunnel Information) message to BPCF. The BPCF stores the IPSec Tunnel information to identify the access point of the H(e)NB in the BBF Access network.

10. The BPCF acknowledges the Gateway Control Session Establishment message by sending an GW Control Session Establishment Ack message to the H(e)NB Policy Function.

5.8.2.1.2 Bearer Activation_Procedure

5.8.2.1.2.1 Bearer Activation when a UE attaches to EUTRAN via HeNB subsystem

The bearer activation procedure for a UE attaches to EUTRAN via HeNB subsystem is depicted in figure 5.6.2.1.2-1.

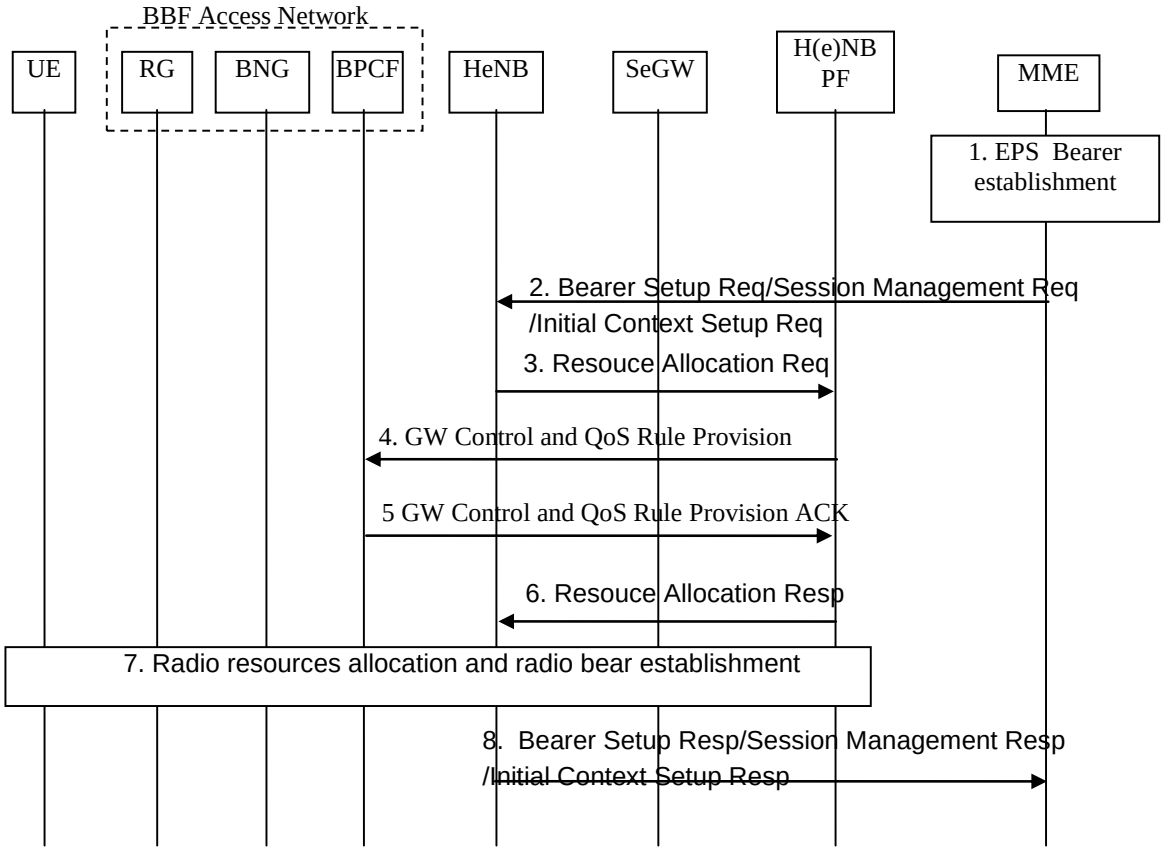


Figure 5.8.2.1.2-1: Bearer activation procedure for a UE attaches to EUTRAN via HeNB subsystem

NOTE: If a HeNB GW is required in the HeNB subsystem, the messages between the HeNB and the MME shall traverse the HeNB GW.

1. If the EPS bearer establishment is required (e.g. default bearer creation, dedicated bearer activation, UE requested bearer resource modification), the Serving GW will send a Create Bearer Request/ Create Session Response message to the MME as defined in TS 23.401 [2].

2. The MME sends to the HeNB the Initial Context Setup Request message during the default bearer creation procedure, or the Bearer Setup Request /Session Management Request message during the dedicated bearer activation procedure and the UE requested bearer resource modification procedure. The messages shall contain the EPS Bearer Identity, the EPS Bearer QoS, as defined in TS 23.401 [2].

3. The HeNB sends the Resource Allocation Request (the EPS Bearer QoS) message to the H(e)NB Policy Function.

4. The H(e)NB Policy Function requests the BPCF to perform admission control. The H(e)NB Policy Function sends the GW Control and QoS Rule Provision (QoS-Rule with the QoS information) message to BPCF. The BPCF performs admission control in BBF access based on the QoS-Rule with the QoS information, which includes QCI, GBR, MBR, and ARP.

5. The BPCF finds the HeNB's access point in the BBF access network, and acquires the available resources at this access point. The BPCF takes into account the information contained in the QoS rule and the available resources at the HeNB's access point, but the details for how admission control is performed in the BBF access is out of scope to 3GPP. If the request is accepted the BPCF may provision the BRAS/BNG with information for QoS control of the service data flow.

   The BPCF sends an GW Control and QoS Rule Provision Ack message to the H(e)NB Policy Function.

6. The H(e)NB Policy Function sends Resource Allocation Response to the corresponding HeNB.

7. The H(e)NB allocates the radio resource, and continue with radio bearer establishment procedure.

8. As defined in TS 23.401 [2], the H(e)NB sends to the MME the Initial Context Setup Response message during the default bearer creation procedure, or the Bearer Setup Response /Session Management Response message during the dedicated bearer activation procedure and the UE requested bearer resource modification procedure.

5.8.2.1.2.2 PDP Context Activation when a UE attaches to UTRAN/GERAN via HNB subsystem

The PDP Context Activation Procedure for a UE attaches to UTRAN/GERAN via HNB subsystem is depicted in figure 5.7.2.1.2-2.

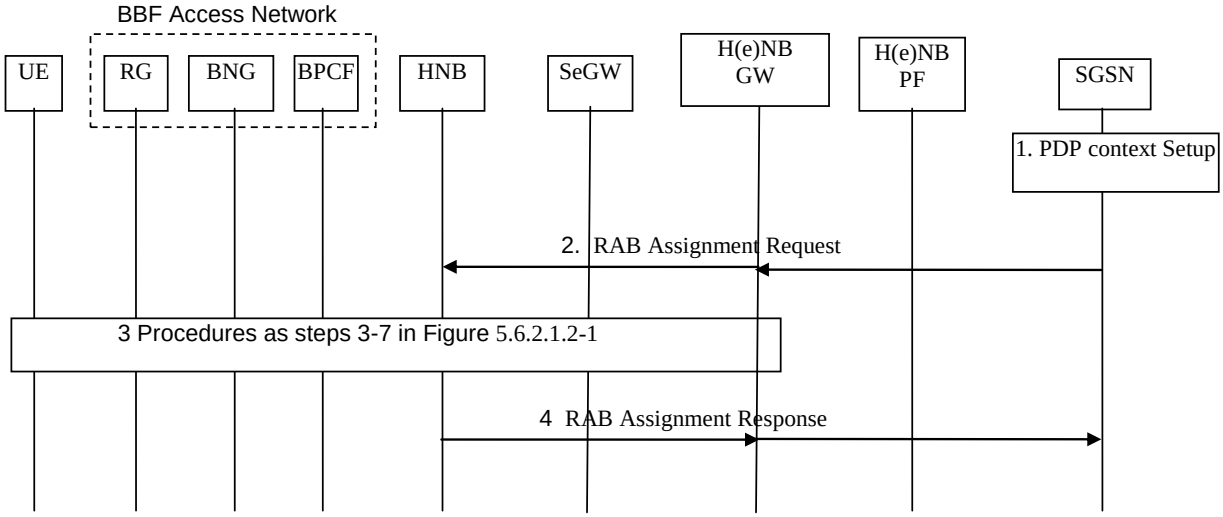


Figure 5.8.2.1.2-2: PDP Context Activation Procedure for a UE attaches to EUTRAN via HeNB subsystem

1. If the PDP Context creation is required (e.g. PDP Context Activation, secondary PDP Context Activation, Network-Requested PDP Context Activation), the GGSN/Serving GW will send a Create PDP Context Response/Create Bearer Request message to the SGSN as defined in TS 23.060 [22].

2. The SGSN initiates RAB setup by the RAB Assignment procedure sending a RAB Assignment Request message to the HNB via HNB GW to establish one or several RABs. The message shall contain the RAB information to be established as defined in TS 23.060 [22].

3. The steps are the same as for steps 3-7 in the clause 5.7.2.1.2.1.

4. The HNB sends to the SGSN the RAB Assignment Response message via HNB GW, as defined in TS 23.060 [22].

5.8.2.1.3 Bearer Deactivation Procedure

5.8.2.1.3.1 Bearer deactivation when a UE attaches to EUTRAN via HeNB subsystem

The bearer deactivation procedure for a UE attaches to EUTRAN via HeNB subsystem is depicted in figure 5.7.2.1.3-1.

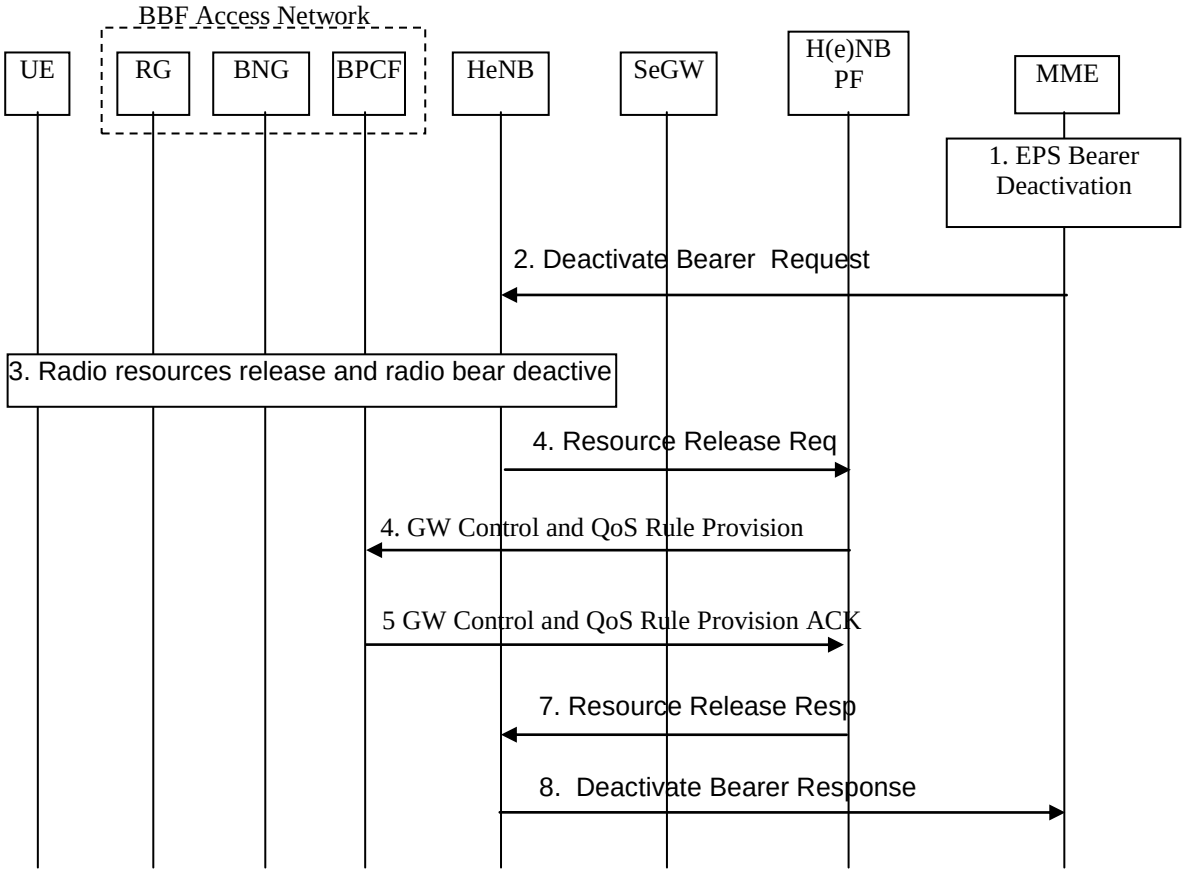


Figure 5.8.2.1.3-1: Bearer deactivation procedure for a UE attaches to EUTRAN via HeNB subsystem

NOTE: If a HeNB GW is required in the HeNB subsystem, the messages between the HeNB and the MME shall traverse the HeNB GW.

1. If the EPS bearer deactivation is required (e.g. PDN GW initiated bearer deactivation, MME Initiated Dedicated Bearer Deactivation detach, S1 release), the Serving GW will send a Delete Bearer Request / Release Access Bearers Response message to the MME as defined in TS 23.401 [2].

2. As defined in TS 23.401 [2], the MME sends to the HeNB the Delete Bearer Request(the EPS Bearer Identity) message during PDN GW initiated bearer deactivation procedure and MME Initiated Dedicated Bearer Deactivation procedure, or sends to the HeNB the S1 UE Context Release Command(cause) message during the detach procedure and the S1 release procedure.

3. The HeNB releases the radio resource, and initiates radio bearer release.

4. The HeNB sends the Resource Release Request (the EPS Bearer QoS) message to the H(e)NB Policy Function.

5. The H(e)NB Policy Function requests the BPCF to release the resource indicated in the Resource Release Request message. The H(e)NB Policy Function sends the GW Control and QoS Rule Provision (QoS-Rule with the QoS information) message to BPCF. The BPCF releases the corresponding resources in BBF access network based on the QoS-Rule with the QoS information.

   If all the activated bearers are released, the H(e)NB Policy Function should send GW Control Session Termination to BPCF to terminate the S9a session.

6. The BPCF takes into account the information contained in the QoS rule and release the corresponding resources, but the details for how to release the resource in the BBF access is out of scope to 3GPP.

   The BPCF acknowledges the GW Control and QoS Rule Provision message by sending an GW Control and QoS Rule Provision Ack message to the H(e)NB Policy Function.

   If the H(e)NB Policy Function indicates the BPCF to terminate the S9a session, the BPCF release the S9a session context and sends GW Control Session Termination Ack to the H(e)NB Policy Function.

7. The H(e)NB Policy Function sends Resource Release Response to the corresponding HeNB.

   If all the activated bearers are released, the H(e)NB Policy Function releases the S9a session.

8. As defined in TS 23.401 [2], the HeNB sends to the MME the Delete Bearer Response / S1 UE Context Release Complete message.

5.8.2.1.3.2 PDP Context Deactivation when a UE attaches to UTRAN/GERAN via HNB subsystem

The PDP Context Deactivation procedure for a UE attaches to UTRAN/GERAN via HNB subsystem is depicted in figure 5.7.2.1.3-2.

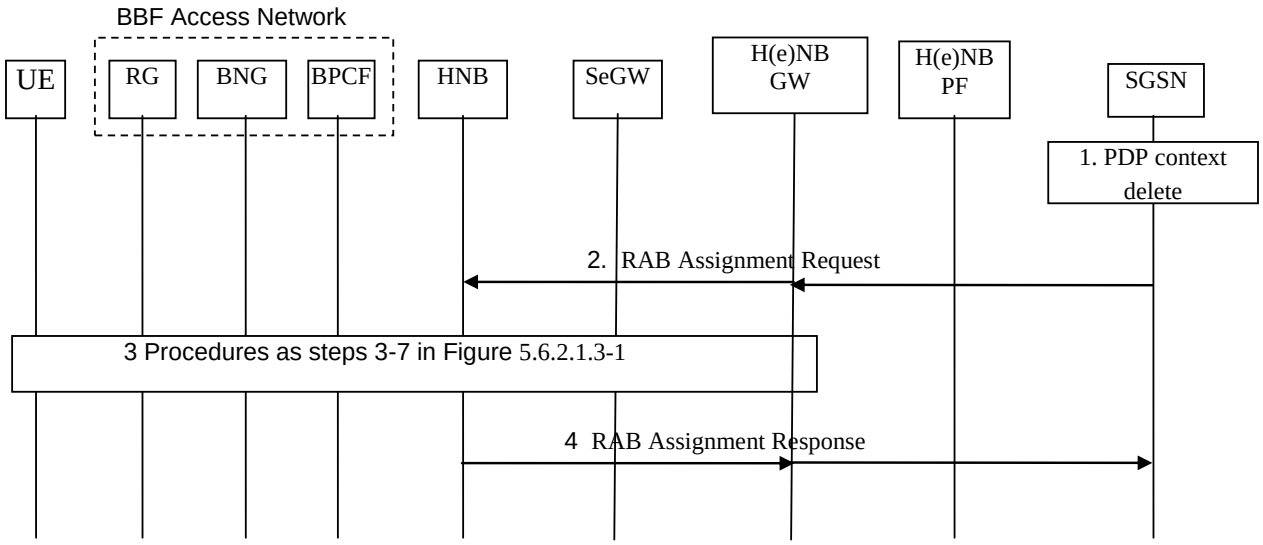


Figure 5.8.2.1.3-2: PDP Context Deactivation procedure for a UE attaches to UTRAN/GERAN via HNB subsystem

1. If the PDP Context delete is required (e.g. PDP Context Deactivation, Detach, RAB Release), the SGSN will be triggered to release the resources as defined in TS 23.060 [22].

2. As defined in TS 23.060 [22], the SGSN initiates RAB release by the RAB Assignment procedure sending a RAB Assignment Request message to the HNB via HNB GW to release one or several RABs. The message shall contain the RAB information to be released.

3. The description of these steps are the same as for steps 3-7 in the clause 5.7.2.1.3.1.

4. The HNB sends to the SGSN the RAB Assignment Response message via HNB GW, as defined in TS 23.060 [22].

5.8.2.1.3.3 Iu Release when a UE attaches to UTRAN/GERAN via HNB subsystem

The Iu Release procedure for a UE attaches to UTRAN/GERAN via HNB subsystem is depicted in figure 5.6.2.1.3-3.

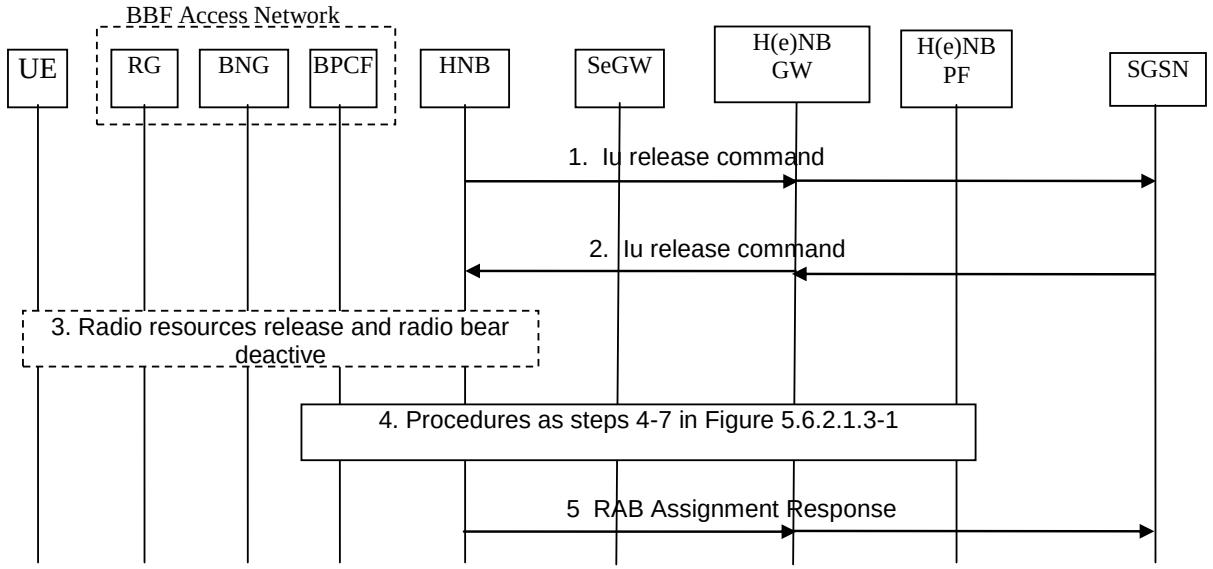


Figure 5.8.2.1.3-3: Iu Release procedure for a UE attaches to UTRAN/GERAN via HNB subsystem

1. HNB initiates Iu Release Procedure, and sends Iu Release Request message to SGSN via HNB GW as defined in TS 23.060 [22].
2. As defined in TS 23.060 [22], the SGSN acknowledges the Iu Release Command message by sending Iu Release Command message.
3. The HNB may release the radio resource, and initiates radio bearer release as defined in TS 23.060 [22].
4. Procedures are the same as for steps 4-7 in the clause 5.7.2.1.3.1.
5. The HNB sends to the SGSN the Iu Release complete message via HNB GW, as defined in TS 23.060 [22].

5.8.2.1.4 Bearer Modification Procedure

5.8.2.1.4.1 Bearer Modification when a UE attaches to EUTRAN via HeNB subsystem

The bearer modification procedure for a UE attaches to EUTRAN via HeNB subsystem is depicted in figure 5.7.2.1.4-1.

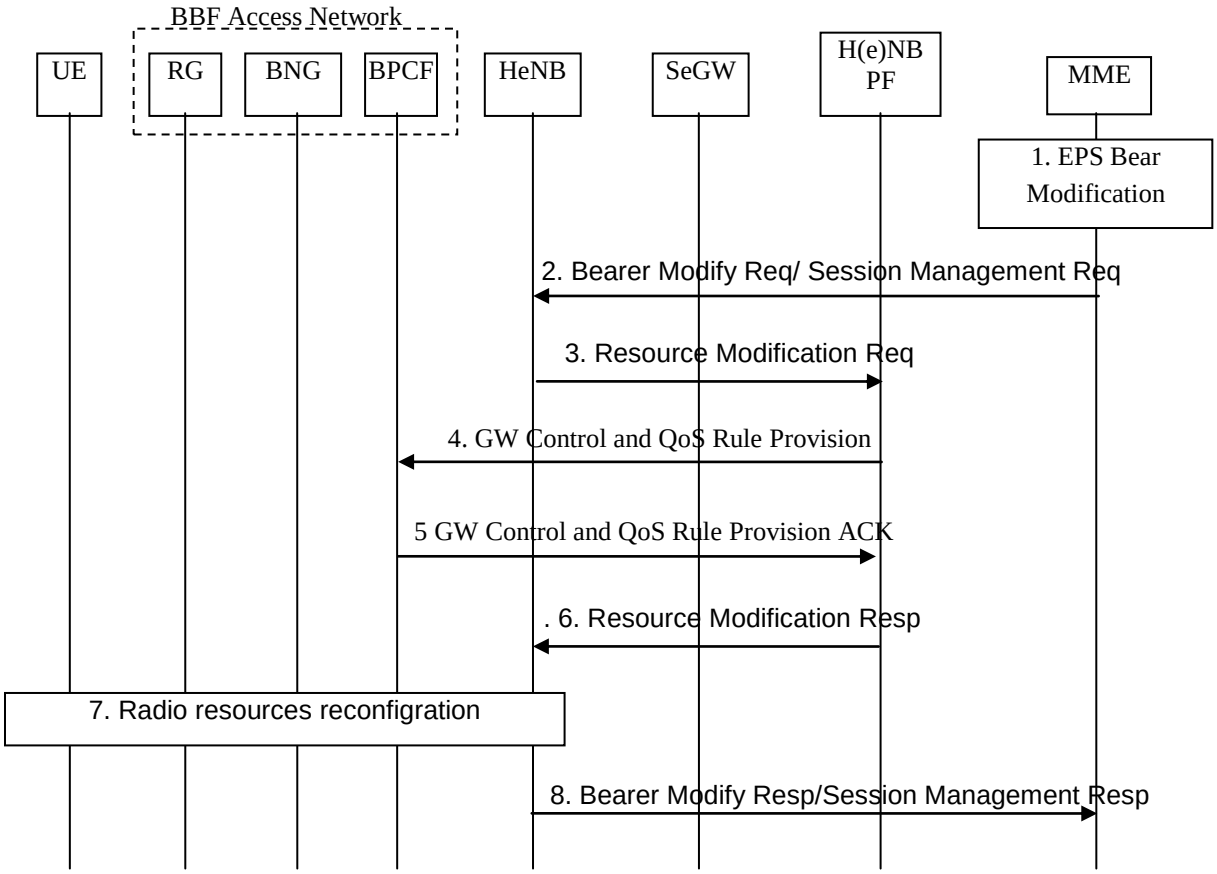


Figure 5.8.2.1.4-1: Bearer modification procedure for a UE attaches to EUTRAN via HeNB subsystem

NOTE: If a HeNB GW is required in the HeNB subsystem, the messages between the HeNB and the MME shall traverse the HeNB GW.

1. If the EPS bearer modification is required (e.g. PDN GW initiated bearer modification with bearer QoS update, HSS Initiated Subscribed QoS Modification), the PDN GW will send a Update Bearer Request message to the MME through the Serving GW as defined in TS 23.401 [2].

2. As defined in TS 23.401 [2], the MME sends the Bearer Modification Request/Session Management Request (the EPS Bearer Identity, EPS Bearer QoS) message to the HeNB.

3. The HeNB sends the Resource Modification Request (the EPS Bearer QoS) message to the H(e)NB Policy Function through the SeGW.

4. The H(e)NB Policy Function requests the BPCF to modify the resource indicated in the Resource Modification Request message. The H(e)NB Policy Function sends the GW Control and QoS Rule Provision (QoS-Rule with the QoS information) message to BPCF. The QoS-Rule with the QoS information indicates the BPCF how to modify the corresponding resources in BBF access network.

5. The BPCF takes into account the information contained in the QoS rule and modifies the corresponding resources, but the details for how to modify the resource in the BBF access is out of scope to 3GPP.

   The BPCF acknowledges the GW Control and QoS Rule Provision message by sending an GW Control and QoS Rule Provision Ack message to the H(e)NB Policy Function.

6. The H(e)NB Policy Function sends Resource Modification Response to the corresponding HeNB according to the Tunnel header information in the S9a Session context.

7. The HeNB initiates the radio resource reconfiguration.

8. As defined in TS 23.401 [2], the HeNB sends to the MME the Bearer Modification Response/Session Management Response message.

5.8.2.1.4.2 PDP Context Modification when a UE attaches to UTRAN/GERAN via HNB subsystem

The PDP Context Modification procedure for a UE attaches to UTRAN/GERAN via HNB subsystem is depicted in figure 5.7.2.1.4-2.

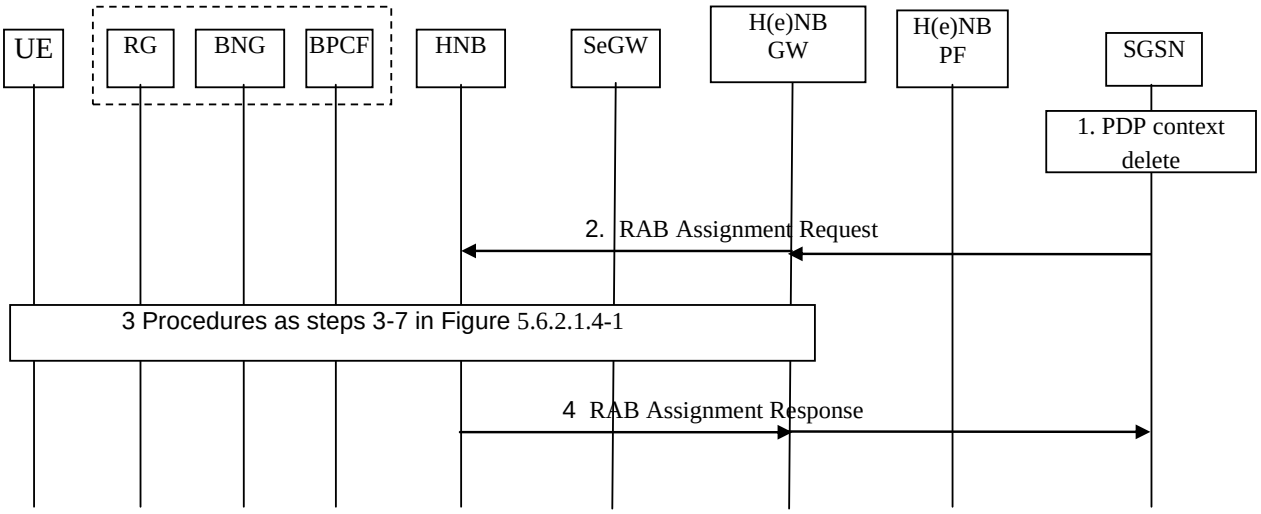


Figure 5.8.2.1.4-2: PDP Context Modification procedure for a UE attaches to UTRAN/GERAN via HNB subsystem

1. If the PDP Context modification is required (e.g. SGSN-Initiated PDP Context Modification, GGSN-Initiated PDP Context Modification, MS-Initiated PDP Context Modification, RAN-initiated RAB Modification), the SGSN will be triggered to modify the RAB parameters as defined in TS 23.060 [22].

2. As defined in TS 23.060 [22], the SGSN initiates RAB modification by the RAB Assignment procedure. sending a RAB Assignment Request message to the HNB via HNB GW to release one or several RABs. The message shall contain the RAB information to be modified.

3. The description of these steps are the same as for steps 3-7 in the clause 5..2.1.4.1.

4. The HNB sends to the SGSN the RAB Assignment Response message via HNB GW, as defined in TS 23.060 [22].

5.8.2.1.5 H(e)NB Deregistration Procedure

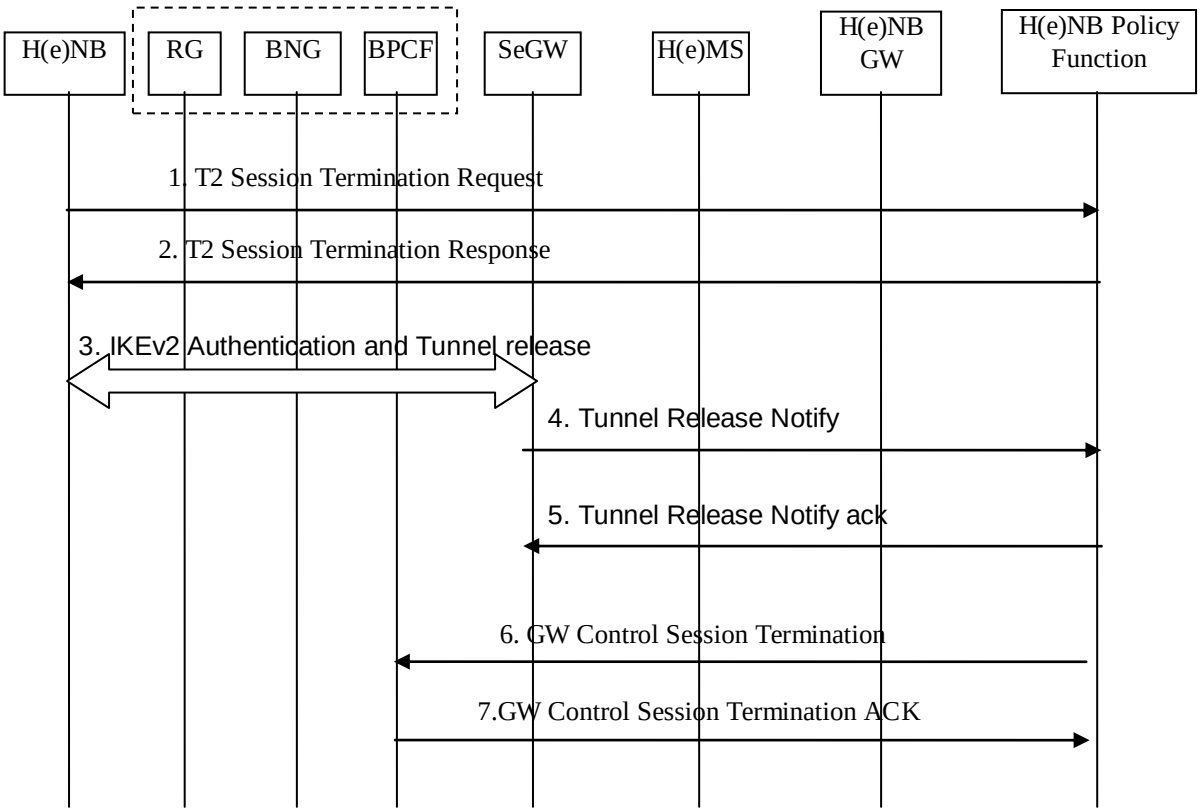


Figure 5.8.2.1.5-1: H(e)NB Deregistration

1. When the H(e)NB deregisters from the 3GPP network, the H(e)NB sends T2 Session Termination Request (H(e)NB ID, H(e)NB IP address) to the H(e)NB PF.
2. The H(e)NB PF responds with T2 Session Termination Response.
3. The H(e)NB may initiate IPSec tunnel release, which may trigger the SeGW to send Tunnel Release Notify to the H(e)NB Policy Function to remove the IPSec tunnel information in the H(e)NB Policy Function.
4. The H(e)NB Policy Function sends Tunnel Release Notify Ack to the SeGW.
5. Triggered by step 1, the H(e)NB Policy Function sends GW Control Session Termination (IPSec tunnel information) to the BPCF to terminate the S9a session.
6. The BPCF sends GW Control Session Termination Ack to the H(e)NB Policy Function.

5.9 Comparison of 3GPP LTE Femto Architecture Options

5.9.1 General

The rows in the comparison table include the solutions and the columns the attributes addressing various aspects of the impact on the network. The table also identifies the NE/s impacted by a particular solution.

The attributes are meant to answer the questions in the following areas:

Roaming transparency

Is the home network aware that the roaming user access the VPLMN via a 3GPP Femto connected to BBF access?

BBF QoS Negotiation

Are Radio Resources allocated to the UE in before it is known whether resources are available in the BBF access?

New Interface/Signalling Sequence in 3GPP (besides S9a)

Does the solution require a 3GPP NE to support a new interface and protocol?

Correlation of UE PCC & S9a QoS sessions

Is the S9a session is independent of the UE PCC session?

Overlay Architecture

Does the solution enhance the existing PCC architecture to handle the S9a session or requires an overlay architecture with new reference point/s and a new policy server (i.e. Femto-PCRF)?

Additional Signalling Load

Does the solution generate additional signalling load in the network? (The S9a signalling is excluded from the comparisons as it is common with all solutions).

Commonality with WLAN PCRF-BBCP IWK

Is the 3GPP Femto solution compatible with the WLAN solution?

Impact on 3GPP NEs

A NE is said to be impacted when the solution requires that the NE supports a new reference point. For instance, the HeNB GW solution requires that the HeNB GW supports a new diameter interface to the F-PCRF and therefore the NE is impacted.

A NE is said not be impacted by the solution when it is required to support only a new IE in he message set and procedures it already supports. For instance, the PCRF based solution does not require the MME, S-GW or P-GW to support a new interface/protocol but a new IE to carry the Tunnel-INFO from the MME to the PCRF using existing messages and signalling sequences. Therefore, the PCRF based solution does not impact these NEs.

Interpretation of the arrows

The arrows in each cell are meant to indicate relative advantage/or disadvantage of a particular solution. A plus sign (+) indicates advantage while a minus sign (-) indicates a disadvantage.

5.9.2 Comparison

5.9.2.1 LTE Architecture options

Table 5.9.2.1-1: LTE Architecture options

Architecture Alternative	Attribute											
	Roaming Transparency	**BBF QoS Negotiation**	**EPC: New Interface/Signalling Sequence (besides S9a)**	**Correlation of UE PCC & S9a QoS sessions (2)**	**Overlay Architecture**	**Additional Signalling Load**	**Commonality with WLAN PCRF-BBCP IWK**	**HeNB**	**SeGW**	**HeNB GW**	**MME**	**PCRF**
PCRF (Alt 2)	No (3) (-)	Yes (+)	No (+)	Yes (+)	No (+)	Low (+)	Yes (+)	No (+)	No (+)	No (+)	No (6) (+)	Yes (7) (-)
MME (option 1.1) (8)	Yes (+)	No (1) (-)	Yes (-)	No (-)	Yes (-)	High (-)	No (-)	No (+)	Yes (4) (-)	No (+)	Yes (-)	No (+)
HeNB GW (Option 1.2) (8)	Yes (+)	No (1) (-)	Yes (-)	No (-)	Yes (-)	High (-)	No (-)	No (+)	Yes (4) (-)	Yes (-)	No (+)	No (+)
HeNB (option 3) (8)	Yes (+)	No (1) (-)	Yes (-)	No (-)	Yes (-)	High (-)	No (-)	Yes (-)	No (+)	No (+)	No (+)	No (+)

Note 1: Backhaul QoS negotiation is possible if the F-PCRF waits for a response from the BPCF before continuing with the remainder of the EPS procedures or the variation detailed in slides are used.
Note 2: Correlation refers the 3GPP network. Note that It is not possible to discriminate individual UE sessions at the BNG due to IP Sec tunnelling.
Note 3: The limitation exists for the GTP HR traffic that is a very small subset of the overall traffic.
- Note that the roaming subscriber must register with the 3GPP Femto in the VPLMN.
- Note that this limitation applies also to the 3GPP-BBF IWK architecture for WLAN.

Note 4: Required at H(e)NB Power up to interface with the F-PCRF/ H(e)NB Policy Function.
Note 5: New Interfaces to the F-PCRF.
Note 6: Open issue on how MME retrieves tunnel info.
Note 7: S1-AP and S5/S8 need to carry additional IE/s (e.g. IP@ of IPSec tunnel). Open issue on how MME retrieves tunnel info.
Note 8: Require a new functional entity - the F-PCRF, that may reside at the PCRF.

5.9.2.2 UMTS Architecture Options

Table 5.9.2.2 -1 UMTS Architecture options

Option	Attribute											
	Roaming Transparency	**QoS Negotiation**	**EPC: New Interface/Signalling Sequence (besides S9a)**	**Correlation of UE PCC & S9a QoS sessions (2)**	**Overlay Architecture**	**Additional Signalling Load**	**Commonality with WLAN PCRF-BBCP IWK**	**HNB**	**SeGW**	**HNB GW**	**SGSN**	**PCRF**
PCRF (Alt 2) (8)	No (3) (-)	Yes (+)	No (+)	Yes (+)	No (+)	Low (+)	Yes (+)	No (+)	No (+)	No (+)	No (6) (+)	Yes (6) (-)
HNB GW (Alt 1) (7) (10)	Yes (+)	No (1) (-)	Yes (-)	No (-)	Yes (-)	High (-)	No (-)	No (+)	Yes (4) (+)	Yes (-)	No (+)	No (+)
HNB (Alt 3) (7) (9) (10)	Yes (+)	No (1) (-)	Yes (-)	No (-)	Yes (-)	High (-)	No (-)	Yes (-)	No (+)	No (+)	No (+)	No (+)

Note 1: Backhaul QoS negotiation is possible if the F-PCRF waits for a response from the BPCF before continuing with the remainder of the EPS procedures or the variation detailed in slides are used.
Note 2: Correlation refers the 3GPP network. Note that It is not possible to discriminate individual UE sessions at the BNG due to IPSec tunnelling.
Note 3: The limitation exists for the GTP HR traffic that is a very small subset of the overall traffic.
- Note that the roaming subscriber must register with the 3GPP Femto in the VPLMN.
- Note that this limitation applies also to the 3GPP-BBF IWK architecture for WLAN.

Note-4: Required at H(e)NB Power up to interface with the F-PCRF/ H(e)NB Policy Function.
Note-5: New Interfaces to the F-PCRF.
Note-6: Gn/Gp, S4 and S5/S8 need to carry additional IE/s (e.g. IP@ of IPSec tunnel). Open issue on how the SGSN obtains the tunnel information.
Note-7: Require a new FE - the F-PCRF, that may reside at the PCRF.
Note-8: Support PS only. It is the same solution as for LTE Femto.
Note-9: The signalling interface with the F-PCRF is not based on the Ruh interface.
Note 10: Supports PS and CS.

5.10 3GPP Femto Architecture Decision

A way forward is based on the architecture diagrams below.

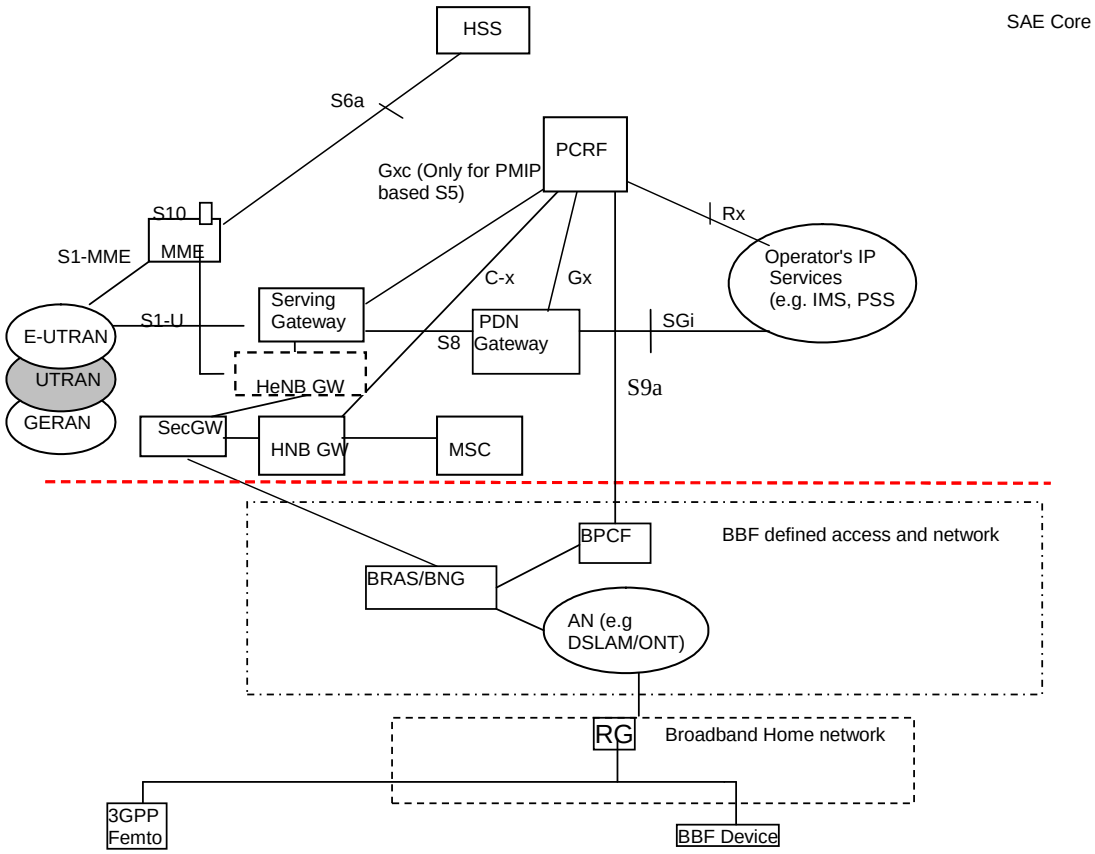


Figure 5.10-1: Architecture for CS and PS support

NOTE 1: CS support is provided by the serving network.

NOTE 2: Dynamic allocation of resources in the BBF access network for circuit switched calls from the HNB can be provided by C-x interface.

Editor's note: It is FFS whether CSG membership based admission control is required. If it does, the impact to the system architecture will be addressed accordingly.

5.10.1 3GPP HNB procedure

5.10.1.1 3GPP HNB for CS service

5.10.1.1.1 S15 session establishment at HNB Power on

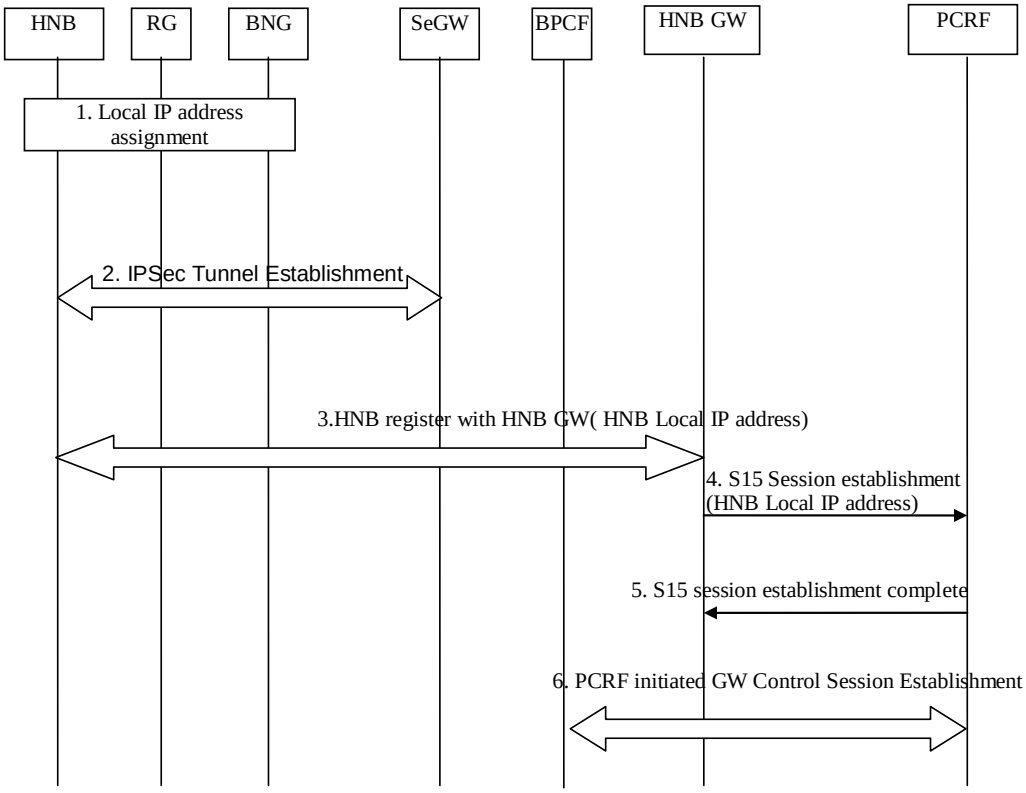


Figure 5.10.1.1.1: HNB power on procedure

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 optionally the UDP port number (if NAT/NAPT is detected).
4. The HNB GW establishes a S15 session with the PCRF including information about the HNB such as, HNB local IP address, UDP Ports if NAT/NAPT is detected and/or the FQDN of Fixed Broadband network at which the HNB is connected to.
5. The PCRF responds to the S15 session establishment request.
6. The PCRF initiates Gateway Control session Establishment to establish S9a session and sends the HNB local IP address and the UDP port number if NAT/NAPT is detected to the BPCF in this step.

5.10.1.1.2 S15 session modification (3G Femto)

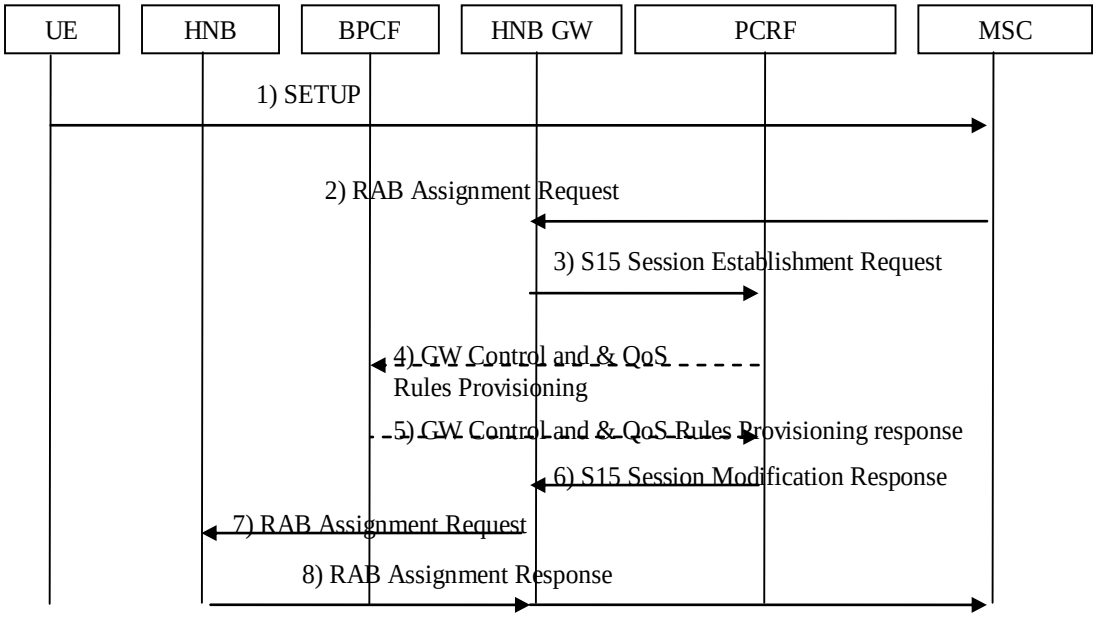


Figure 5.10.1.1.2: S15 session modification

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

1. The UE initiates call setup using a SETUP message.
2. The MSC sends a RAB Assignment Request message towards the HNB.
3. The HNB GW requests S15 session modification to the PCRF. The message includes QoS information derived from the RAB message.
4. The PCRF initiate the GW Control and & QoS Rules Provisioning procedure as per TS 23.203 [4].
5. The BPCF acknowledges the changes to the GW Control and & QoS Rules Provisioning.
6. 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.
7. The HNB GW sends the RAB assignment message to the HNB.
8. The remainder of the call setup procedure completes.

5.10.1.1.2 S15 session termination (3G Femto)

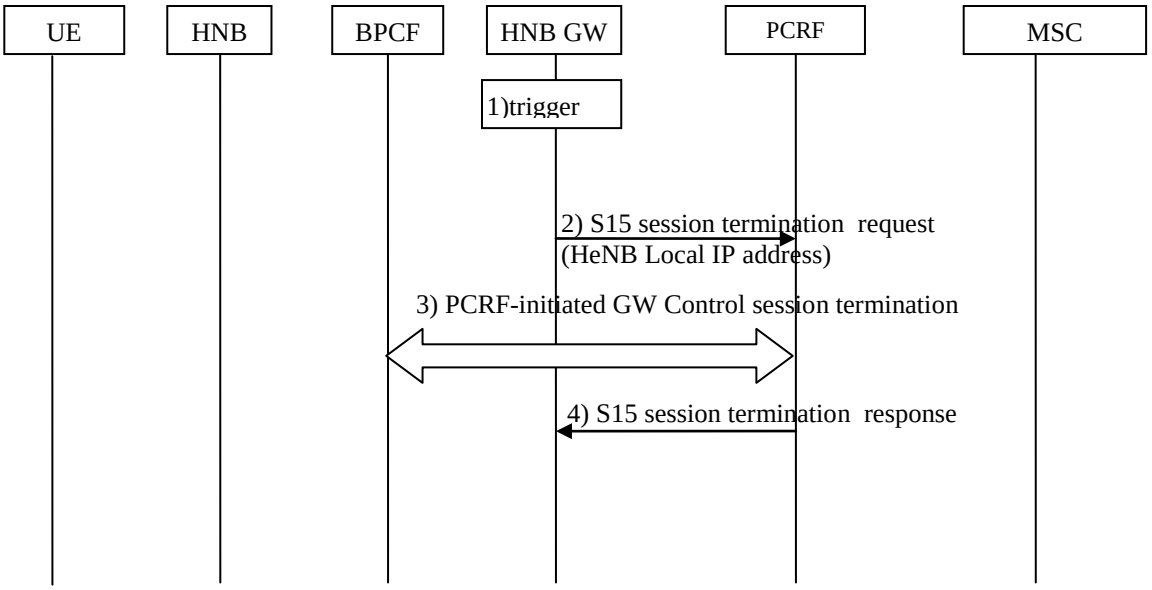


Figure 5.10.1.1.3: S15 session Release

1. the HNB GW detects the trigger for initiates termination of S15 session. The trigger may be the Deregistration of HNB from HNB GW etc.
2. The HNB GW requests S15 session termination to the PCRF.
3. The PCRF starts a PCRF initiated the GW control session termination via S9a session toward BPCF.
4. The PCRF acknowledge the request for termination of S15 session.

5.10.1.2 3GPP HNB procedures for signalling of Tunnel Information for PS services

The HNB GW sends the tunnel information and the FQDN of the BPCF to the SGSN in the [RANAP] DIRECT TRANSFER message (for the message refer to TS 25.413).

Depicted in Figure 5.10.1.x-1 is the PDP Context Activation procedure.

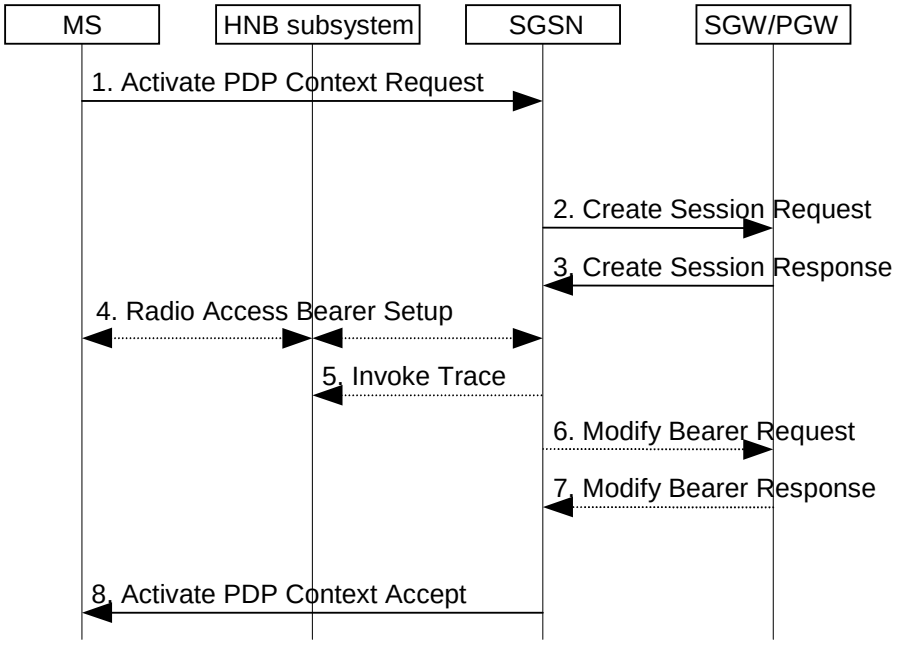


Figure 5.10.1.2-1: PDP Context Activation Procedure for EPS-connected 3G access

This procedure is similar to the combination of procedures described in TS 23.060 [22] clauses 9.2.2.1 and 9.2.2.1A, with modifications to the following steps:

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] DIRECT TRANSFER message the HNB Local address, UDP port numbers when NAT/NAPT is detected, and/or the FQDN of the BPCF in the BBF access network.

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 address, UDP port numbers when NAT/NAPT is detected, and/or FQDN of BPCF in the Create Session Request sent to the SGW/PGW. The HNB Local address, UDP port numbers when NAT/NAPT is detected, and/or FQDN of the BPCF are then forwarded to the PCRF over Gx (not shown).

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).

Editor's note: RAN WG3 need to confirm whether the RANAP impact due to signalling of tunnel information is acceptable.

5.11 Conclusions

The study for BB1 can be considered concluded with the description of requirements in this clause. The normative requirements for supporting BBF interworking with home routed traffic for WLAN and H(e)NB is defined in TS 23.139 and TS 23.203 [4]. Any further enhancements for BBAI BB1 are included directly in the TS 23.139 and TS 23.203 [4], so this clause of the TR 23.839 will be not up-to-date any more with respect to BB1 aspects.

6 Building Block II

Editor's note: This clause will contain the material related to Building Block II.

Editor's note: This clause may not be up-to-date; please refer to the normative TS 23.139 and TS 23.203 [4] for up-to-date content.

6.1 Architecture

Editor's note: This clause will identify the architectural requirements and assumptions as well as architecture common for building block II. The architecture reference model is already defined in building block I. This clause only captures additions to building block I.

Editor's note: Agreements so far:

- QoS is a requirement for non-seamless WLAN offload. In some scenarios providing QoS may not be possible; see FFS list below.

- The UE needs to authenticate to EPC such that UE policies can be sent to BBF (see clauses 6.2 and 6.3 step 1).

Editor's note: FFS:

- Upstream QoS by means of reflective QoS (6.2).

Editor's note: Whether or not the same reference point SWa/STa is used for Authentication/Authorization and for Accounting and the introduction of SWo and SWf reference points needs to be verified by SA WG5.

6.1.1 Architecture for WLAN

6.1.1.1 Reference model

Figure 6.1.1.1-1 shows the reference architecture for non-seamless WLAN offload. The non-seamless traffic is routed to an external network directly from BBF network.

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

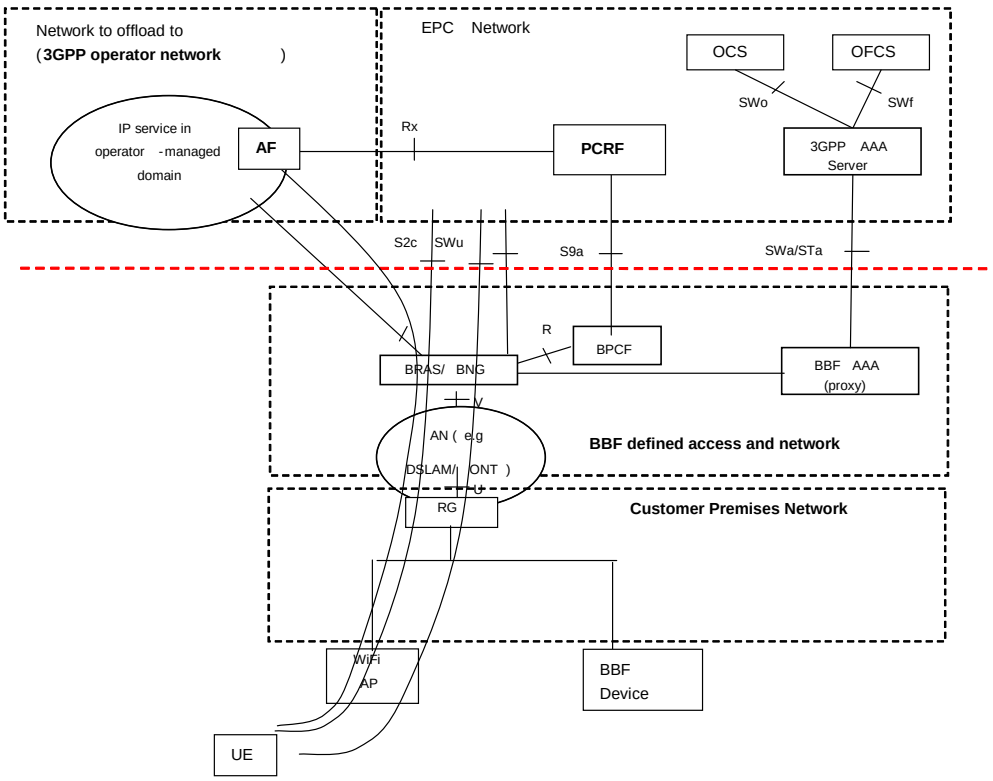


Figure 6.1.1.1-1: WLAN offload with the network to offload to being 3GPP domain with AF- non-roaming scenario

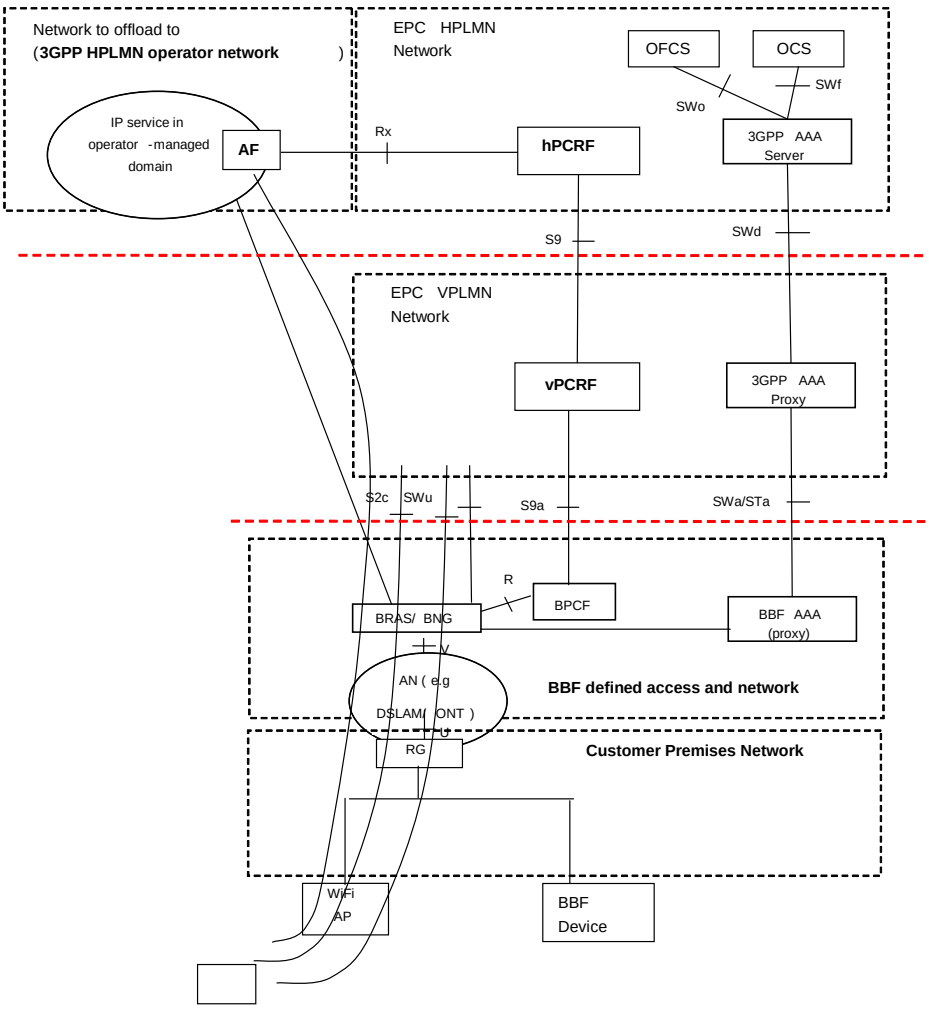


Figure 6.1.1.1-2: WLAN offload with the network to offload to being 3GPP domain with AF - roaming scenario

In this architecture scenario the AF interface the PCRF directly.

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

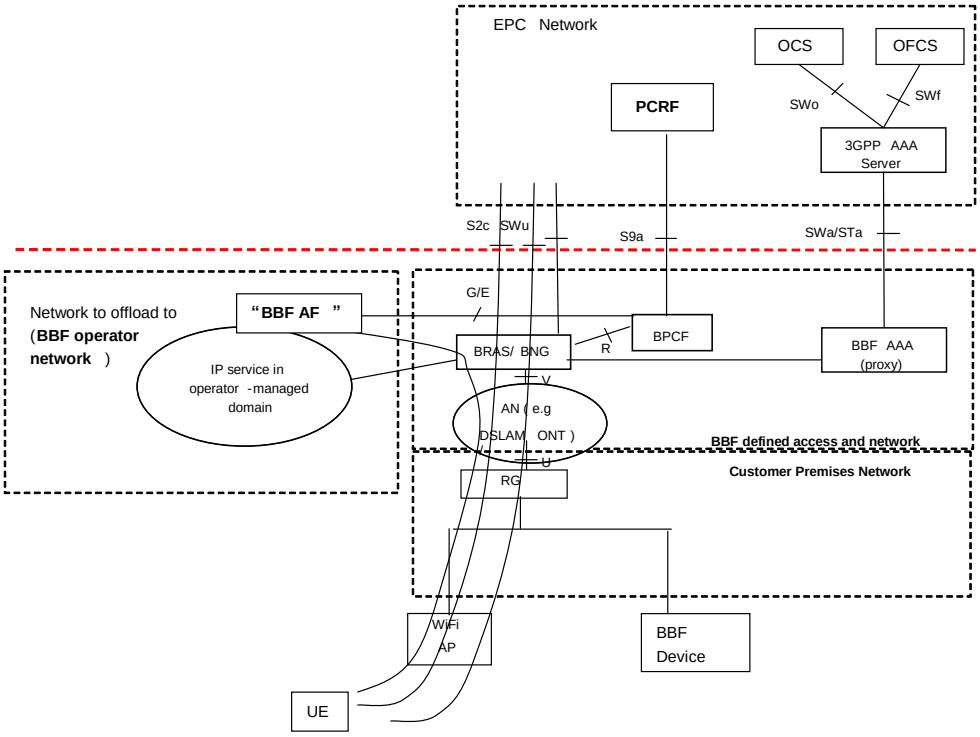


Figure 6.1.1.1-3: WLAN offload with the network to offload to being BBF domain with AF - non-roaming scenario

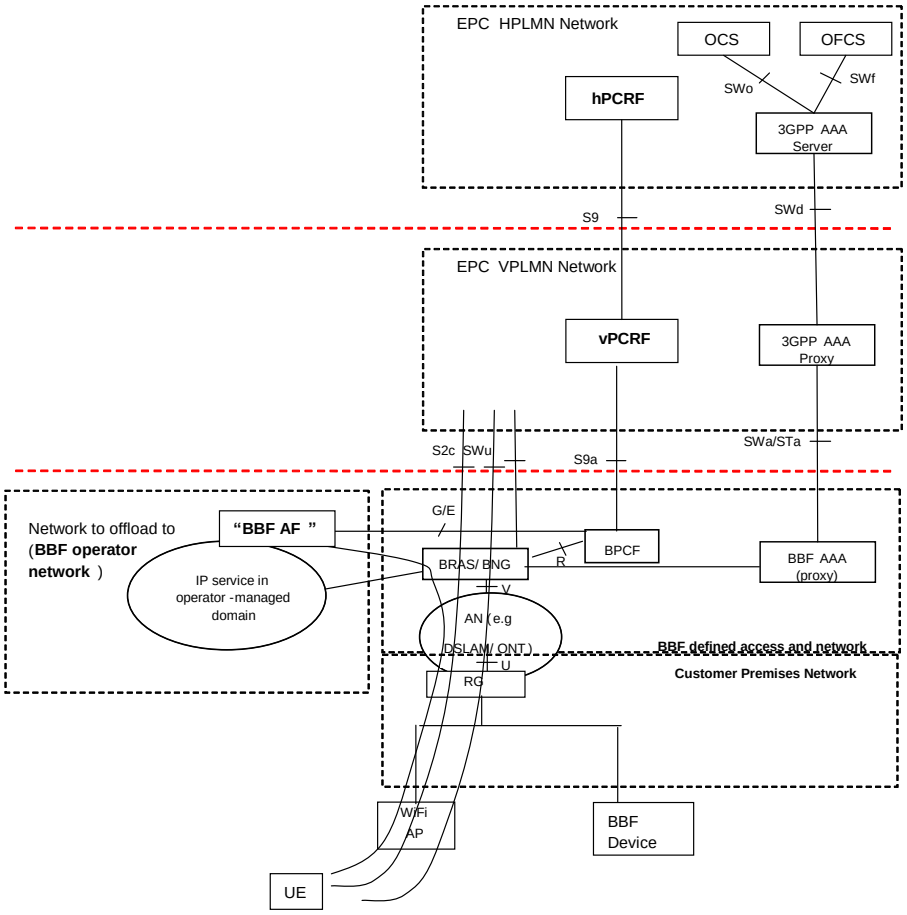


Figure 6.1.1.1-4: WLAN offload with the network to offload to being BBF domain with AF - roaming scenario

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

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

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

- The BPCF needs to map the request received on E/G (with UE local IP address) to the right S9a session (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.

Editor's note: The above assumption needs to be checked with BBF.

Architecture scenario C: TDF

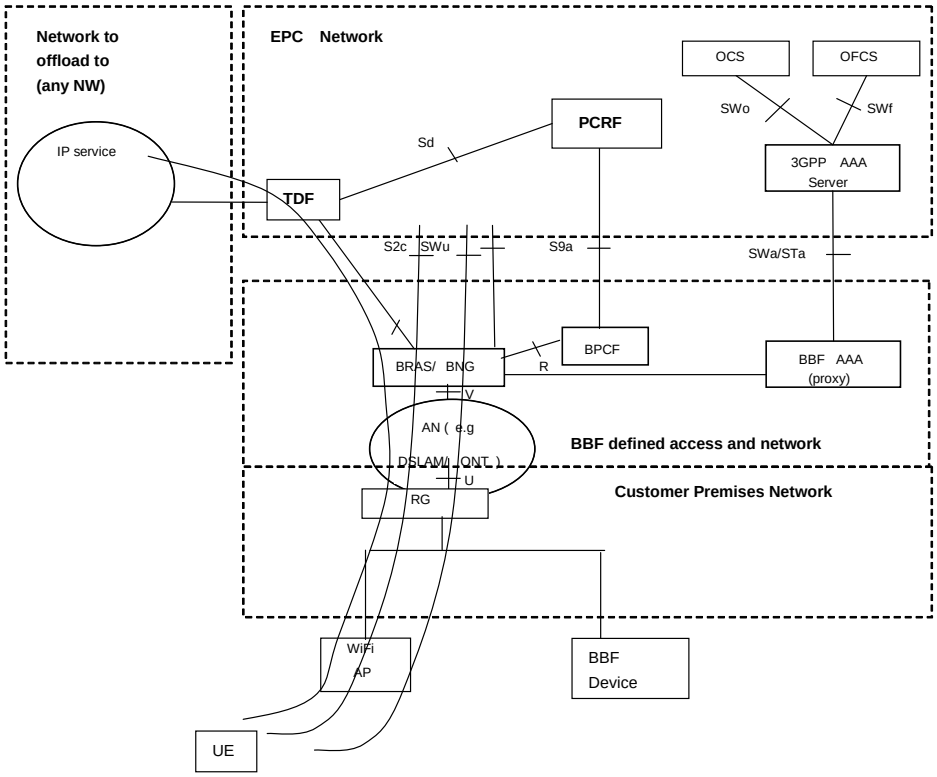


Figure 6.1.1.1-5: WLAN offload with TDF – non-roaming scenario

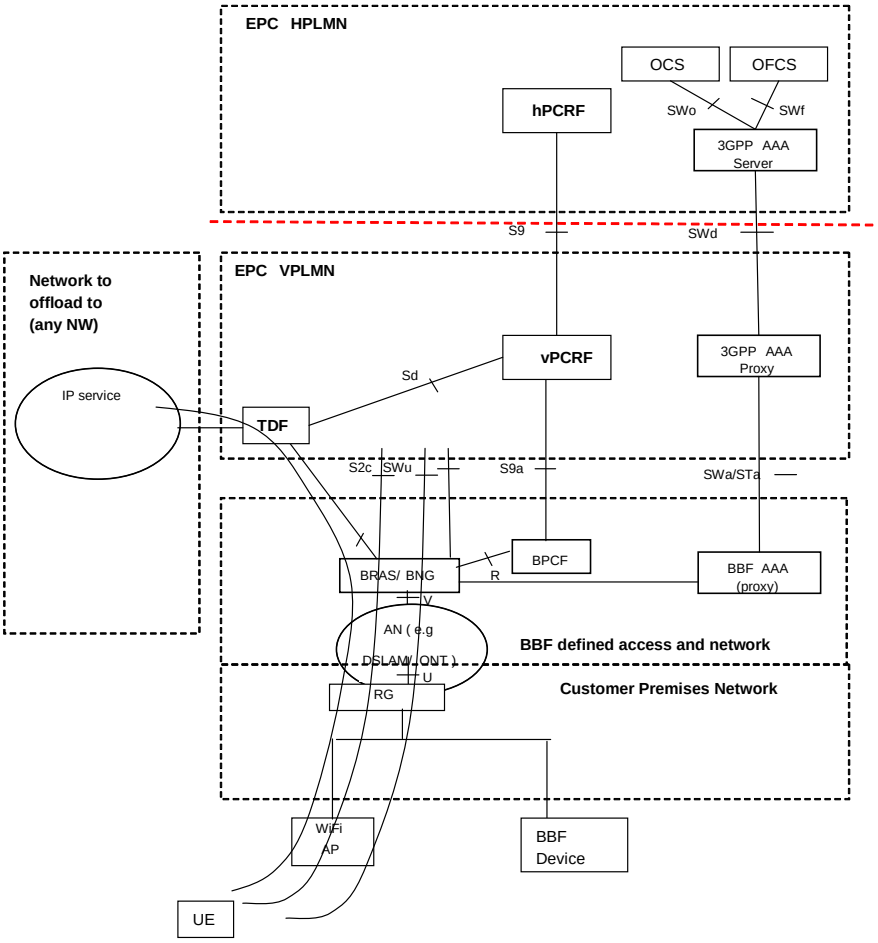


Figure 6.1.1.1-6: WLAN offload with TDF – roaming scenario

In this architecture alternative:

- It is assumed that multiple TDFs may be deployed.
- It is assumed that 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.
- In the solicited model, it is assumed that the PCRF can 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 subject to packet inspection by the TDF.
- Policies for roaming users may be locally configured in the vPCRF and/or TDF.

The following assumptions are made about 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 packet inspection may physically bypass the TDF.

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

Architecture variants out of scope

The architecture variant with TDF in the BBF domain with an interface between the TDF and other entities in the BBF domain (e.g. BPCF) is out of scope for BB2.

6.1.1.2 Architectural requirements and assumptions

For interworking purposes, non-seamless WLAN offload as defined in TS 23.402 [3], clause 4.1.5 is applicable.

The UE might or might not be behind a NAT. The NAT might reside in the BBF access network or in the customer premises network.

Policy interworking via S9a for offloaded traffic in this release is supported for scenarios without NAT in the BBF domain.

NOTE 1: The BBF network may apply local policies for offloaded traffic from 3GPP UEs behind a NATed RG.

NOTE 2: Support for scenarios with NATed RGs in BBF domain can be considered in a future release.

For performing non-seamless WLAN offload, the UE needs to acquire a local IP address on WLAN access, but is not required to establish S2c or SWu. For policy interworking purposes, if the UE did not establish S2c or SWu, it is assumed that the UE has performed 3GPP based access authentication.

Policies may be provided by the PCRF even though they are not triggered by an Rx or Sd request.

Editor's note: (requirements related to) Charging and account is FFS.

Editor's note: Other mechanisms for PCRF and TDF addressing/discovery, for unsolicited and solicited models respectively, are FFS

6.1.1.3 PCRF and TDF discovery

Editor's note: This clause identifies problems and solutions with discovering and addressing the PCRF and TDF in the BB2 architecture scenarios.

Editor's note: In the description of the solutions below, it is assumed that there is no NAT. The solution that includes NAT is FFS.

PCRF discovery by BPCF when establishing the S9a session is the same as for Building Block 1 and is described in TS 23.203 [4], Annex P.

The DRA may be used to find the correct PCRF. At S9a session establishment the DRA in the HPLMN stores the relation between the IMSI, UE local IP address and selected PCRF. If there are multiple PCRFs serving the UE (for different PDN Connections) the DRA may select one of the PCRFs to handle the policies for the offloaded traffic.

PCRF discovery by the AF and TDF for the different architecture scenarios is described below:

Architecture scenario A:

The DRA stores, in addition to the parameters described in TS 23.203 [4], also the UE local IP address.

PCRF can be found by the AF by using the mapping from UE local IP address or IMSI to PCRF stored in DRA.

The AF may find the correct DRA in the same PLMN based on UE local IP address and/or IMSI (if available). The AF may also have pre-configured information to find the DRA, e.g. DRA IP address.

In case of no DRA, the AF may be preconfigured with PCRF address based on IP address ranges.

Architecture scenario B:

The means for how the "BBF AF" finds the BPCF is out of 3GPP scope.

Architecture scenario C:

One solution for TDF addressing in the solicited model is that the TDF address is configured in the PCRF. It is assumed that UL and DL traffic is routed via the same TDF as was configured in the PCRF.

Alternatively, the PCRF may also receive the TDF address as part of S9a signalling.

Editor's note: The above assumption needs to be checked with BBF.

The DRA selects the PCRF at unsolicited service reporting over Sd.

The DRA stores, in addition to the parameters described in TS 23.203 [4], also the UE local IP address.

6.1.1.4 Network Elements

The 3GPP network elements are defined in details in TS 23.401 [2] and TS 23.402 [3].

The Offline Charging System is within the 3GPP network. Offline Charging system is a collection of charging function, specified in TS 32.240 [24], used for offline charging.

The Online Charging System (OCS) is located within the 3GPP network. The OCS is described in TS 32.296 [25].

To support online and offline charging of offloaded traffic, the 3GPP AAA Server is enhanced to report per-user charging/accounting information about offloaded traffic to the HPLMN Offline Charging System. The 3GPP AAA Proxy is enhanced to relay accounting data between the BBF AAA Proxy in VPLMN and the 3GPP AAA Server in HPLMN. The 3GPP AAA Proxy is further enhanced to report per-user charging/accounting information to the VPLMN Offline Charging System for roaming users.

6.1.1.5 Reference Points

The reference point S1-MME, S1-U, S3, S4, S10, S11 are defined in TS 23.401 [2].

The reference points S2b, S2c, S6a, S6b, SWx, SWa, SWm, SWn, SWu, SGi, Rx, Gxc are defined in TS 23.402 [3].

The reference points SWo and SWf connect the 3GPP AAA Server to the OCS and OFCS respectively. These reference points may be based on Wo/Wf as defined in TS 23.234 [23].

SWa It connects the BBF AAA proxy with the 3GPP AAA Server/Proxy and transports access authentication, authorization and accounting information in a secure manner.

STa 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.

Editor's note: Whether or not the same reference point SWa/STa is used for Authentication/Authorization and for Accounting and the introduction of SWo and SWf reference points needs to be verified by SA WG5.

6.1.1.6 Charging

The charging support for 3GPP UEs when traffic is offloaded in the local wireline network can be supported when the BBF network reports per-user accounting data via the STa/SWa reference points.

Both offline and online charging may be supported by the 3GPP domain.

NOTE: It is assumed that the BBF does not need to be aware of whether online or offline charging is used.

It is assumed that 3GPP based access authentication is performed so that STa/SWa is established.

It is assumed that the BNG is able to recognize the traffic of individual 3GPP UEs.

Editor's note: Charging for 3GPP UEs that have not performed 3GPP based access authentication is FFS.

In order to allow the 3GPP operator to perform charging for 3GPP UEs when traffic is offloaded in the local wireline network, the following assumptions are made about functionality in the BBF Access Network:

- The BBF network is able to collect per user accounting data for offloaded traffic of 3GPP UEs and to periodically report this data via the STa/SWa reference points.

6.1.2 Architecture for Femto

Editor's note: This clause covers femto-specific architecture aspects for offloading.

6.2 Policy and QoS

6.2.1 QoS interworking solution

Editor's note: In the description below, it is assumed that there is no NAT. The solution that includes NATs is FFS.

Policies for a UE's offloaded traffic are sent from the EPC Network to the BBF access network via S9a.

Establishment of S9a for a UE is either done as a result of the UE's 3GPP-based access authentication, or as a result of S2b/S2c tunnel setup. If neither 3GPP-based access authentication nor tunnel setup is performed, then no policies from the EPC Network can be sent to the BBF access network for the offloaded traffic.

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

For architecture variant B, it is assumed that BPCF shall bind the request from AF with an existing S9a session using the UE local IP address received from AF and the subscriber ID (e.g. IMSI), if available.

For architecture variant C, in solicited 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 mode, the TDF notifies the PCRF the detected service using Sd interface.

The BBF access network might be pre-configured with policies for a UE.

It is assumed that QoS for a UE's offloaded traffic is enforced by the BBF access network, based on rules received via S9a from the EPC Network. For the WLAN case, the BBF domain sets a per-flow DSCP marking on each packet. Which BBF entity is performing the DSCP marking is out of scope of 3GPP (e.g. BNG).

Editor's note: The feasibility of implementing DSCP setting for DL traffic needs to be acknowledged by BBF.

For the WLAN case, DSCP marking on offloaded traffic may be performed by the UE by means of reflective QoS as defined in TS 23.139 clause 6.3. In order to protect the Fixed Broadband Network from misbehaving UEs, the Fixed Broadband Network might implement protective measure as outlined in TS 23.139 clause 6.3. Additional protective measures might be implementation by the Fixed Broadband Network. All these protective measures are out-of-scope for 3GPP.

Editor's note: The feasibility of the implementing protective measures in the Fixed Broadband Network, as a result of introducing reflective QoS also for offloaded traffic needs to be acknowledged by BBF.

A distinction is made between static and dynamic policies. Static policies for a UE are those policies that are known by the EPC Network at the time of UE attachment. Dynamic policies for a UE are those policies that cannot be known by the EPC Network at the time of UE attachment.

The UE may simultaneously have a connection to the HPLMN 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 WLAN offload traffic QoS rules sent by PCRF shall include in IP filter 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 (for trusted S2c) or the UDP source port for used by IPSec tunnel traffic.

6.2.2 S9a procedures for offloaded traffic

6.2.2.1 General

The BNG is assumed to support only Policy Control Functions for IP-CAN sessions therefore the indication of IP-CAN session establishment over S9a means that only policy control functions applies for the IP-CAN session for offloaded traffic.

A successful session binding of an AF session to an IP-CAN session for UE local IP address will generate QoS Rules by the PCRF for the purpose of policy control in the BBF domain (i.e. BNG).

The purpose of the QoS Rules provisioned for the UE local IP address is to enable policy control in the BBF domain (i.e. BNG) in two different ways:

- Gate enforcement. The BNG is expected to allow a service data flow, which is subject to policy control, to pass through the BNG if and only if the corresponding gate is open.
- QoS enforcement: The BNG is expected to enforce the authorized QoS of a service data flow according to the QoS information provided over R interface (e.g. to enforce downlink DSCP marking).

6.2.2.2 Non-Roaming and Roaming Procedures

Indication of IP-CAN Session Establishment for offloaded traffic

This procedure results in an S9a session for provisioning QoS Rules for the IP-CAN session for the UE local address.

There are two possibilities for how to trigger establishment of an S9a session for offloaded traffic.

Scenario A: BPCF-initiated Indication of IP-CAN Session Establishment:

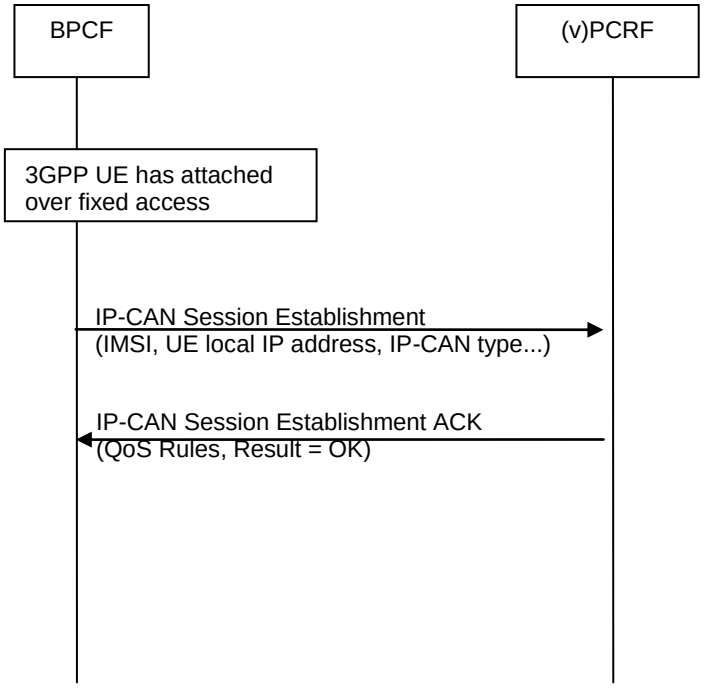


Figure 6.2.2.2-1: Indication of IP-CAN Session Establishment for offloaded traffic scenario A

The BPCF can trigger the Indication of IP-CAN session establishment if it becomes aware that a 3GPP UE has attached via the BBF access and also learns the IMSI of the subscriber. and the UE local IP address. The information contained in the request message includes e.g. IMSI, IP-CAN type and the UE local IP address. The reply message contains the result code and may also include QoS Rules as described in TS 23.203 [4].

Scenario B: PCRF-initiated Indication of IP-CAN Session Establishment:

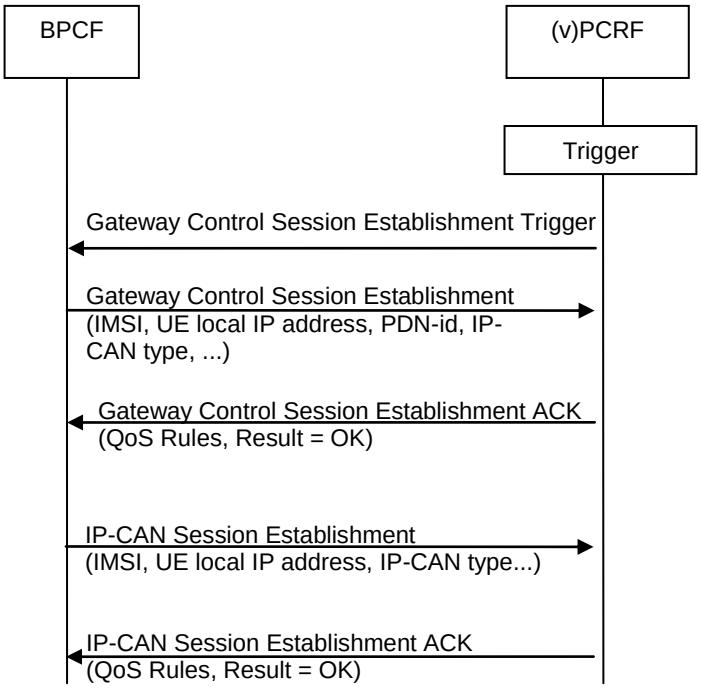


Figure 6.2.2.2-2: Indication of IP-CAN Session Establishment for offloaded traffic Scenario B

If the UE attaches to EPC, the procedure described in BB1 to establish a gateway control session to provision QoS Rules for traffic routed to EPC is performed. In addition, the BPCF triggers the indication of IP-CAN session establishment to PCRF if not already established.

PCRF-Initiated IP-CAN Session Modification for offloaded traffic

This procedure results in provisioning QoS Rules for the IP-CAN session for the UE local address. As a result the BPCF and the BNG are able to associate IP flows to SDF and perform policy control according to the QoS information provided for the IP-CAN session.

NOTE: Implementation of IP-CAN session and Gateway Control Session messages is defined in stage 3 specifications

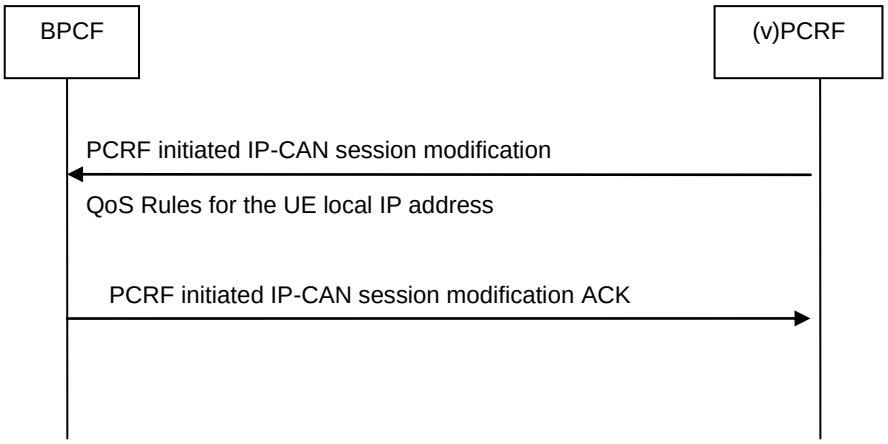


Figure 6.2.2.2-3: Indication of IP-CAN session modification for offloaded traffic

The PCRF initiated IP-CAN session Modification includes the QoS Rules for the UE local IP address: The BPCF translates the QoS rule as received of the S9a interface into access specific QoS parameters applicable in the BBF domain.

BPCF-Initiated IP-CAN Session Termination

This procedure would be initiated by the BPCF to terminate a IP-CAN session for the UE local IP address. The trigger in BPCF for initiating this procedure may be that the 3GPP UE is no longer connected via the BBF access (e.g. if the local IP address is released), if any gateway control session exists for home routed traffic it is also terminated.

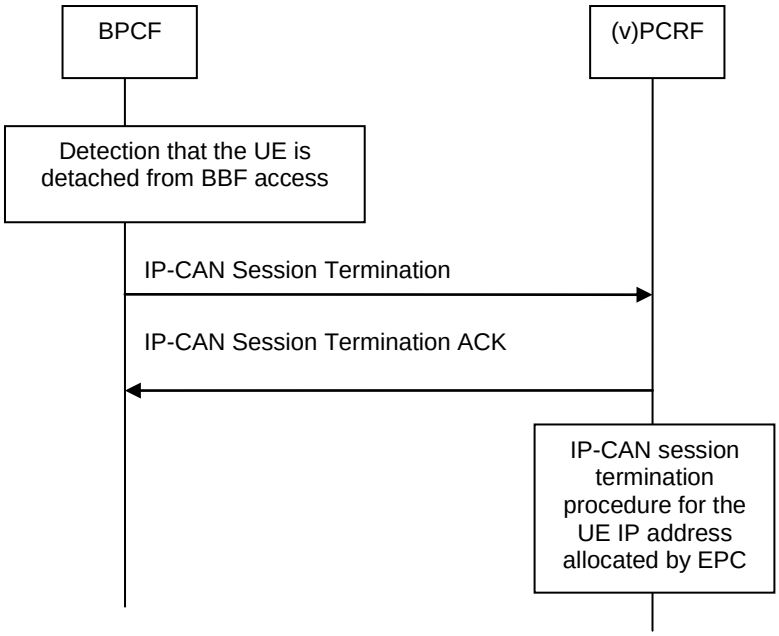


Figure 6.2.2.2-4: IP-CAN Session termination for the offloaded traffic

6.3 Procedures WLAN

6.3.1 Attach and handover flows with or without simultaneous attach to EPC

This procedure is applicable if the UE accesses via a Fixed Broadband Access network, traffic is offloaded in the BNG and if dynamic PCC is deployed. The purpose is to establish a session between the BPCF and the PCRF to provision QoS Rules for offloaded traffic in the Fixed Broadband Access.

Depending on scenario, either the steps shown in (A) or the steps in (B) are performed. There is a need to create an S9a session for offloaded traffic which can be triggered by the 3GPP access authentication as described in (A) or by the successful tunnel authentication procedure when the UE connects to EPC as described in (B).

NOTE 1: It is up to stage 3 to determine how policy rules for IP-CAN sessions for NS-WLAN offloaded traffic and policy rules for Gateway Control Sessions for the EPC routed traffic are transferred from PCRF to BPCF and if these procedures are combined or not.

NOTE 2: The TDF for home traffic and the TDF for offloaded traffic may or may not be the same.

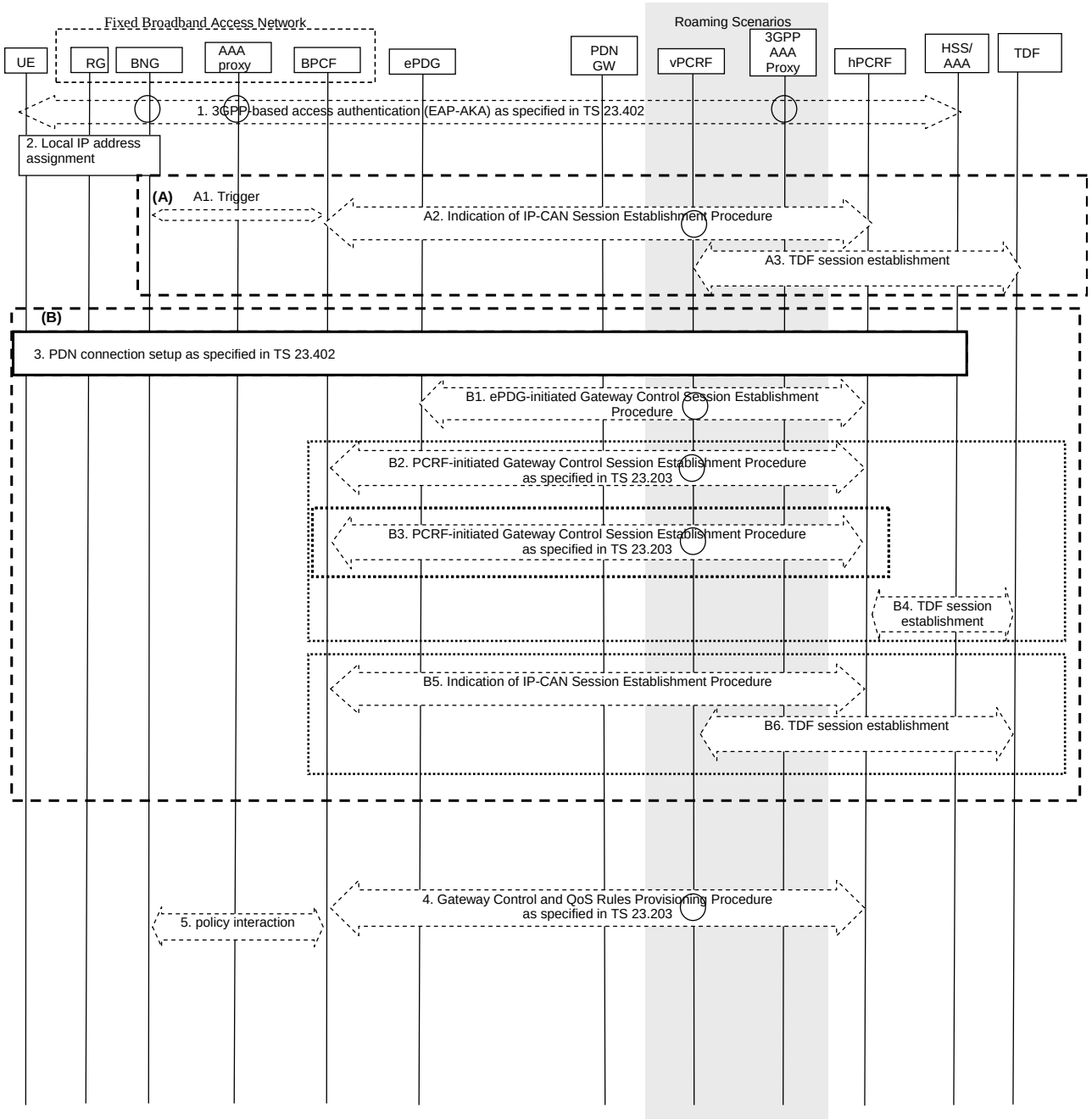


Figure 6.3.1-1: Initial attach or handover from 3GPP access procedure in WLAN

Editor's note: In the description of the steps below, it is assumed that there is no NAT. The solution that includes NATs is FFS.

1, 2, A1, A2) For details of this step, see the initial attach and handover call flows in building block 1. In this step the UE receives its local IP address. The UE authenticates to the 3GPP network either by means of 3GPP-based access authentication or as part of the S2b/S2c tunnel setup. As a result, the BPCF sends an indication that the IP-CAN session is established for this UE. After this step, the UE local IP address is known to the PCRF (non-roaming case), hPCRF (roaming, home-routed case) or vPCRF (roaming, local break-out case). QoS rules for this UE may be sent to the BBF access network. These rules are applicable for offloaded traffic of a UE identified by the UE local IP address, which enables the BBF domain to correlate packets to this UE.

A3) Triggered by the successful establishment of the IP-CAN session for the UE local IP address in step A2, the vPCRF (roaming) and the PCRF (non-roaming) establishes a session with the TDF to provision ADC Rules for that UE local IP address.

3, B1, B2, B3) If the UE establishes an IP-CAN session for EPC routed traffic, these steps take place, for details see initial attach and handover call flows in building block 1 for S2b and S2c cases.

B4) Triggered by the indication of IPCAN session establishment and for the solicited service mode the TDF session is established to provision ADC Rules for that UE IP address from EPC.

B5) Triggered by the request to establish a Gateway Control Session to provision QoS Rules for EPC routed traffic, the BPCF sends an indication that the IP-CAN session for offloaded traffic is established if step A2 did not take place.

B6) After successful establishment of the IP-CAN session for offloaded traffic, the TDF session is established to provision ADC Rules for the offloaded traffic.

4, 5. Policy interactions as described in building block 1.

6.3.2 Network-Initiated Dynamic Policy Control for offloaded traffic

This procedure is applicable if the UE accesses via a Fixed Broadband Access network, traffic is offloaded in the BNG and if dynamic PCC is deployed. The purpose is to provision QoS 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 for the UE local IP address and enforced QoS.

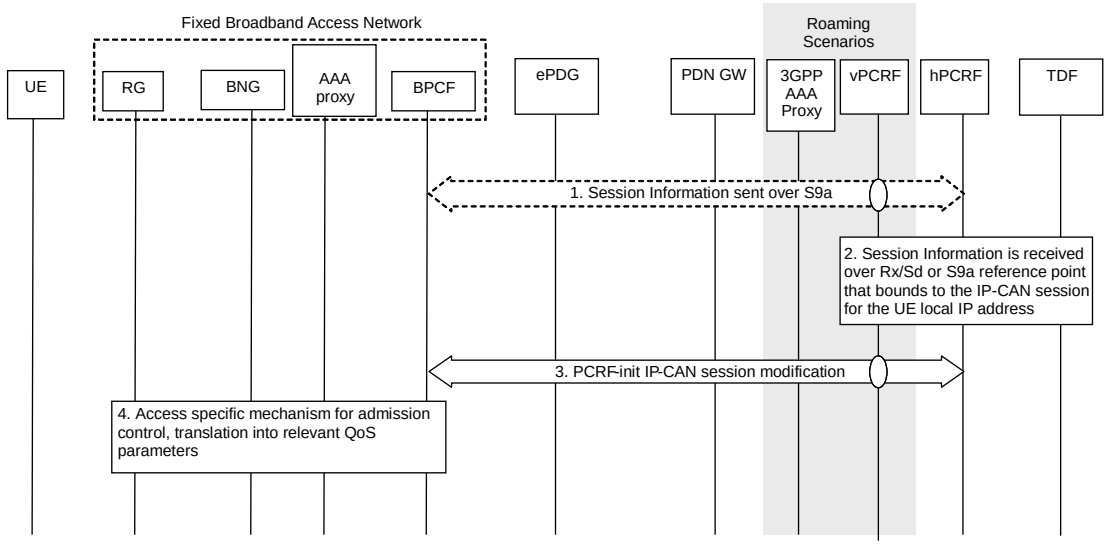


Figure 6.3.2-1: Network-initiated dynamic policy control procedure for offloaded traffic

1. Optionally, for variant B for non roaming scenarios service information for a 3GPP UE identified by the UE local IP address or the IMSI is received by BPCF then sent over S9a to the PCRF. For roaming scenarios the service information received by hPCRF over Rx interface (variant A) or by the vPCRF over Sd interface (variant C) or sent over S9a (variant B) is sent to the hPCRF over S9 interface.

2. PCRF generates QoS 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 vPCRF (for roaming case) initiates the PCRF-init IP-CAN session modification Procedure with the BPCF over S9a to provision QoS Rules for the UE local IP address. In roaming scenario, the hPCRF will initiate the procedure over S9 towards the vPCRF and the vPCRF in turns initiates the procedure over S9a towards the BPCF.

4. 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.

6.3.3 UE or NW detach procedure

This procedure is applicable if the UE is detached from the Fixed Broadband Access, e.g. UE local IP address is released. As a result, the IP-CAN session for the UE local IP address is released. This also triggers the released of all Gateway Control Sessions for the same UE by the BPCF.

Editor's note: It requires investigation if and how the BBF access network is informed that the UE has not any PDN connection established to trigger the termination of the IP-CAN session for offloaded traffic.

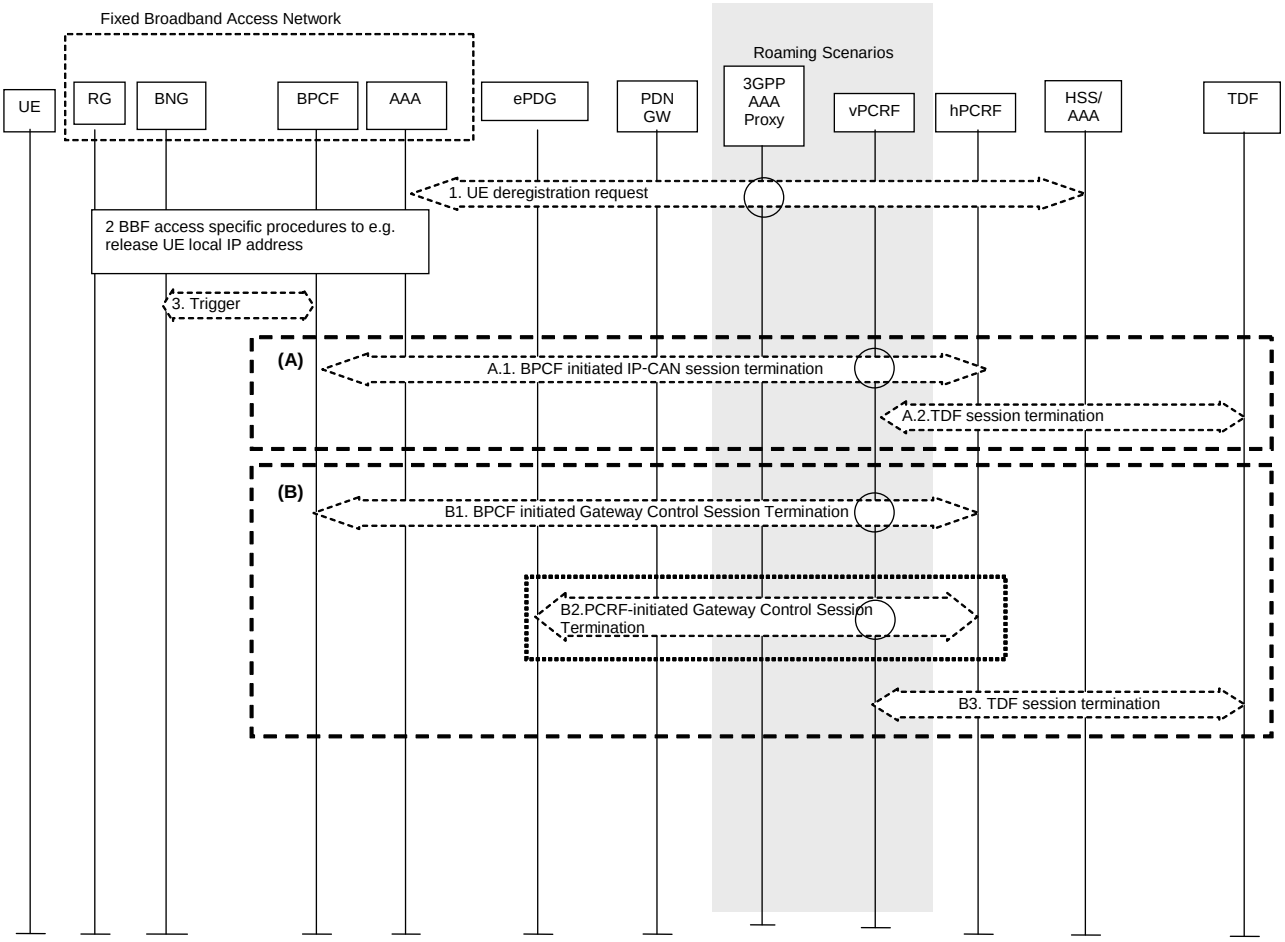


Figure 6.3.3-1: UE or NW detach from the fixed broadband access

1. The detached may be triggered by the NW or by the UE. When triggered by the NW, the 3GPP AAA may send deregistration request to the BBF access.
2. Triggered by step 1, or by other BBF internal procedures (e.g. timer expires) the UE is detached by the BBF domain.
3. The notification that the UE is detached is sent to the BPCF.

A) These steps remove the IP-CAN session for offloaded traffic:

A1 Trigger by step 3, the BPCF sends an indication that the IP-CAN session for the UE local IP address is released to the PCRF

A2 The PCRF terminates the TDF session for the UE local IP address, if exists.

B) These steps remove the Gateway Control Session to provision QoS Rules for the EPC routed traffic.

B1) Triggered by step 3, the BPCF sends an indication that the Gateway Control Sessions described in building block 1.

B2) Optionally, if one or several Gateway Control Session with the BBERF in the ePDG exist, PCRF terminates all Gateway Control Sessions with that BBERF as described in building block 1.

B3) Optionally if one or several TDF session exists, the PCRF terminates the all TDF sessions for that UE IP address.

NOTE: This procedure is based on the assumption on the BBF access can detect when the UE has been disconnected. How this is done is out of scope of 3GPP.

6.3.4 Dynamic ADC Rules provisioning

This procedure is applicable if the UE accesses via a Fixed Broadband Access network, traffic is offloaded in the BNG and if dynamic PCC is deployed. The purpose is to provision or to remove ADC Rules to the TDF over Sd reference point.

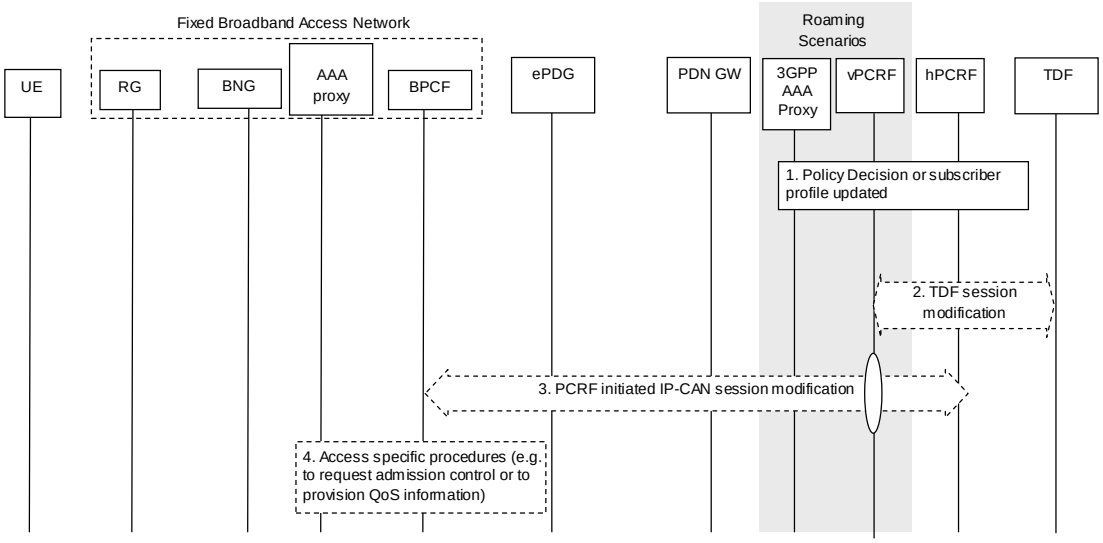


Figure 6.3.4-1: Network-initiated dynamic policy control procedure for offloaded traffic

1. A Policy decision in the PCRF (for non-roaming) or in the hPCRF (for home routed or visited access) or subscriber profile update occurs.
2. Optionally, PCRF (for non-roaming) or vPCRF (for home routed and visited access) sends ADC Rules over Sd reference point.
3. Optionally, PCRF (for non-roaming) or vPCRF (for home routed and visited access) provides QoS Rules to the BPCF.
4. 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.

6.4 Procedures Femto

Editor's note: This clause will identify the procedure for offloaded traffic when the UE attaches via Femto.

6.5 Conclusions

The study for BB2 can be considered concluded with the description of requirements in clause 6. The normative requirements for supporting BBF interworking where traffic is offloaded in the fixed broadband network will be defined in TS 23.139 and TS 23.203 [4]. Any further enhancements for BBAI BB2 are included directly in the TS 23.139 and TS 23.203 [4], so this clause of the TR 23.839 will be not up-to-date any more with respect to BB2 aspects.

7 Building Block III

Editor's note: This clause will contain the material related to Building Block III.

7.1 Scenarios

Within Rel-11, the following scenarios will be considered:

- WLAN S2b: UE connects to WLAN/BBF with traffic routed to ePDG/PDN GW.
- WLAN S2c: UE connects to WLAN/BBF with traffic routed to PDN GW via s2c.
- WLAN S2c (untrusted): UE connects to WLAN/BBF with traffic routed to PDN GW via ePDG and S2c.
- NS-WLAN Offload: UE connects to WLAN/BBF with traffic routed directly from BNG.
- Femto 3GPP routed: H(e)NB connected to BBF with traffic routed to PDN GW.

Rel-11 will cover QoS rule provisioning from the PCRF to the BNG for:

- Default QoS for fixed access session.
- Dynamic QoS for 3GPP UE connected to a fixed access.
- Dynamic QoS for fixed access session.

In this release dynamic QoS for fixed access session is considered only for session associated with an IP Address, layer 2 based sessions, i.e. session identified by layer 2 identity, e.g. VLAN Tag, are not considered in this 3GPP Release.

Editor's note: Support of 3GPP based charging for the fixed access session is FFS.

Editor's note: The interaction between Default QoS for fixed access session and dynamic QoS for 3GPP UE needs to be clarified.

Editor's note: The target of the work is to define the architecture and functionality for convergence in PCRF in an access agnostic way. Anyway support of access specific parameters will be considered as needed.

Editor's note: 3GPP will study and define the set of parameters sent by PCRF to the BNG for the provision of default QoS and dynamic QoS for the fixed access session. Such parameters will be anyway checked with BBF.

7.2 Architecture

Editor's note: This clause will identify the architectural requirements and assumptions as well as architecture common convergent network for building block III.

7.2.1 Requirements and assumptions

General assumptions:

- The definition of AAA functionality for authentication of the fixed access line (access line authentication) or fixed access session (e.g. PPPoE or IP Session) is out of scope of 3GPP.

General architectural assumptions:

- There is a direct interface between PCRF and BNG.
- The BNG is the policy enforcement point for QoS in the fixed access.

NOTE 1: How the BNG performs policy enforcement and binding if Gxd sessions with PPPoE or IP sessions in the BBF access is out of scope of 3GPP.

- More than one access session (e.g. a PPPoE session) can be supported per fixed access line (e.g. RG).

- A device connected to the R.G (e.g. VoIP phones) may also initiate an IP session.
- There is one IP-CAN session per fixed access session. It is assumed that each fixed access session is associated with one IPv4 address and/or one IPv6 prefix.

Architectural assumptions for "Default QoS parameters BBF":

- Default QoS applies per fixed access session.
- Default QoS includes the QCI and ARP according to TS 23.203 [4] and BBF requirements.

Editor's note: Whether additional parameters (e.g. Maximum Bit Rate UL/DL and Flow Filters) are included in Default QoS is FFS.

- The BNG shall be able to enforce policies and to perform the appropriate mapping from QoS parameters it receives from the PCRF to BBF specific parameters.

7.2.1.1 QoS Support at the Service Data Flow Level

It shall be possible to apply QoS control on a per service data flow basis in the BNG PCEF according to TS 23.203 [4] requirements.

7.2.1.2 Event-Trigger Provisioning and Detection

The BNG PCEF shall be able to detect event triggers provisioned by the PCRF.

Upon detection of an event the BNG PCEF shall request policy rules re-authorisation from the PCRF.

Editor's note: The list of applicable even triggers from TS 23.203 [4] plus additional BBF specific event-triggers is FFS

7.2.1.4 Charging

Editor's note: Charing requirements are for further study pending BBF's study of the impact of Gz/Gy interfaces on BNG.

7.2.2 Reference architecture

The converged network architecture for BB3 is shown in the following figures.

This architecture supports the scenario of a single network operator deploying both the 3GPP EPC and the BBF access network. Furthermore the architecture supports the roaming scenario between two PLMN operators.

The architectures in the following figures show only entities and interfaces that are in scope of the work and/or are impacted by BB3.

Editor's note: The impact, if any, for interworking between a fixed network supporting the BBF interworking solution defined in BB1 and BB2 and a HPLMN supporting the BBF convergent solution is FFS.

For support of 3GPP UE the BBF AAA proxy may be deployed as part of the BBF network. If the BBF AAA proxy is not present the SWa reference point is terminated on the BNG. In this release the BBF AAA server is used for fixed access session authentication and the SWa/STa is not applicable.

The fixed access device is only supported in non-roaming scenario. The reference interfaces S2c, SWu and SWn are not applicable for the fixed device.

In the figures the UE is shown to be connected with WLAN/BBF access, but it can be connected to H(e)NB as well for the case of traffic routed to EPC.

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.

Editor's note: The architecture for trusted WLAN with s2a is not considered in this release.

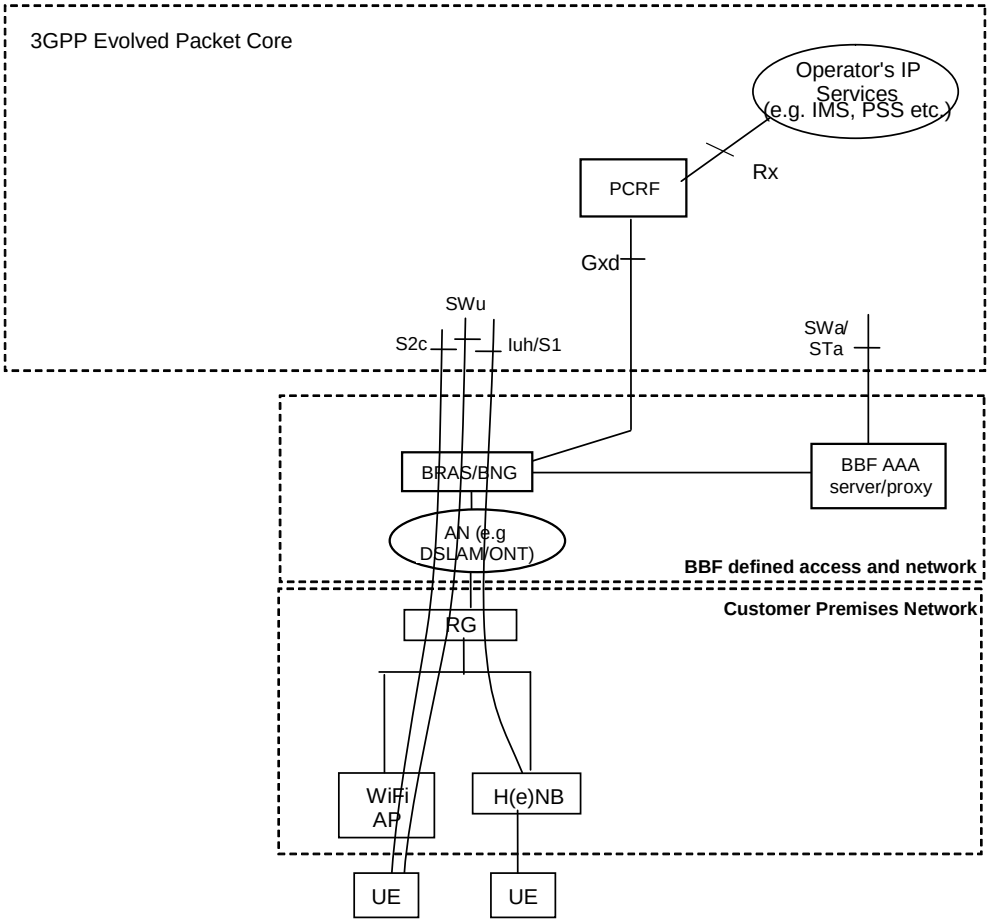


Figure 7.2.2-1: Non-Roaming Architecture for Fixed Broadband Access Interworking traffic routed to EPC domain (Converged PCRF)

In this architecture:

- PCRF provisions QoS Rules to BRAS/BNG over Gxd reference point.
- PCRF provisions PCC Rules to the PCEF in the PDN GW.

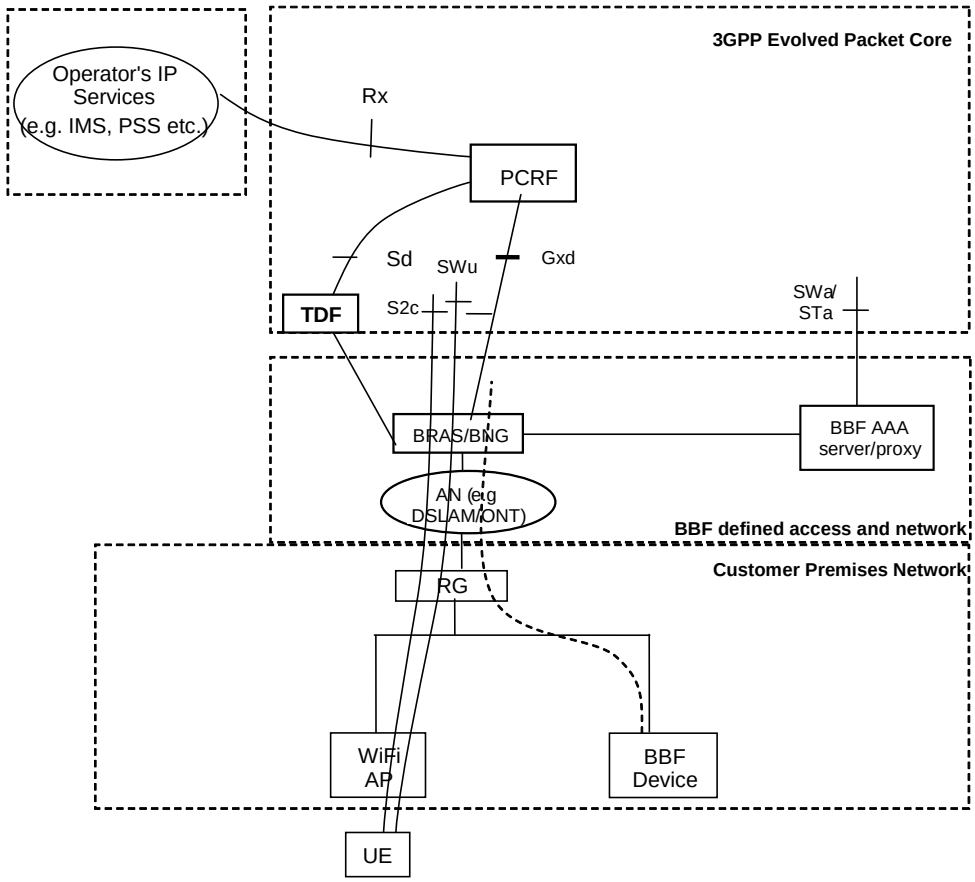


Figure 7.2.2-2: Non-Roaming Architecture for Fixed Broadband Access Interworking traffic offloaded to BNG (Converged PCRF)

NOTE 1: The dotted line from the BBF device represents plain IP traffic, for example towards the Internet.

In this architecture:

- PCRF provisions QoS Rules to BRAS/BNG.
- Both a UE and a BBF device may access Operator's IP services in the EPC or in the BBF defined network or both. Any extensions to Rx reference point to support a BBF AF are FFS.

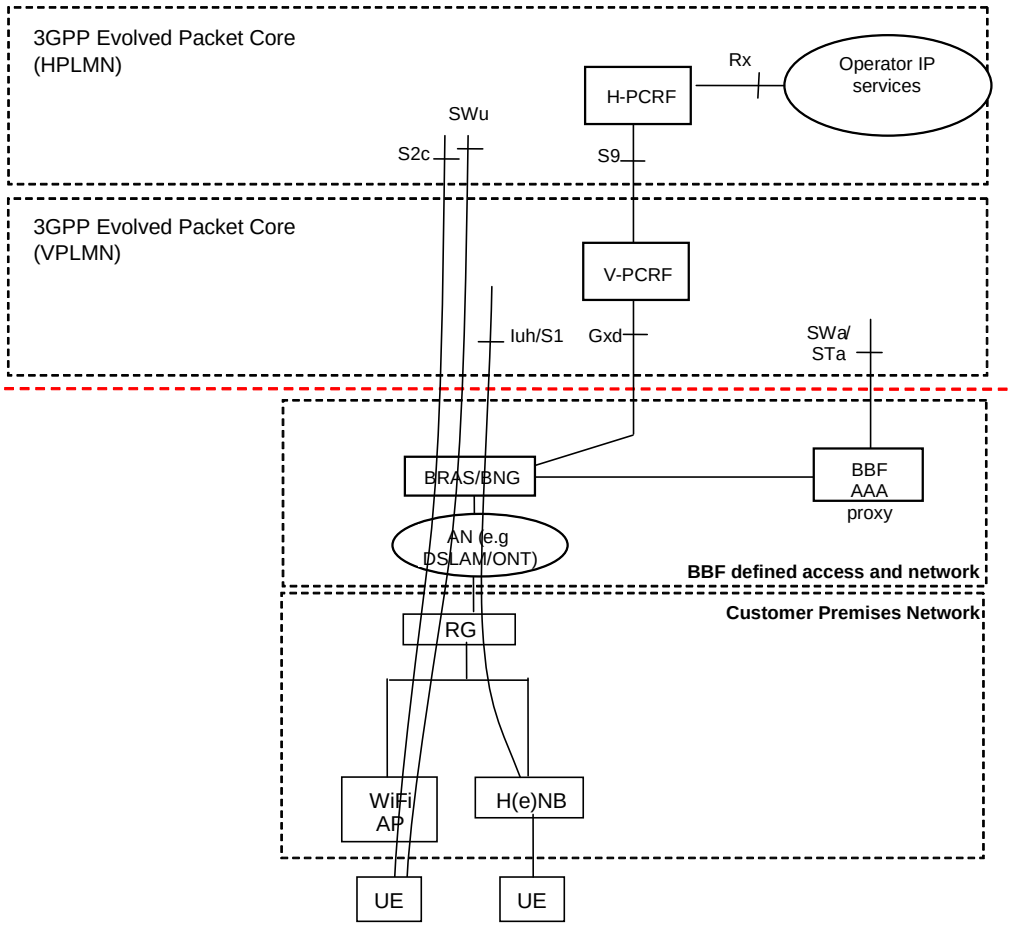


Figure 7.2.2-3: Roaming Architecture for Broadband access interworking traffic routed to EPC - Home routed traffic (Converged vPCRF)

NOTE 2: The SWu reference point is terminated on the ePDG, that can be located either in HPLMN or in VPLMN.

NOTE 3: For H(e)NB connections the Iu/S1 control plane terminates in the VPLMN network but the user plane is routed to the HPLMN.

In this architecture:

- vPCRF provisions QoS Rules to BRAS/BNG.
- hPCRF provisions PCC Rules to the PDN GW in EPC HPLMN domain.
- UE may accesses Operator's IP services in the EPC HPLMN.

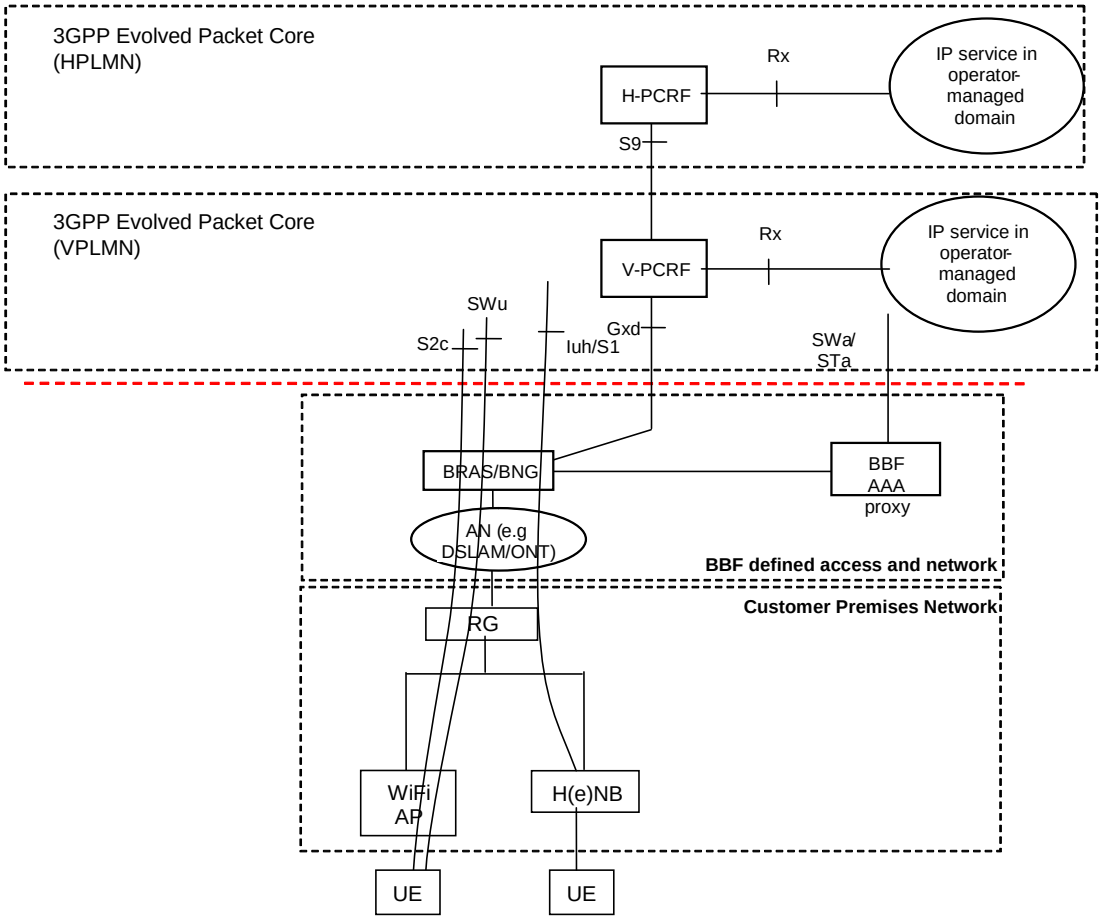


Figure 7.2.2-4: Roaming Architecture for Fixed Broadband Access Interworking traffic routed to EPC visited access case (Converged vPCRF)

NOTE 4: The SWu reference point is terminated on an ePDG located in VPLMN.

In this architecture:

- vPCRF provisions QoS Rules to BRAS/BNG.
- vPCRF provisions PCC Rules to the PDN GW in EPC VPLMN domain.
- UE may accesses Operator's IP services in the EPC HPLMN and or EPC VPLMN.

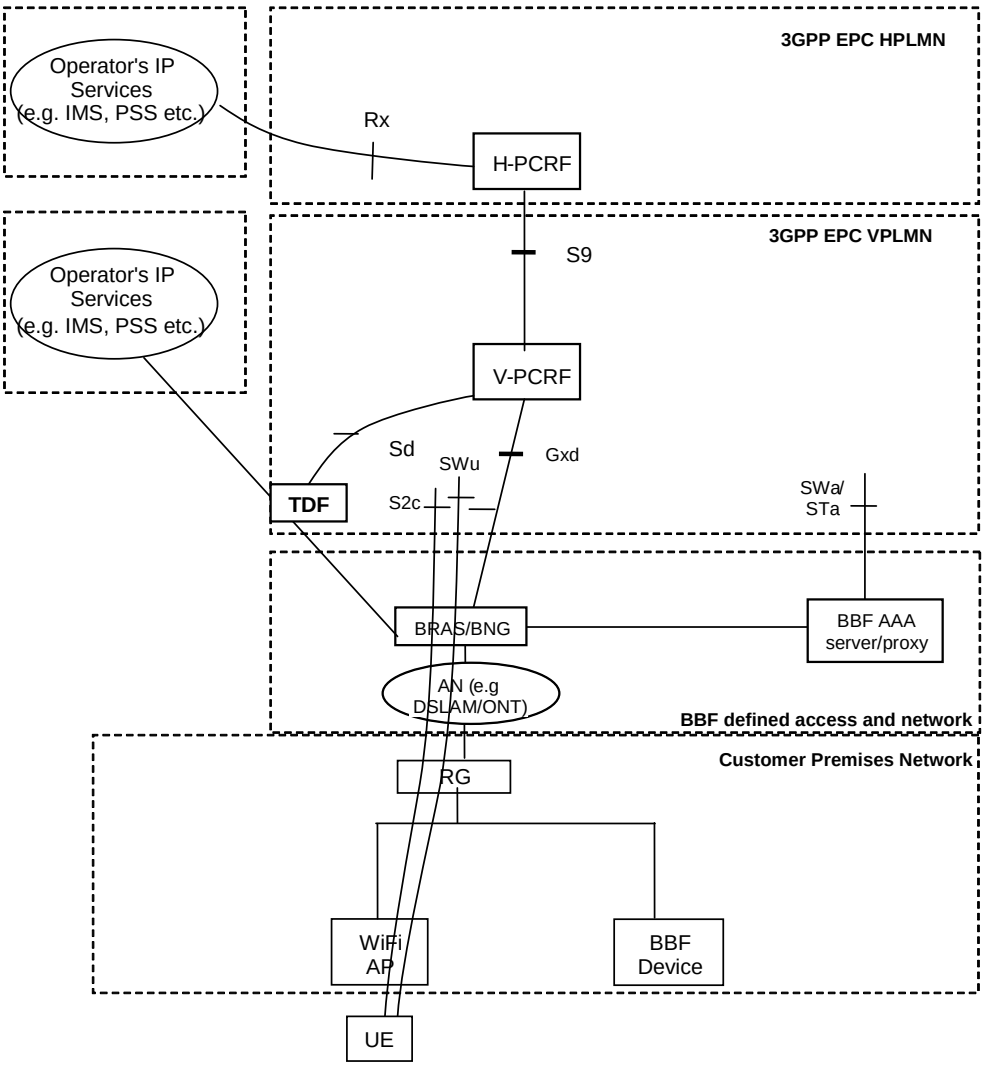


Figure 7.2.2-5: Roaming Architecture for Fixed Broadband Access Interworking traffic offloaded in BRAS/BNG (converged vPCRF)

In this architecture:

- vPCRF provisions QoS Rules to BRAS/BNG.
- Both a UE and a BBF device may accesses Operator's IP services in the EPC HPLMN and or EPC VPLMN or in BBF network.
- The TDF belongs to and is controlled by the VPLMN.
- Policies for roaming users may be locally configured in the vPCRF and/or TDF.

7.2.3 Network Elements

The 3GPP network elements are defined in details in TS 23.401 [2], TS 23.402 [3] and TS 23.203 [4].

7.2.3.1 PCRF

The PCRF functionality defined in TS 23.203 [4] shall apply. In addition, to support convergence between 3GPP and BBF network, the PCRF shall:

- Send the QoS rules to the BNG over Gxd interface for QoS control in the Fixed Broadband Access Network.

- for PCRF-initiated Gxd session establishment, send to the BNG the UE/H(e)NB local IP address and UDP port number to allow the Fixed Broadband Access to identify UE/H(e)NB traffic.
- for BNG-initiated Gxd session establishment, receive from the BNG the UE/H(e)NB local IP address and UDP port number.
- Be able to receive the UE local IP address and UDP source port from the ePDG (for S2c and PMIP-based S2b) and PDN GW (for GTP-based S2b).
- Be able to receive from the PDN GW the H(e)NB Local IP address and UDP source port for H(e)NB PS scenario.
- Be able to receive the HNB local IP address and UDP source port from HNB GW for the HNB CS scenario.

When PCRF receives the IP-CAN session establishment indication, PCRF determines if a Gxd session is already present for this IP-CAN session. If Gxd session is not already established, the PCRF shall trigger Gxd session establishment procedure towards the BNG. The PCRF identifies when the UE is connecting via Fixed Broadband access network from the IP-CAN type.

7.2.3.2 BNG

It is assumed that the BNG performs the function of PCEF as defined in TS 23.203 [4].

Editor's note: It is FFS whether the BNG can support 3GPP based charging function.

Specifically, it is assumed that the BNG:

- Receives from the PCRF the QoS rules for QoS control in the Fixed Broadband Access network;
- Requests the QoS rules to the PCRF for QoS control in the Fixed Broadband Access network;
- Terminates the Gxd session towards the PCRF;
- Enforces the QoS rules in the Fixed Broadband Access network and performs the appropriate mapping between 3GPP QoS parameters and BBF specific QoS parameters.
- Perform admission control in fixed access or delegates admission control decision to other BBF nodes. Based on the admission control, the BNG accepts or rejects the request received over Gxd.

NOTE: How the BNG performs QoS enforcement in the BBF access and mapping between 3GPP QoS parameters and BBF specific parameters is out of scope of 3GPP.

Editor's note: The assumption in this clause shall be checked with BBF.

7.2.3.3 ePDG

The ePDG functionality defined in TS 23.402 [3] shall apply. In addition, to support convergence between 3GPP and BBF network, the functionality defined in TS 23.139 clause 5.1.1.1 shall apply.

7.2.4 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 is defined in TS 23.203 [4].

Gxd For the purpose of convergence between 3GPP and BBF network it transfers QoS control policies from the Home PCRF to the BNG in non-roaming scenario and from the Visited PCRF to the BNG in roaming scenario.

Gxb* For purpose of convergence between 3GPP and BBF network the same extension defined in TS 23.139 clause 5.2 are applicable

S2b For purpose of convergence between 3GPP and BBF network the same extension defined in TS 23.139 clause 5.2 are applicable

SWa For purpose of convergence between 3GPP and BBF network the same extension defined in TS 23.139 clause 5.2 are applicable

STa For purpose of convergence between 3GPP and BBF network the same extension defined in TS 23.139 clause 5.2 are applicable

The Reference points within the BBF access network are defined in BBF TR 058 [7], BBF TR-101 [8], BBF WT 145 [10] and BBF WT-134 [11] and they are considered out of the scope of 3GPP. Any enhancement of reference points within the BBF access network for supporting convergence scenario is out of the scope of 3GPP.

Editor's note: It is FFS whether Gxd is Gx or an enhancement of Gx.

Editor's note: It is FFS whether S9 requires enhancements for supporting BBF convergent scenario.

7.2.4.1 Gxd Reference Point

The Gxd reference point resides between the BNG PCEF and the PCRF.

The Gxd reference point enables a PCRF to have dynamic control over the PCC behaviour at a PCEF.

The Gxd reference point enables the signalling of PCC decision and it supports the following functions:

- Request for PCC decision from BNG/PCEF to PCRF;
- Provision of PCC decision from PCRF to BNG/PCEF;
- Termination of Gxd session by BNG/PCEF or PCRF.

A PCC decision consists of zero or more PCC rule(s) and IP-CAN attributes.

7.3 Convergent Policy and QoS

Editor's note: This clause will identify the requirements and assumptions for convergent Policy and QoS for WLAN and 3GPP H(e)NB for Home routed and LBO traffic and for NS-WLAN offload traffic.

7.3.1 Policy and charging control rule

For convergent purpose the definition of PCC rules in clause 6.3 of TS 23.203 [4] are applicable with the modification describe in this clause.

NOTE 1: The procedure for provisioning predefined PCC rules is out of scope for this TS.

Table 7.3.1-1 lists the information contained in a PCC rule applicable to convergent scenario on Gxd reference point. The definition of information contained in PCC rules in clause 6.3 of TS 23.203 [4] shall apply to convergent scenario.

Editor's note: Whether the charging related parameters including those for Sponsored data connectivity and Usage Monitoring Control are included, is FFS.

Editor's note: Whether information elements can be deleted and/or added to the QoS rules for BBF access, is FFS.

Table 7.3.1-1: The PCC rule information

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the BNG	Applicable for (H(e)NB, WLAN, fixed BBF ,All
Rule identifier	See table 6.3 TS 23.203 [4]	Mandatory	no	All
Service data flow detection	This clause defines the method for detecting packets belonging to a service data flow.			All
Precedence	See table 6.3 TS 23.203 [4]	Mandatory	yes	All
Service data flow template	See table 6.3 TS 23.203 [4]	Mandatory	yes	All
Policy control	This clause defines how the BNG shall apply policy control for the service data flow.			All
Gate status	See table 6.3 TS 23.203 [4]		Yes	Fixed BBF Device, NSWO
QoS class identifier	See table 6.3 TS 23.203 [4]	Mandatory	Yes	All
UL-maximum bitrate	See table 6.3 TS 23.203 [4]	Conditional (NOTE 1)	Yes	All
DL-maximum bitrate	See table 6.3 TS 23.203 [4]	Conditional (NOTE 1)	Yes	All
UL-guaranteed bitrate	See table 6.3 TS 23.203 [4]		Yes	All
DL-guaranteed bitrate	See table 6.3 TS 23.203 [4]		Yes	All
ARP	See table 6.3 TS 23.203 [4]	Conditional (NOTE 2)	Yes	All
NOTE 1: Mandatory when policy control on SDF level applies. NOTE 2: Applicable per BBF WT-134 requirements.				

7.3.2 Gating

The Gate Function enables or disables the forwarding of service data flow packets. A gate is described within a policy rule. The rule shall describe if the possible uplink and possible downlink gate is opened or closed.

Opening or closing the gate shall lead to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed all packets of the related IP flows shall be dropped. If the gate is opened the packets of the related IP flows are allowed to be forwarded.

The gate function is applicable for fixed BBF device and NSWLAN offload service data flows.

7.3.3 PCRF discovery and selection

For BBF access session the BNG discovers and selects the PCRF following the principles defined in TS 23.203 [4] clause 7.6 and Annex P. The BNG finds the DRA based on the Subscriber-ID, for example Access Line Identifier (Logical Access ID and Physical Access ID) or BBF identity, with the role of UE ID and the Local IP addressed assigned to the BBF access session. The PDN connection ID is not applicable to IP-CAN session for BBF access. The roaming scenario is not applicable to BBF access session.

7.4 Procedures for fixed access

Editor's note: This clause will identify the requirements and assumptions for convergent Policy and QoS for fixed line session.

7.4.1 General

For the dynamic QoS for fixed access session the following requirements shall be supported:

- interaction between PCRF and BNG with session establishment.
- policy change requests originated from Applications Function after session establishment.
- policies apply to individual fixed access sessions.
- policy evaluation is triggered by the change in state of an fixed access session.

The following scenario are not considered for support in PCC in this Release:

- policies that apply to aggregates of subscriber sessions sharing logical interfaces and/or layer 2 interfaces and/or physical access e.g. DSL loop.
- policies that apply to logical interface/layer 2 interface based on individual subscriber session policies when a logical interface and/or layer 2 interfaces and/or physical access e.g. DSL loop, is shared among subscriber sessions belonging to multiple subscribers.

For a fixed access session, the IP-CAN session is represented by the association between a fixed line or subscriber of BBF access network and an IP address assigned to the session.

7.4.2 Provisioning Default QoS for fixed access session

Default QoS is installed in the BNG as part of the access session setup as follows:

1. Upon RG activation, the access session is authenticated by the BBF AAA. As part of this, the BBF AAA may provide Default QoS to the BNG.

NOTE 1: The previous step is defined by BBF and is out of the scope of 3GPP.

NOTE 2: The IP address for the fixed access session to the RG or to fixed device is assigned in case of successful authentication.

Editor's note: Accounting procedure is not considered in above step and left FFS.

2. Once the access session has been authenticated, the BNG initiates the PCRF session. If the BNG received Default QoS from the BBF AAA, it also forwards this Default QoS to the PCRF.
3. The PCRF sends Default QoS to the BNG.

NOTE 3: The PCRF may override the QoS received from the BNG / BBF AAA.

Editor's note: The definition of parameters included in Default QoS for fixed access session is FFS. Such parameters will be checked with BBF.

7.4.2 IP-CAN Session Establishment

This clause describes the signalling flow for Gxd IP-CAN Session establishment. The session is initiated after the BBF device has been authenticated and assigned an IP@ per BBF specifications that out of scope in 3GPP.

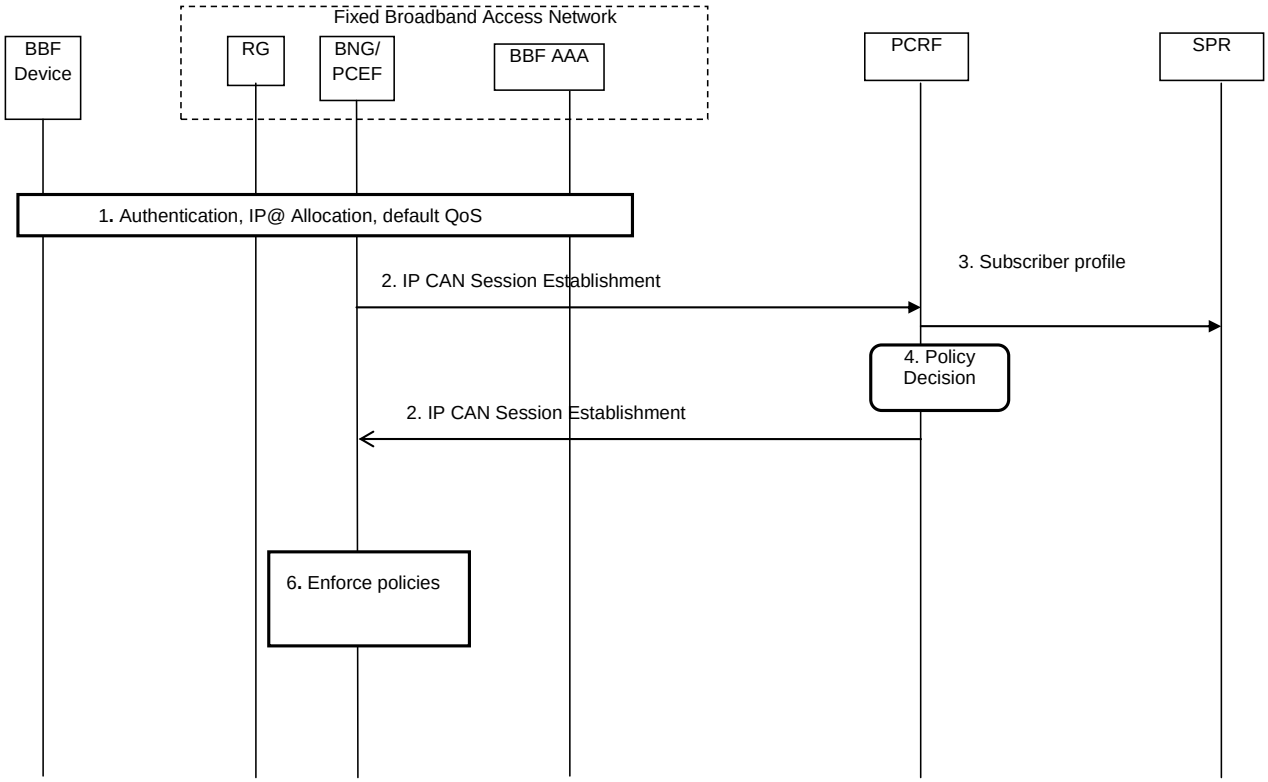


Figure 7.4.2-1: BBF Device Initial Attach

1. BBF device, e.g. by RG initiates a BBF access session. The BBF access line authentication is performed as specified by BBF. As part of this step, the BBF AAA may provide Default QoS to the BNG. The BNG assigns the IP address to the BBF device. This step is BBF specific and as such out of scope of this specification.

2. The BNG/PCEF triggers the establishment of the IP-CAN session with the PCRF. The message includes the subscription-ID, the Access Line Identifier (physical and logical circuit ID), default QoS, if available, the IP-CAN type, the IPv4 address and/or the IPv6 network prefix and subscribe priority per WT-134 and WT-146 requirements.

3. The PCRF obtains the subscriber's profile related to the BBF device.

Editor's note: Enhancements to the subscriber profile for BBF access is FFS.

4. The PCRF makes policy decision and derives QoS rules. The PCRF may change the default QoS of the subscriber it received from the PCEF. In this step the PCRF sends the decision(s) to the BNG. The PCRF may include the following information: Default QoS, the QoS Rules and the Event Triggers to report. The Event Triggers indicate to the BNG what events must be reported to the PCRF.

5. The PCRF provisions the QoS rules at the PCEF.

6. This step is BBF specific. The BNG communicates with other network elements in the BBF access network per BBF specifications.

Editor's note: Whether additional parameters are required for BBF access session is FFS.

7.4.3 PCRF Initiated IP-CAN Session Modification

This clause is related to IP-CAN session modification for BBF access session initiated by PCRF. The AF can be involved.

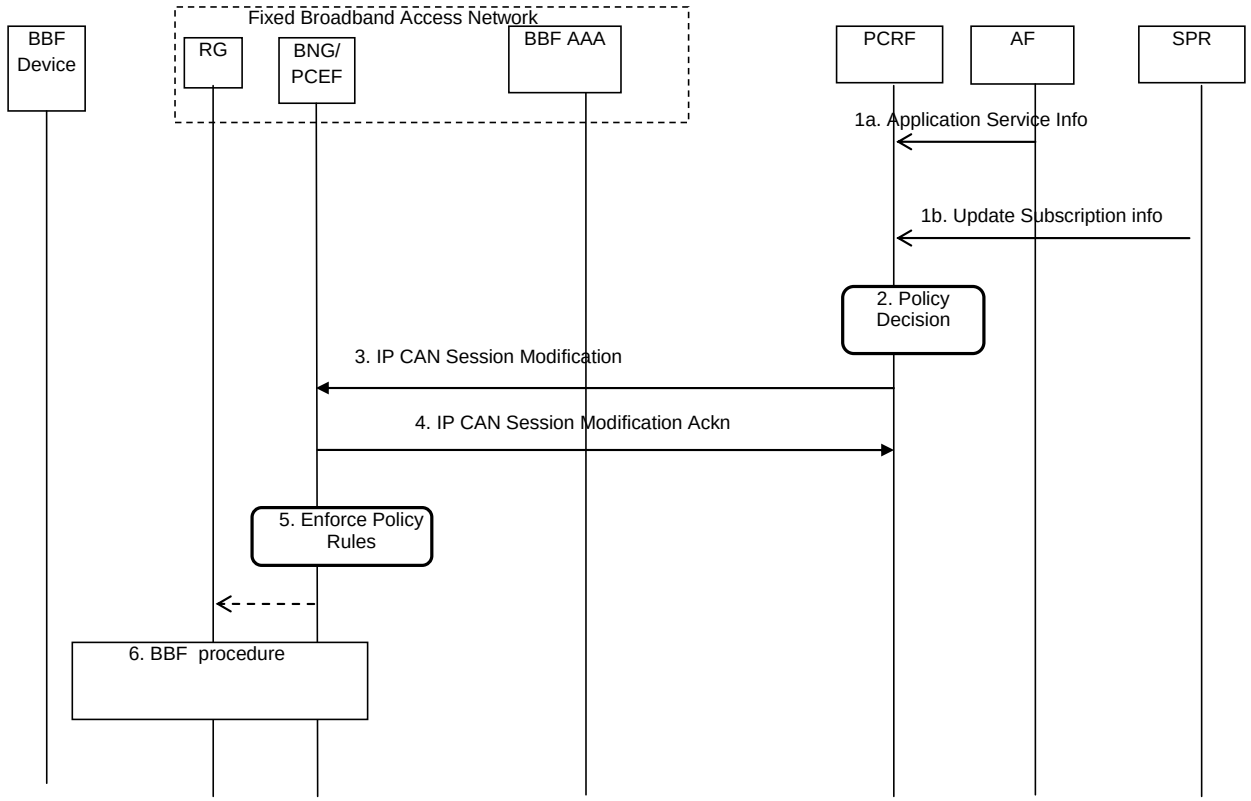


Figure 7.4.3.-1: PCRF initiated IP-CAN Session Modification

1a. The AF requests QoS resource authorization. The request includes the bandwidth requirements, media type, session priority and other information according to TS 23.203 [4].

Editor's note: Rx specific enhancements for BBF AF are FFS.

1b. The SPR notifies the PCRF when the user's profile changes.

Alternatively, the PCRF may initiate this procedure based on PCRF internal logic.

Editor's note: Enhancements to the subscriber profile for BBF access is FFS.

2-3. the PCRF makes policy decisions and determines the QoS rules (QCI, UL/DL max/minimum or guarantee Bitrate and priority for the service) and the Event Triggers to report. The Event Triggers indicate to the BNG what events must be reported to the PCRF.

Editor's note: Whether additional parameters are required for BBF access session is FFS.

4. The BNG/PCEF responds with an acknowledgment.

5. The BNG/PCEF enforces the QoS rules.

NOTE 1: How the BNG performs QoS enforcement in the BBF is out of the scope of 3GPP.

NOTE 2: The BNG performs the mapping between the QoS rules and the parameters specific in BBF network.

6. The BNG communicates with other entities in BBF access per BBF specifications.

7.4.4 BNG/PCEF Initiated IP-CAN Session Modification

This clause is related to IP-CAN session modification for BBF access session initiated by BNG. The procedure is applicable when the BNG makes a decision to request a modification of QoS rules. The trigger to start the modification procedure by BNG can be a provisioned event-trigger by the PCRF or a BBF specific trigger.

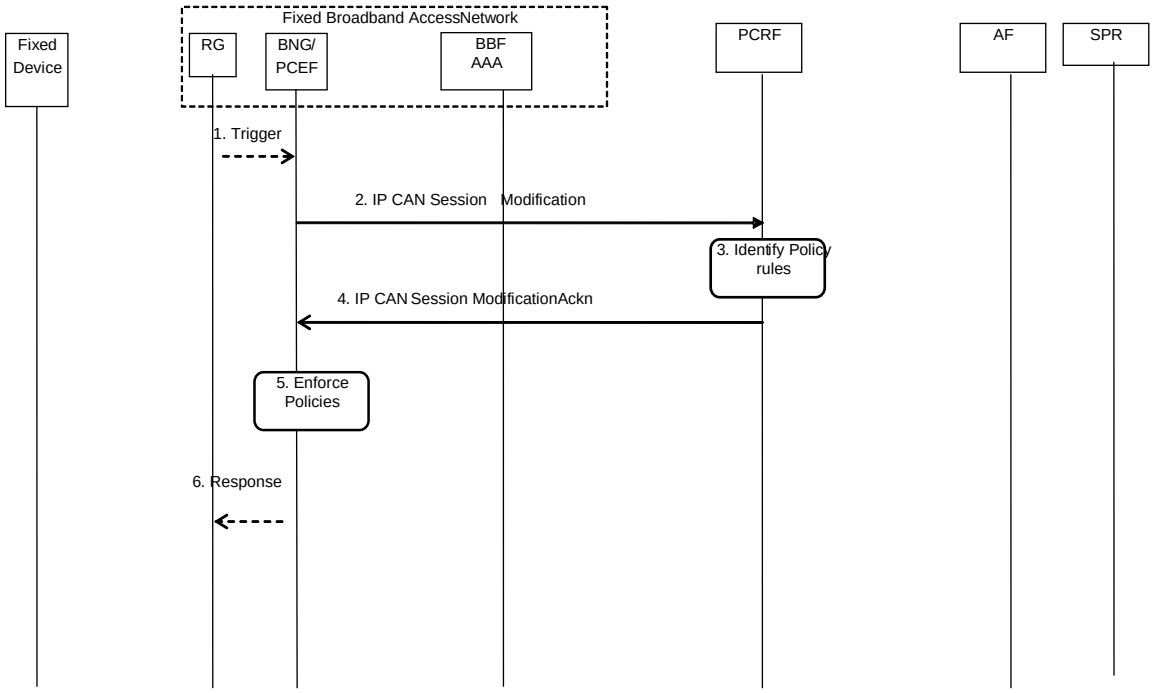


Figure 7.4.4-1: BNG/PCEF IP-CAN Session Modification

1. The BNG may receive a trigger to modify an access session due to partial network failure, failure to enforce a QoS rule or other BBF specific triggers per BBF specification that are out of scope of 3GPP.
2. The BNG may initiate the session modification procedure based on internal triggers or when event-triggers provisioned by the PCRF are detected. The message includes the Event Report and affected QoS Rules.
3. The PCRF makes policy decisions and derives new or modified QoS rules.

Editor's note: Whether additional parameters are required for BBF access session is FFS.

4. The PCRF provisions QoS rules at the BNG/PCEF.
5. The BNG/PCEF enforces the QoS rules.

NOTE 1: How the BNG performs QoS enforcement in the BBF is out of the scope of 3GPP.

NOTE 2: The BNG performs the mapping between the QoS rules and the parameters specific in BBF network.

6. The BNG/PCEF may respond to the session modification trigger per BBF specification.

7.4.5 BNG/PCEF initiated IP-CAN Termination

This clause is related to termination of the IP-CAN session for BBF access session initiated by BNG. The procedure is applicable when BBF access session is terminated, the trigger for start the termination by BNG is BBF specific (e.g. RG switch off, PPPoE session termination, etc) and out of the scope of 3GPP.

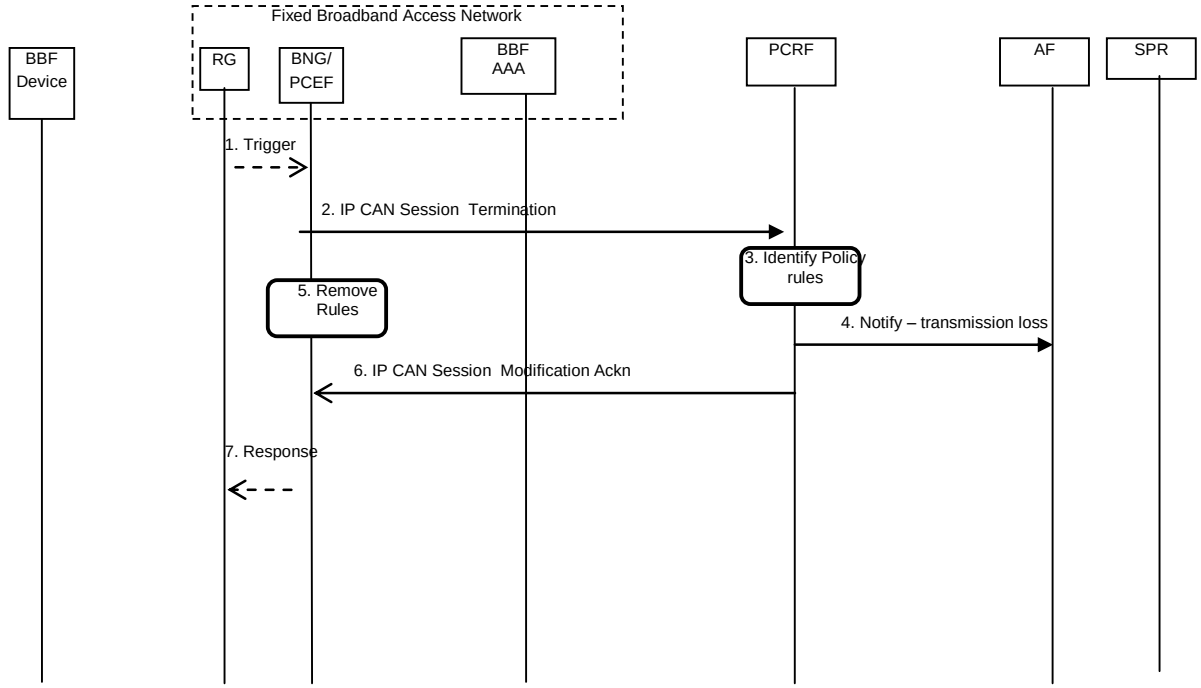


Figure 7.4.5-1: BNG/PCEF Initiated IP-CAN Session Termination

1. The BNG/PCEF receives a request to terminate the session with the PCRF based on BBF triggers (both external and internal to the BNG) for example due to termination of session, power off of RG, etc.

NOTE 1: How the BNG detects or is informed that BBF access session is terminated is BBF specific and is out of the scope of 3GPP.

2. The BNG/PCEF initiates the IP-CAN Session termination procedure.

3. The PCRF identifies the affected rules.

4. The PCRF notifies the AF about loss of transmission.

5. The BNG/PCEF removes the rules.

6. The PCRF acknowledges the termination of the session.

7. The BNG/PCEF responds to the session termination request per BBF specifications.

7.4.6 Update of the subscription information in the PCRF

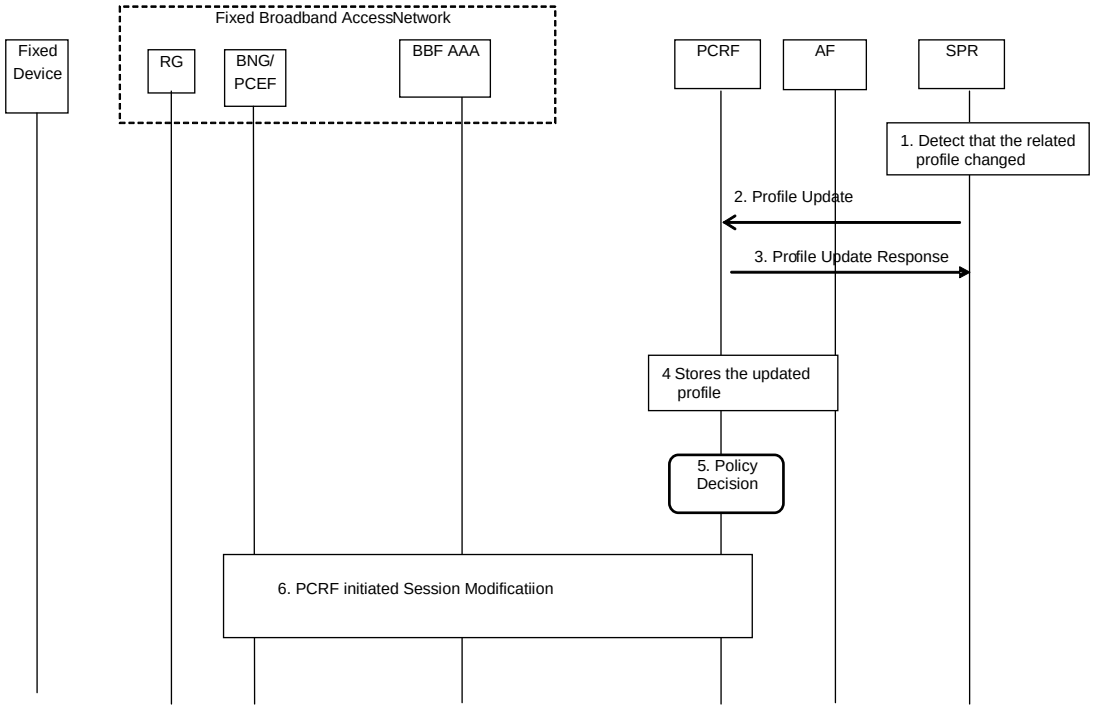


Figure 7.4.6-1: Update of the subscription information in the PCRF

1) The SPR detects that the subscriber's profile changed.

Editor's note: Enhancements to the subscriber profile for BBF access is FFS

2) The SPR notifies the C-PCRF of the profile change provided the C-PCRF subscribes to notification event(s).

3) The PCRF responds to the SPR notification message.

4) The PCRF stores the updated profile.

5) The PCRF indentifies the rules affected and derives new/modified ones.

6) The PCRF initiates the IP-CAN Session Modification procedure per clause towards the BNG PCEP if BBF access or 3GPP UEs are affected.

7.5 Procedures for WLAN

Editor's note: This clause will identify the procedures for traffic when the UE attaches via WLAN.

7.5.1 Functional Description and Procedures for Fixed Broadband Access network over untrusted S2b

Editor's note: This clause will identify the procedures for traffic when the UE attaches via WLAN with untrusted s2b.

7.5.2 Functional Description and Procedures for Fixed Broadband Access network over trusted S2c

Editor's note: This clause will identify the procedures for traffic when the UE attaches via WLAN with trusted s2c.

7.5.3 Functional Description and Procedures for Fixed Broadband Access network over untrusted S2c

Editor's note: This clause will identify the procedures for traffic when the UE attaches via WLAN with untrusted s2c.

7.5.4 Functional Description and Procedures for Non-seamless WLAN offload

Editor's note: This clause will identify the procedures for Non-seamless WLAN offloaded traffic.

7.6 Procedures for 3GPP H(e)NB connected to BBF access

Editor's note: This clause will identify the procedures for traffic when the UE attaches via 3GPP H(e)NB.

8 P4C Building blocks II: Policy and Charging Control for 3GPP UE terminals connected to Broadband Forum access network as Trusted network in Interworking scenario

Editor's note: This clause will contain items being part of Building Block 2 P4C-TI.

8.1 Architectural requirements and assumptions

Editor's note: This clause will identify the architectural requirements and assumptions for P4C Building Block 2 (P4C_TI).

8.1.1 General architecture assumptions

General architectural assumptions:

- 3GPP-based access authentication as defined in TS 33.402 is mandatory to be performed for Trusted WLAN access.
- The high-level functions of Trusted WLAN access are described in TS 23.402 [3].

General architecture assumptions on BBF access network:

- The IP Edge is the policy enforcement point for QoS in the fixed access network.
- The BBF network element shall be able to perform the appropriate mapping from 3GPP mobile QoS parameters to BBF specific parameters.

Editor's note : The assumptions listed above shall be verified with BBF.

Editor's note : Whether any further enhancement or modification requirement for Trusted WLAN access to support P4C-TI is FFS and needed to be consulted with BBF.

8.2 Key issues

Editor's note: This clause will identify the key issues for P4C Building Block 2.

8.2.1 Key Issue 1 - How to provide location information for Policy and Charging Control

Charging and Policy were not thoroughly defined as part of SaMOG Rel-11.

In order to ensure proper Charging data collection and Policy control at the PGW (for user charging/policy control/statistics purpose), when EPC services are accessed over a TWAN, following information needs to be transferred to the PGW:

- The network identity.
- The location of the AP.
- Optionally, additional information such as geo-location.

8.3 Alternative Solutions

Editor's note: This clause will describe the alternative solutions for P4C Building Block II, if more than 1 solution will be proposed.

8.3.1 Alternative 1 - GTP Based S2a Solution

8.3.1.1 General principles

Editor's note: This clause will describe the general principles for alternative 1 for P4C Building Block 2.

The architectural assumptions for this solution alternative are:

- The S2a interface terminates at the TWAG.
- The architecture is compatible with trusted WLAN Access Network as defined in TS 23.402 [3], clause 16.
- For EPC-routed traffic the accounting is performed by PDN GW, (so no need to send charging rules to TWAG/IP edge).
- If the S2a reference point is an inter-operator interface then same security consideration applies as for the STa interface.
- According to TS 23.402 [3] clause 16, the GTP-C protocol carries over S2a the QoS requirements associated with the IP flows carried by the S2a bearers. From this the BBF access may:
  - Determine the relevant BBF QoS policies that are to apply to the IP flows exchanged on this PDN connection.
  - Perform, where necessary, resource and admission control.
- Admission control is a function of the BBF defined network and is out of scope of 3GPP
- The BBF network shall be able to perform the appropriate mapping between the EPS Bearer QoS parameters received via GTP based S2a interface and the QoS parameters used in Fixed Broadband access.
- The details of the mapping from EPS Bearer QoS parameters on S2a to QoS parameters applicable in the BBF domain are out of scope of 3GPP.

Editor's note: When the BBF network can not sustain the QoS requested over S2a, whether a report or notification mechanism initiated from BBF network is needed for GTP based S2a solution is FFS.

Editor's note: The above assumptions needs to be verified with BBF, where applicable.

8.3.1.2 Reference architecture

Editor's note: This clause will describe the reference architecture for Non-roaming and for roaming scenario for alternative 1 for P4C Building Block II.

The Interworking network architecture for the BB2 solution based on GTP based S2a is shown in the following figures.

This architecture addresses the scenario where the 3GPP EPC and the BBF access network are operated by different administrative entities. Furthermore the architecture supports the roaming scenario between two PLMN operators.

Editor's note: The same solution can also be applied to scenario of a single network operator deploying both the 3GPP EPC and the BBF access network. See TR 23.839.

The architectures in the following figures show only entities and interfaces that are in scope of the work and/or are impacted by BB2.

Admission control is a function of the BBF defined network and may involve BBF entities not shown in the architecture figures below, e.g. BPCF.

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: Both TWAN and IP Edge integrated and TWAN and IP Edge standalone cases are supported and are represented by the following architectures.

Editor's note: The TWAG and IPEdge standalone case needs further clarification depending on ongoing BBF work.

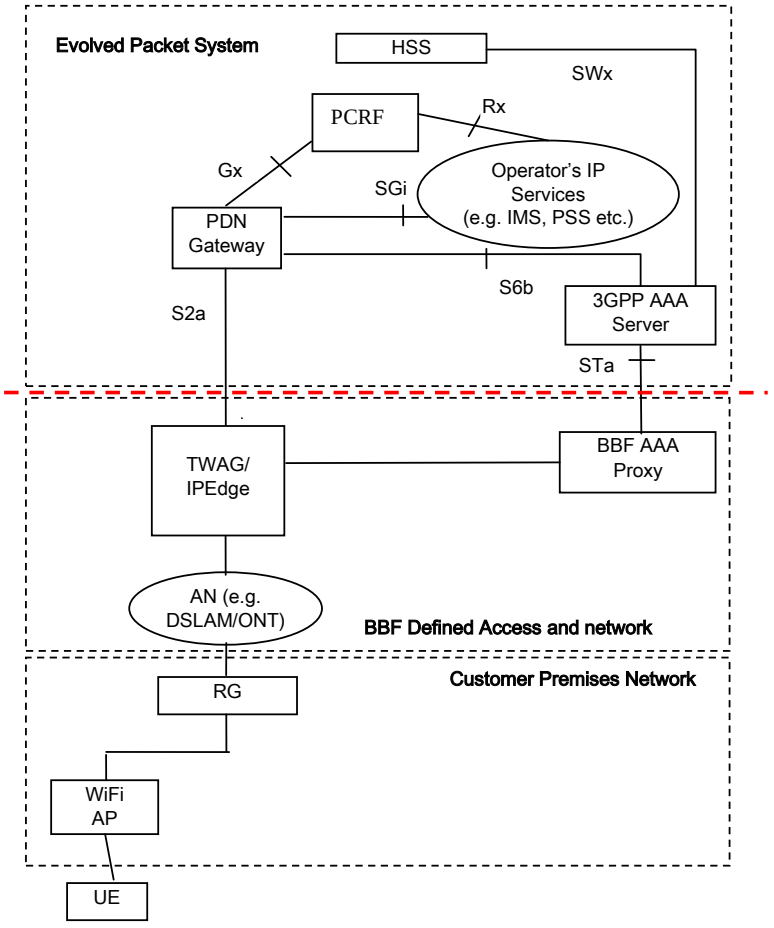


Figure 8.3.1.2-1: Non-Roaming Architecture

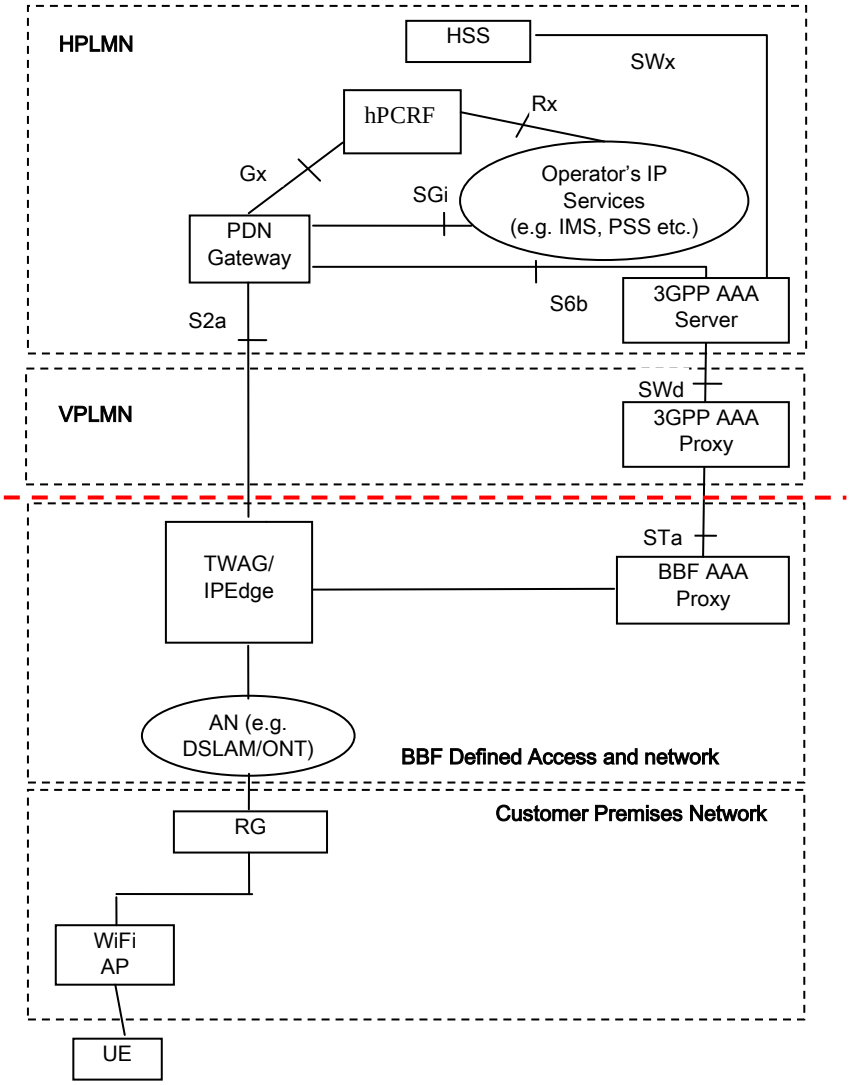


Figure 8.3.1.2-2: Roaming Architecture - Home Routed

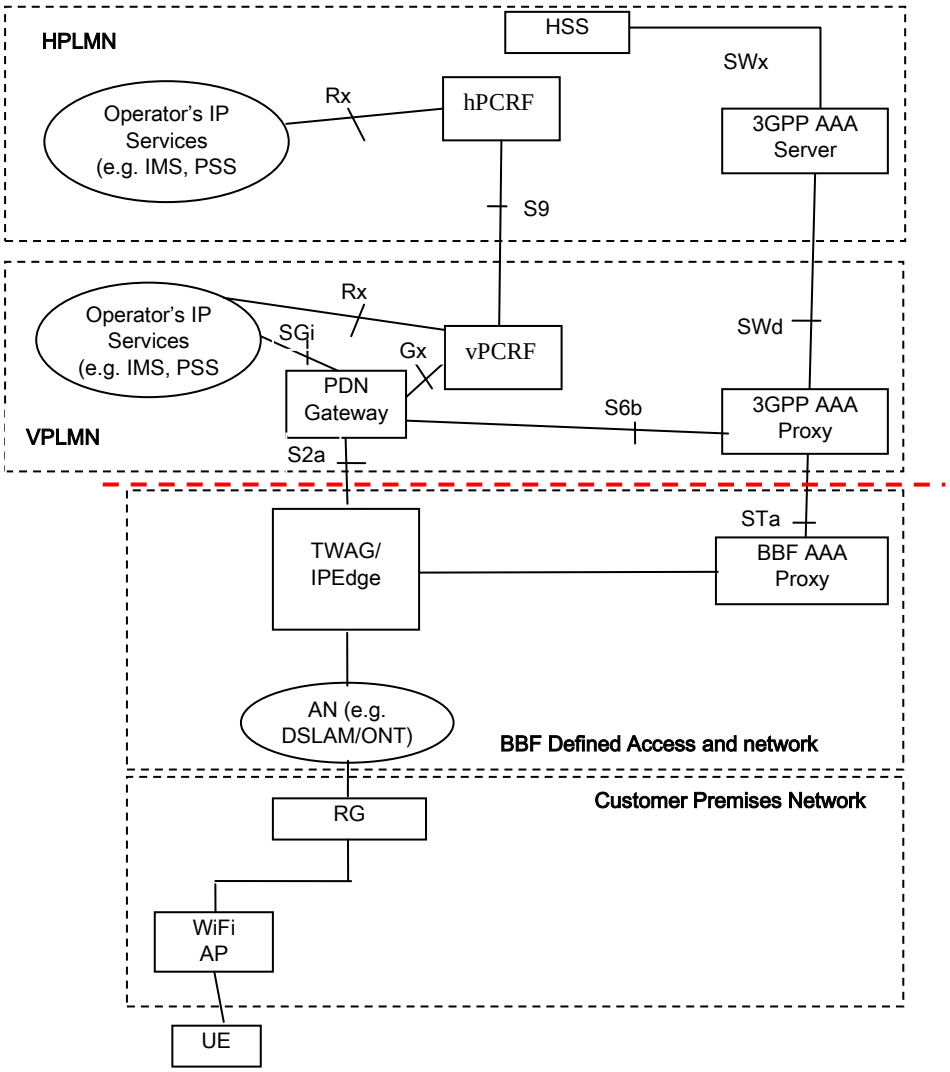


Figure 8.3.1.2-3: Roaming Architecture - Local Break Out

8.3.1.3 Reference points

Editor's note: This clause will describe the reference points of architecture for roaming for alternative 1 for P4C Building Block II.

S2a For the purpose of Interworking between 3GPP and BBF networks it transfers QoS information from the PDN GW to the TWAG.

Editor's note: It is FFS whether S2a needs enhancement or not.

8.3.1.4 Policy and QoS

Editor's note: This clause will identify the requirements and assumptions for Policy and QoS for P4C Building Block II.

8.3.1.4.1 General assumptions

This solution is based on the S2a bearer model described in TS 23.402 [3], clause 16.1.6. An S2a bearer uniquely identifies traffic flows that receive a common QoS treatment.

In case TWAG and IP Edge are not co-located, it is assumed that QoS parameters can be transferred from TWAG to IP Edge. How this is done is out of scope to 3GPP.

8.3.1.4.2 Location information provided over S2a-GTP to PGW,

In order to ensure proper Policy control and charging data collection at the PGW (for user charging/statistics purpose), when EPC services are accessed over a TWAN, following information needs to be transferred to the PGW:

- The SSID used by the UE: an operator may allocate a SSID to a collection of AP supporting the access to its EPC services and wish to apply a specific tariff or QoS to an EPC session when this session is supported over such SSID.
- BSSID (MAC address of the AP) as an indication of the actual AP having been used: this information may be collected to apply a specific tariff or the QoS depending on the actual AP or for statistical purposes. It corresponds to the common situation where an operator may re-use the same SSID in different hotspots.

The solution shall allow the PGW to receive from the TWAN and then forward to the PCRF/OCS/OFCS the following information:

- the SSID used by the UE to reach the EPC.
- the BSSID (MAC address of the AP).

In addition, the solution, based on agreement between the 3GPP and the BBF/FBB networks, may also allow the TWAN to send to the PGW, and the PDN GW to forward to the PCRF/OCS/OFCS, the following information:

- More detailed geographical information such as geo-location of the AP being used.

Editor's note: Whether the TWAN can provide these information elements to the PGW is to be clarified by BBF.

Editor's note: The geographical information for charging support is defined by SA WG5.

8.3.1.5 Procedures

Editor's note: This clause will identify the procedures for Policy and QoS in TS 23.402 [3] and/or TS 23.203 [4] style for P4C Building Block II.

The procedures described in this clause are based on the procedures defined in TS 23.402 [3], clause 16. The only difference compared to the procedures described in TS 23.402 [3] clause 16 is that the TWAN used in TS 23.402 [3] is replaced by the BFF defined network.

8.3.1.5.1 Initial Attach in WLAN on GTP S2a

This procedure is the same as in TS 23.402 [3], clause 16.2.1 with the following clarifications:

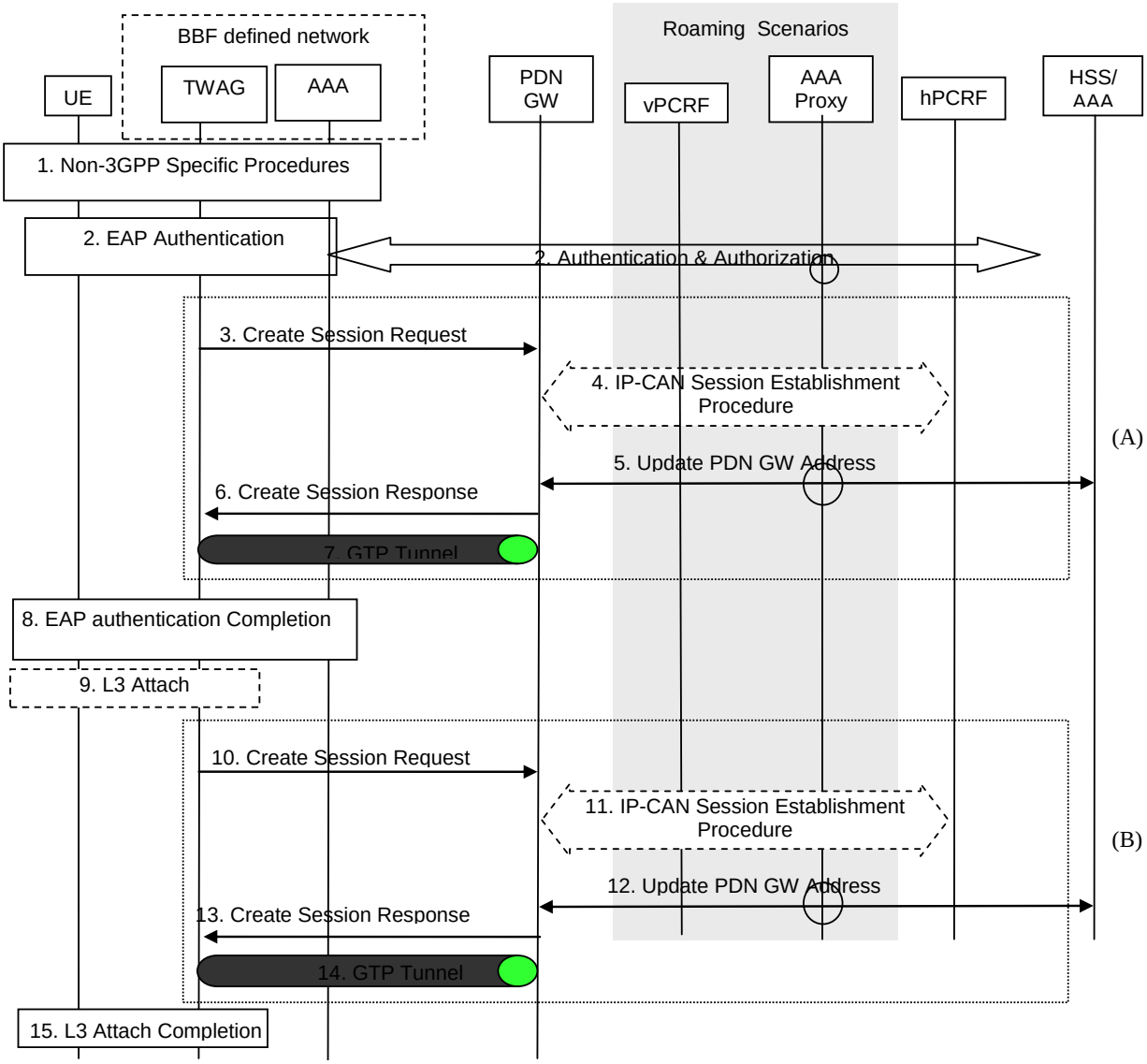


Figure 8.3.1.5.1-1: Initial attachment in WLAN on GTP S2a for roaming, LBO and non-roaming scenarios

The steps in this call flow are the same as in TS 23.402 [3], clause 16.2.1 with the following clarifications:

Steps 6 and 13: These steps include the default S2a bearer EPS Bearer QoS. The BBF defined network uses this EPS bearer QoS to determine the relevant BBF QoS policies that are to apply to the IP flows exchanged on this S2a bearer.

8.3.1.5.2 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

This procedure can be used to deactivate an S2a dedicated bearer or deactivate all S2a bearers belonging to a PDN address, for e.g., due to IP-CAN session modification requests from the PCRF. If the default S2a bearer belonging to a PDN connection is deactivated, the PDN GW deactivates all S2a bearers belonging to the PDN connection.

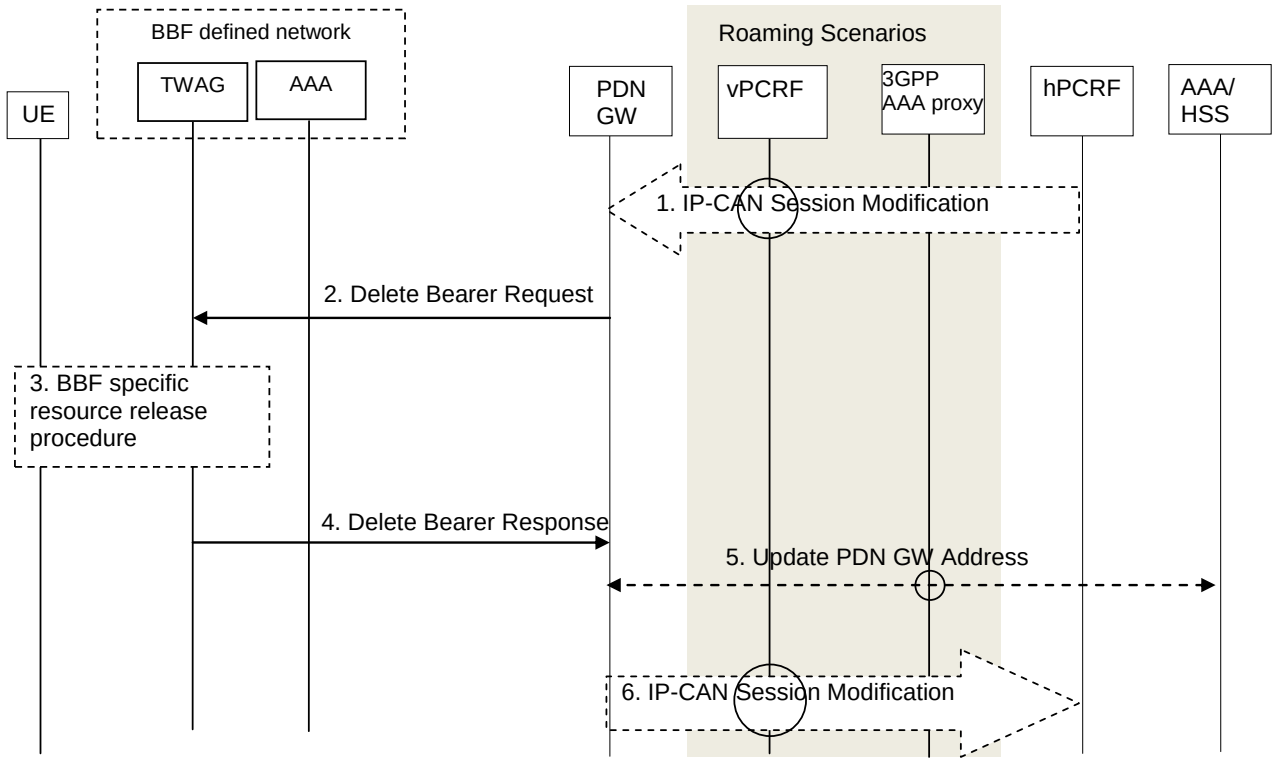


Figure 8.3.1.5.2-1: PDN GW Initiated Bearer Deactivation with GTP on S2a

This procedure applies to the Non-Roaming, Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the non-roaming and home routed roaming cases, the vPCRF is not involved at all.

The optional interaction steps between the PDN GW and the PCRF in the procedures in figure 8.3.1.5.3-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured within the PDN GW.

1. This step is the same as step 1 in TS 23.402 [3], clause 16.4.1

2. The PDN GW sends a Delete Bearer Request message (EPS Bearer Identity, Cause) to the TWAG. This message can include an indication that all bearers belonging to that PDN connection shall be released.

3. BBF specific resources may be released in the Fixed Broadband access. The details of this step are out of the scope of 3GPP.

4. The TWAG deletes the bearer contexts related to the Delete Bearer Request, and acknowledges the bearer deactivation to the PDN GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

5. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server/HSS of the PDN disconnection.

6. The PDN GW deletes the bearer context related to the deactivated S2a bearer. If the dedicated bearer deactivation procedure was triggered by receiving a PCC decision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision was successfully enforced by completing the PCRF-initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], proceeding after the completion of IP-CAN bearer signalling.

8.3.1.5.3 Dedicated bearer activation in WLAN on GTP S2a

This procedure is based on the dedicated bearer activation procedure for GTP based S2a is described in TS 23.402 [3] clause 16.5.

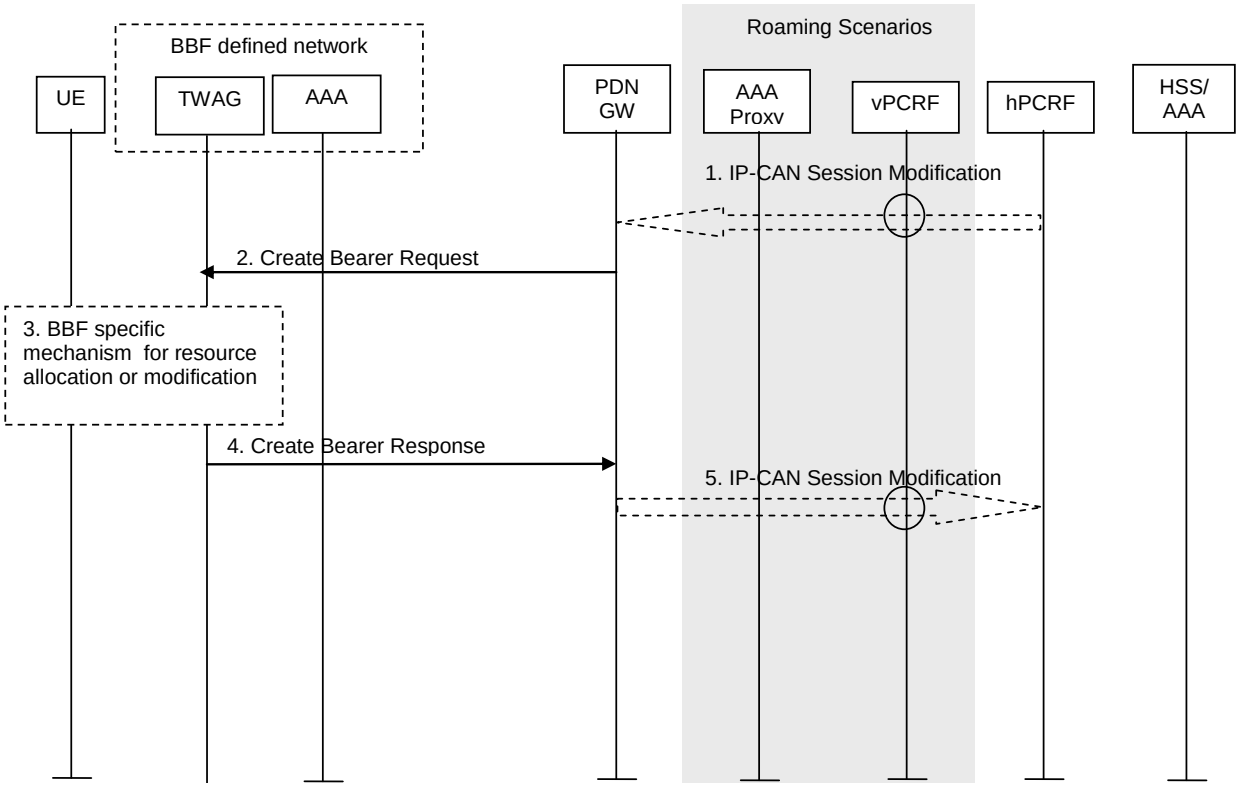


Figure 8.3.1.5.3-1: Dedicated S2a Bearer Activation Procedure with GTP on S2a

1. This step is the same as step 1 in TS 23.402 [3], clause 16.5.

2. The PDN GW uses this QoS policy to assign the S2a bearer QoS, i.e., it assigns the values to the bearer level QoS parameters QCI, ARP, GBR and MBR. The PDN GW sends a Create Bearer Request message (IMSI, EPS bearer QoS, TFT, PDN GW Address for the user plane, PDN GW TEID of the user plane, Charging Id, LBI) to the TWAG in the BBF domain. The Linked EPS bearer Identity (LBI) is the EPS bearer Identity of the default bearer.

3. A BBF specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.

4. The TWAG selects an EPS bearer Identity, which has not yet been assigned to the UE. The TWAG then stores the EPS bearer Identity and links the dedicated bearer to the default bearer indicated by the Linked Bearer Identity (LBI). The TWAG uses the uplink packet filter (UL TFT) to determine the mapping of uplink traffic flows to the S2a bearer. The TWAG then acknowledges the S2a bearer activation to the PGW by sending a Create Bearer Response (EPS bearer Identity, TWAN Address for the user plane, TWAN TEID of the user plane) message.

5. This step is the same as step 5 in TS 23.402 [3], clause 16.5.

8.3.1.5.4 Network-initiated bearer modification in WLAN on GTP S2a

8.3.1.5.4.1 PDN GW Initiated Bearer Modification

The dedicated bearer activation procedure for GTP based S2a is based on PDN GW Initiated Bearer Modification procedure described in TS 23.402 [3] clause 16.6.1.

The PDN GW initiated bearer modification procedure for a GTP based S2a is depicted in the figure below. This procedure is used to update the TFT for an active default or dedicated S2a bearer, or in cases when one or several of the S2a bearer QoS parameters QCI, GBR, MBR or ARP are modified (including the QCI or the ARP of the default S2a bearer e.g. due to the HSS Initiated Subscribed QoS Modification procedure, as described in clause 8.3.1.5.2.2).

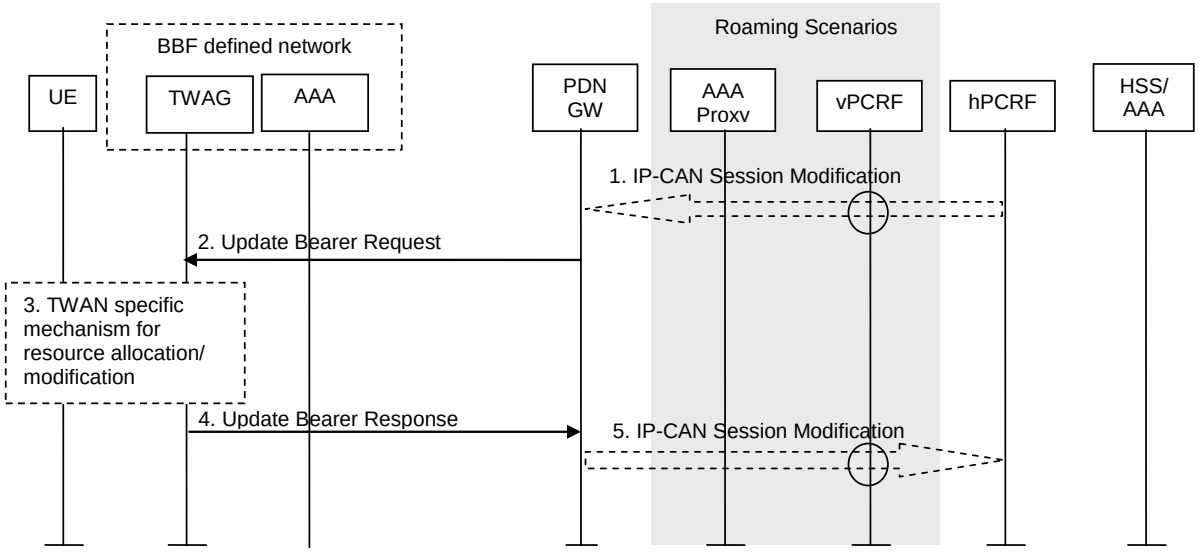


Figure 8.3.1.5.4.1-1: PDN GW-initiated S2a Bearer Modification Procedure with GTP on S2a

1. This step is the same as step 1 in TS 23.402 [3], clause 16.6.1.
2. The PDN GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active S2a bearer or that the authorized QoS of a service data flow has changed. The PDN GW generates the TFT and updates the S2a bearer QoS to match the traffic flow aggregate. The PDN GW then sends the Update Bearer Request (EPS bearer Identity, EPS bearer QoS, TFT) message to the TWAG in the BBF domain.
3. A BBF specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.
4. The TWAG uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the S2a bearer and acknowledges the S2a bearer modification to the PGW by sending an Update Bearer Response (EPS bearer Identity) message.
5. This step is the same as step 5 in TS 23.402 [3], clause 16.6.1.

8.3.1.5.4.2 HSS Initiated Bearer Modification

The dedicated bearer activation procedure for GTP based S2a is described in TS 23.402 [3] clause 16.6.2.

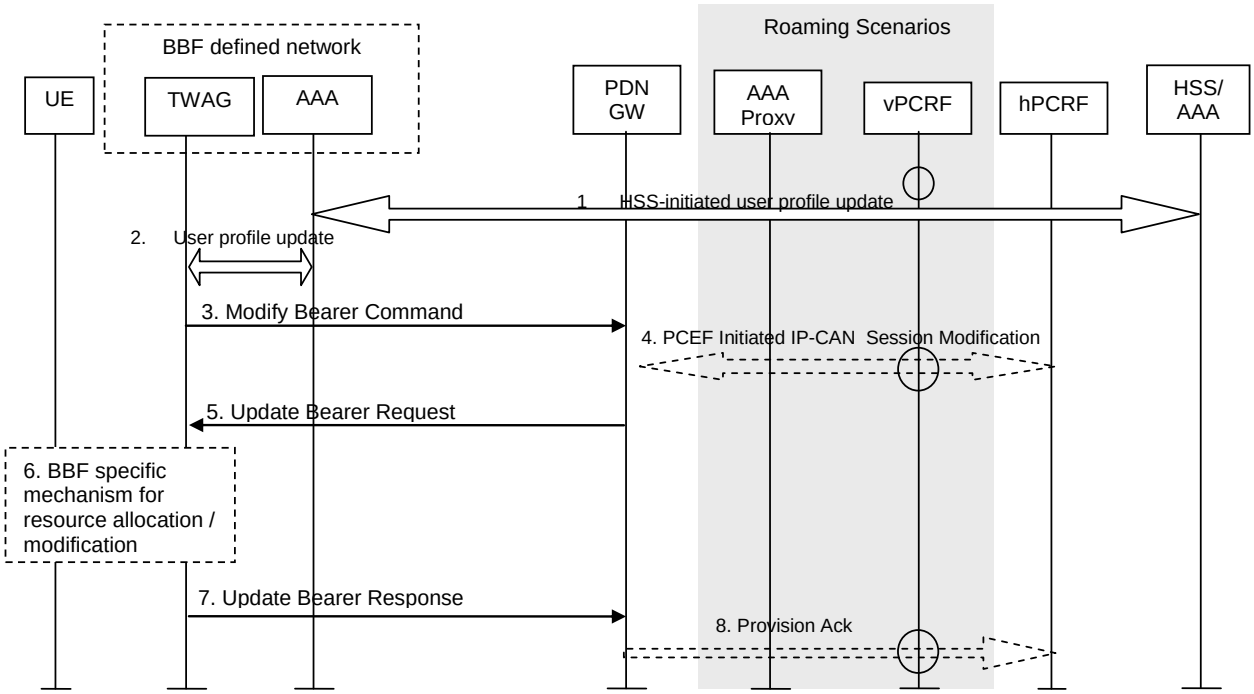


Figure 8.3.1.5.4.2-1: HSS Initiated Subscribed QoS Modification

1. The HSS updates the User Profile as specified in TS 23.402 [3] clause 12.2.1.
2. The BBF network provides the updated subscription data to the TWAG. The details of this step are out of the scope of 3GPP.
3. If the QCI and/or ARP and/or subscribed APN-AMBR has been modified and there is a related active PDN connection with the modified QoS Profile, the TWAG sends the Modify Bearer Command (EPS bearer Identity, EPS bearer QoS, APN AMBR) message to the PDN GW. The EPS bearer Identity identifies the default bearer of the affected PDN connection. The EPS bearer QoS contains the EPS subscribed QoS profile to be updated.
4. This step is the same as step 3 in TS 23.402 [3], clause 16.6.2
5. The PDN GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the PDN GW shall also modify all dedicated S2a bearers having the previously subscribed ARP value unless superseded by PCRF decision. The PDN GW then sends the Update Bearer Request (EPS bearer Identity, EPS bearer QoS, TFT, APN AMBR) message to the TWAG.
6. A BBF specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.
7. The TWAG acknowledges the bearer modification to the PDN GW by sending an Update Bearer Response (EPS bearer Identity) message. If the bearer modification fails the PDN GW deletes the concerned S2a Bearer.
8. This step is the same as step 7 in TS 23.402 [3], clause 16.6.2.

8.3.2 Alternative 2 - PMIP based S2a Solution

8.3.2.1 General principles

General architectural assumptions for alternative 2:

- QoS rules are provided by the PCRF to the PGW via Gx, then to the TWAG via S2a-PMIP;
- BRAS/BNG obtains QoS rules via the TWAG, which is outside the scope of 3GPP.

Editor's note: The specification of QoS transfer over PMIPv6 is work in progress by IETF as the Internet-Draft, draft-ietf-netext-pmip6-qos [26].

8.3.2.2 Reference architecture

The policy interworking network architecture for BB 2 for this alternative solution is shown in the following figures.

This architecture supports the scenario of a single or separate network operator(s) deployment of the 3GPP EPC and/or the BBF access network (Figure 8.3.2.2-1). It also supports the roaming scenario between two PLMN operators (Figure 8.3.2.2-2) and the one with the local breakout in VPLMN (Figure 8.3.2.2-3). These figures illustrate the separated model, where the TWAG and the BNG/BRAS functionalities are independently located; however, the collocated model, where these functionalities reside in one entity, is also covered, which is shown by dotted boxes surrounding them.

WLAN Access is connected to the TWAG via the BBF access for constructing Trusted WLAN Access (TWAN) and QoS rules that are provided to the TWAG are transferred to WLAN AN via Tn interface as defined in TR23.852 (not shown in the figures in this document).

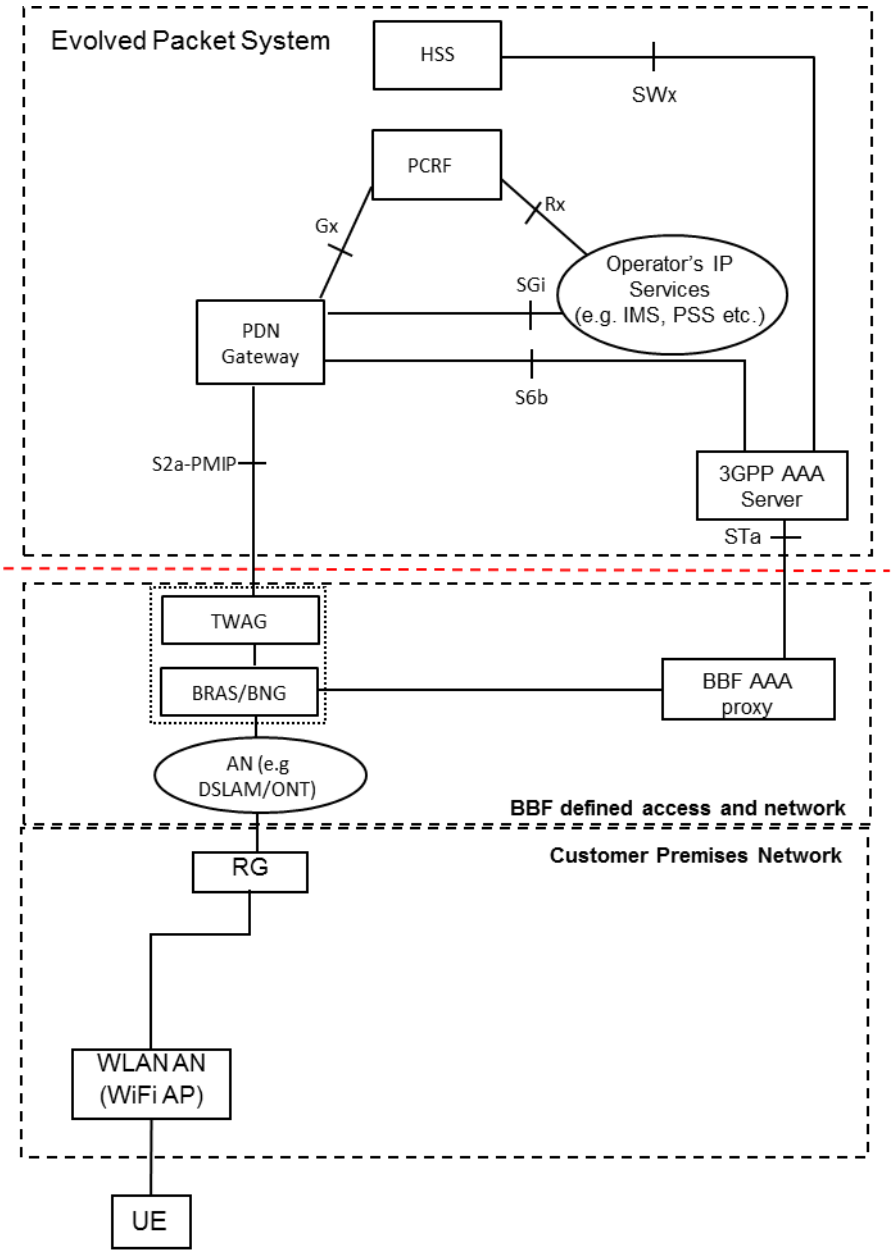


Figure 8.3.2.2-1: Non-Roaming Architecture with S2a-PMIP

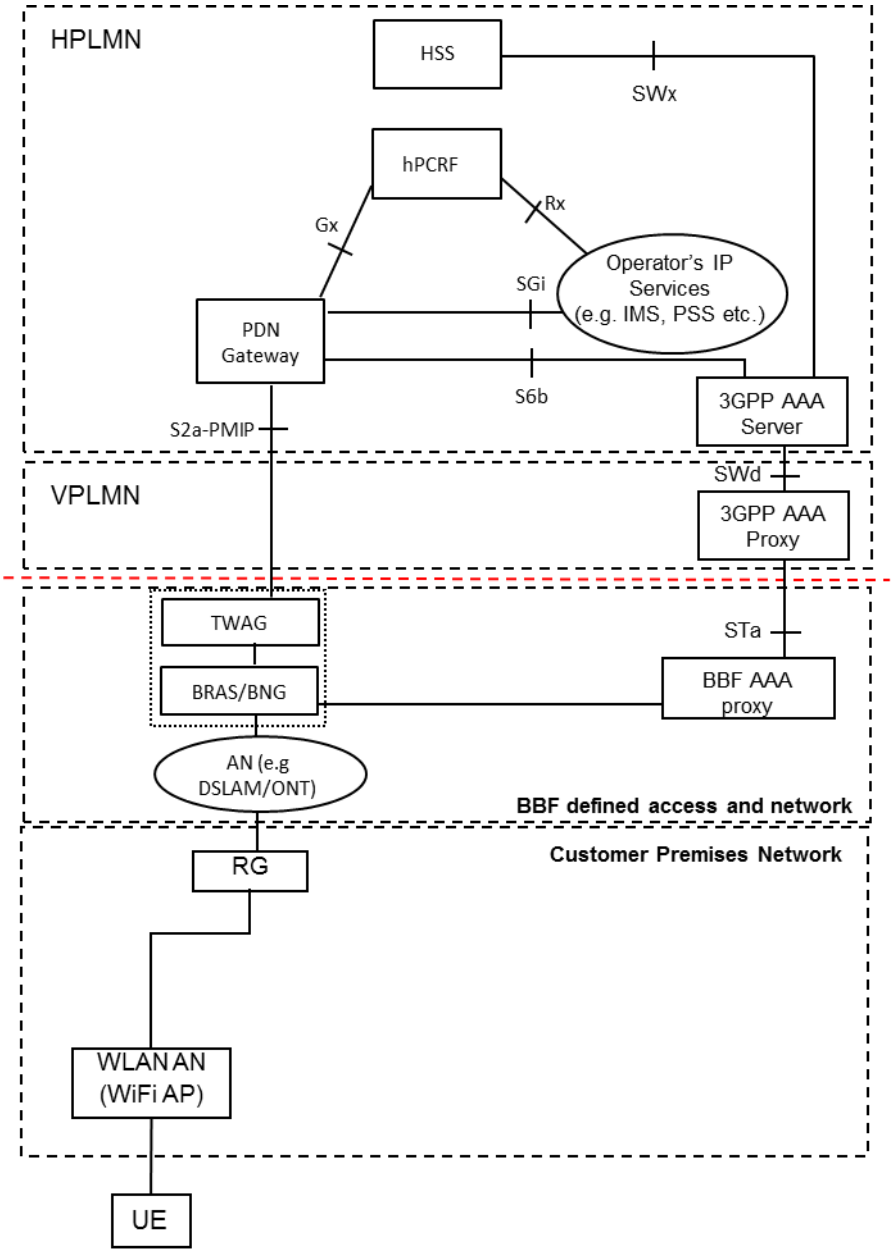


Figure 8.3.2.2-2: Roaming Architecture with S2a-PMIP – Home Routed

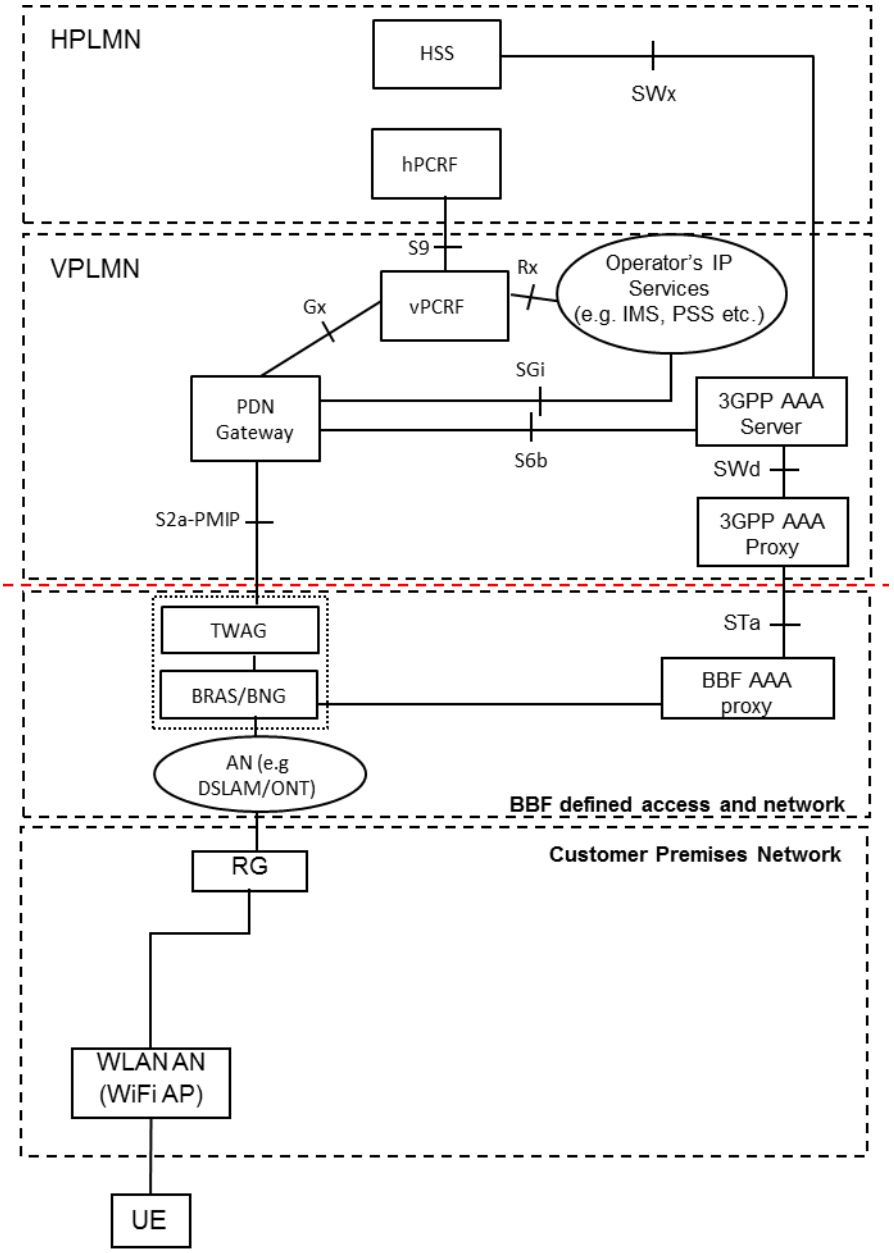


Figure 8.3.2.2-3: Roaming Architecture with S2a-PMIP - Local Break Out

8.3.2.3 Reference points

For the purpose of interworking between 3GPP and BBF network, the following interface is used:

S2a QoS control policies should be transferred to the TWAG from the P-GW. Location information is transferred to the P-GW from the TWAG.

8.3.2.4 Policy and QoS

Policy and QoS are controlled by the PCRF and they are transferred to TWAG over S2a signalling.

Editor's note: When the TWAG and BRAS/BNG are separated, how the QoS and PCC information is transferred from the TWAG to the BRAS/BNG is outside the scope of 3GPP.

8.3.2.5 Location information provided over S2a-PMIP to PGW

In this architecture, location information described in clause 8.2.1 (i.e., the network identity, the location of the AP and the geo-location) is transferred from the TWAN to PGW using S2a signalling as specified in TS 23.402 [3], clause 16.2.1.

8.3.2.6 Procedures

Editor's note: This clause will identify the procedures for Policy and QoS in TS 23.402 [3] and/or TS 23.203 [4] style for Building Block 2.

8.3.2.6.1 General

The call flow figures in the subsequent clauses are based on the caluses 16.2.2 and 16.3.2 of TS 23.402 [3]. The home routed roaming, LBO and non-roaming scenarios are depicted. In the LBO case, 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 is not involved.

8.3.2.6.2 Initial Attach/Gateway control session establishment

This clause specifies the procedures at the UE's initial attachment to a Fixed Broadband access network via PMIPv6-based S2a interface, for the UE to establish the first PDN connection over the Fixed Broadband Access with S2a. The TWAG transfers PCC rules received by the PDN GW to the BRAS/BNG to provision policy decisions for EPC routed traffic.

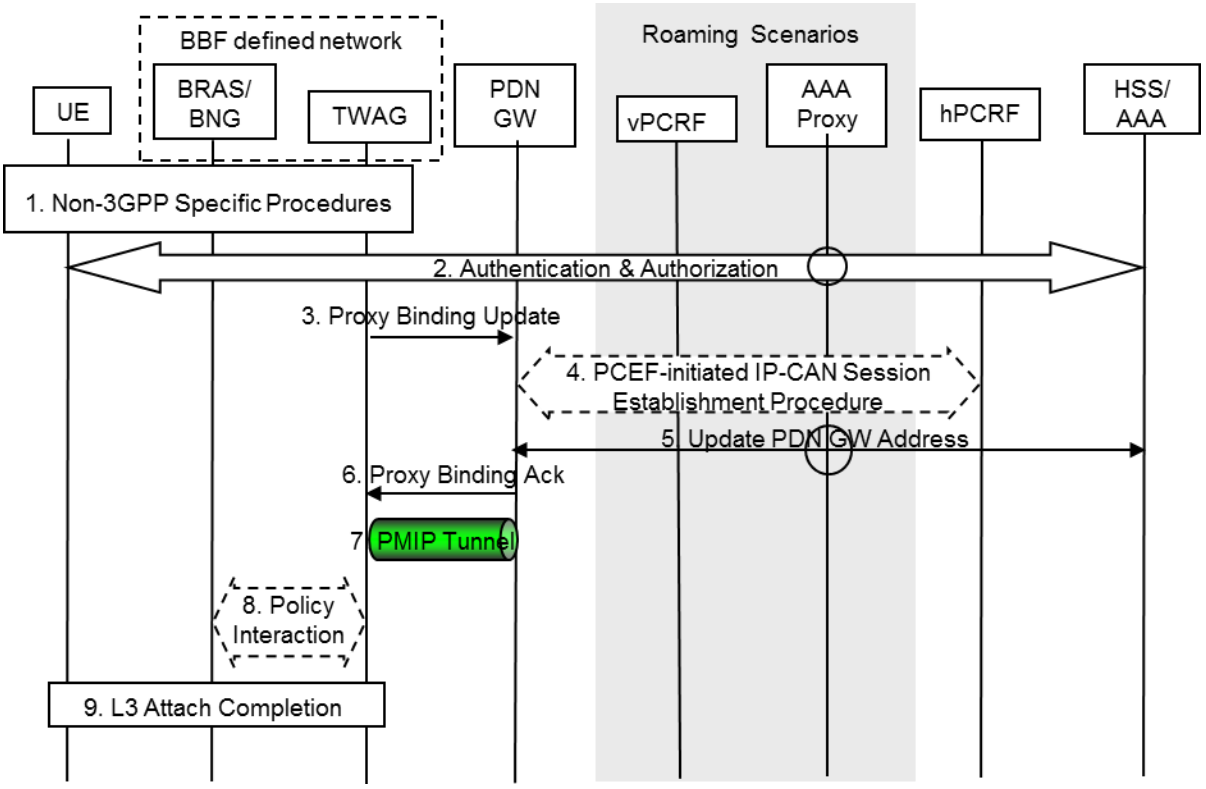


Figure 8.3.2.6.2-1: Initial Attach/Gateway control session establishment

The steps in this call flow follow TS 23.402 [3], clause 16.2.2 with the following clarifications:

Step 3: The TWAG sends the Proxy Binding Update with Default EPS Bearer QoS.

Step 6: The PDN GW returns the Proxy Binding Ack with EPS Bearer QoS.

Step 8: The BBF defined network uses the EPS bearer QoS to determine the relevant BBF QoS policies that are to apply to the IP flows exchanged on this S2a bearer.

8.3.2.6.3 Detach or PDN disconnection / Gateway control session termination procedure

This clause specifies the procedures at the UE's Detach or PDN disconnection from Fixed Broadband Access network via PMIPv6-based S2a interface.

8.3.2.6.3.1 UE/TWAG Initiated Detach and UE/TWAG Requested PDN Disconnection Procedure on S2a-PMIP

The procedure for UE/ TWAN Initiated Detach is represented in Figure 8.3.2.6.3-1 and described below.

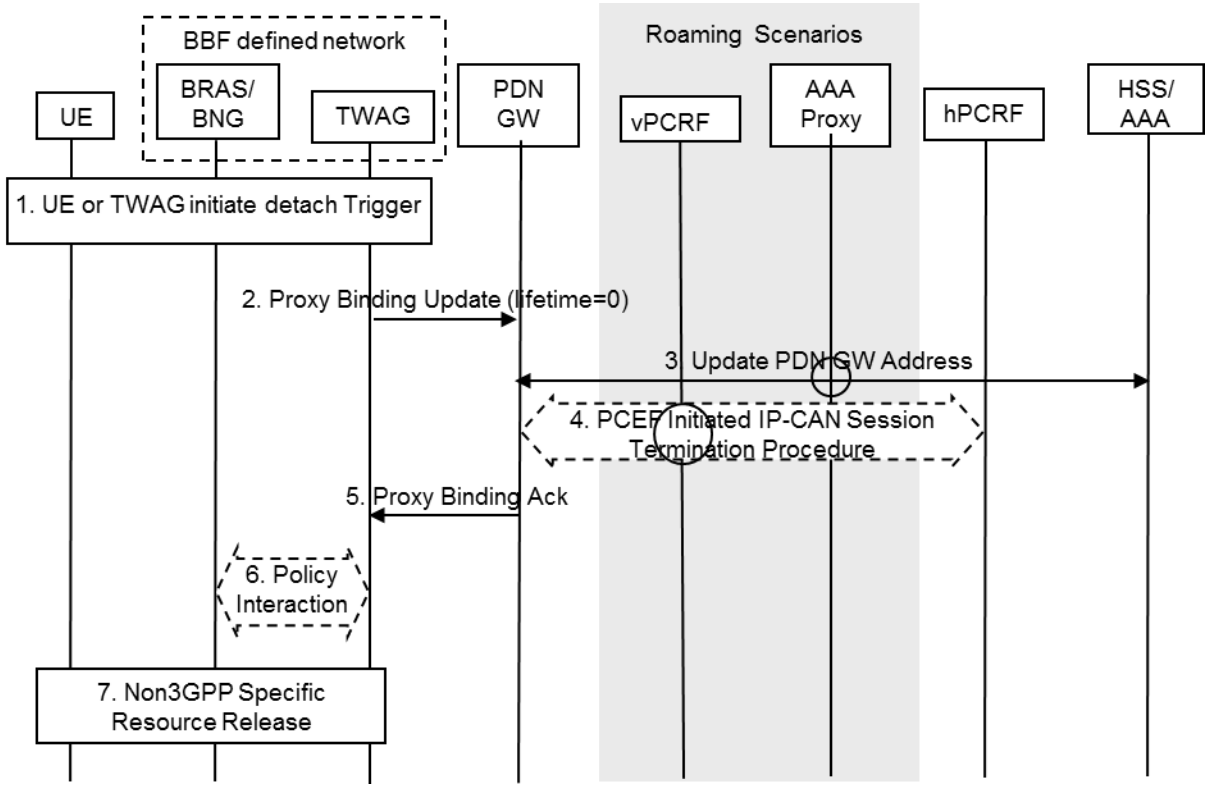


Figure 8.3.2.6.3-1: UE/TWAG Initiated Detach or PDN disconnection and UE/TWAG Requested Gateway control session termination procedure

The steps in this call flow follow TS 23.402 [3], clause 16.3.2.1 with the following clarifications:

Steps 6 and 7: Triggered by Step 5, the TWAG may interact with the BRAS/BNG to release the local policy session, which is defined by BBF.

8.3.2.6.3.2 HSS/AAA Initiated Detach Procedure on S2a-PMIP

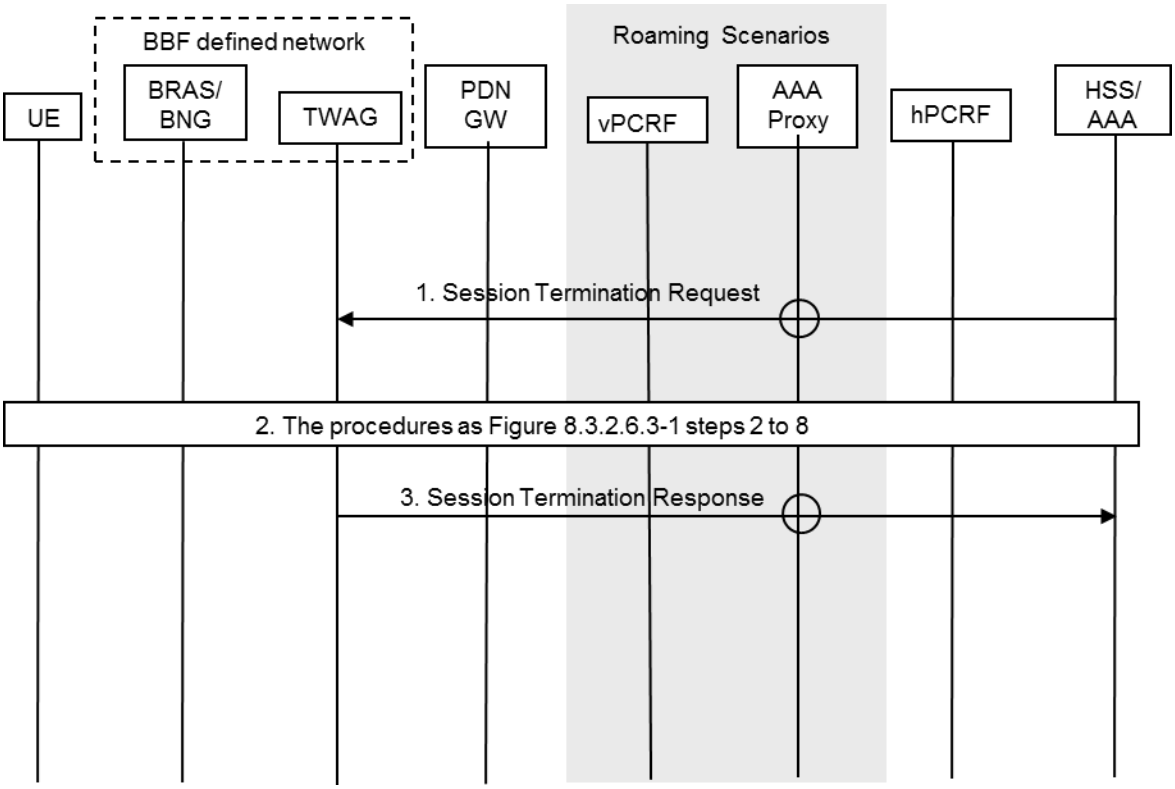


Figure 8.3.2.6.3-2: HSS/AAA Initiated Detach on S2a-PMIP

The procedure is similar to the call flow in TS 23.402 [3] clause 16.3.2.2. The difference is that step 2 refers to Figure 8.3.2.6.3-1.

8.3.3 Alternative 3 - Policy and QoS control via S9a

8.3.3.1 General principles

General architectural assumptions for alternative 1:

- S9a interface is between BPCF and PCRF
- PCRF provides QoS rules via S9a interface to BPCF for both S2a-GTP and S2a-PMIP cases.
- The BBF network shall be able to continue the same practice to perform the appropriate mapping with the QoS parameters received from the PCRF over the S9a interface.
- The policy control interface is agnostic to the deployment of S2a-GTP or S2a-PMIP.
- The policy control interface is agnostic to the internal configuration of TWAN (e.g. standalone or integrated TWAN and IPEdge/BNG configurations).

NOTE: An additional policy session (i.e. IP-CAN session) associated with the same UE may be established for NSWO traffic over the same S9a interface.

8.3.3.2 Reference architecture

The Interworking network architecture for BB 2 is shown in the following figures.

This architecture supports the scenario of a single network operator deploying both the 3GPP EPC and the BBF access network. Furthermore the architecture supports the roaming scenario between two PLMN operators.

The architectures in the following figures show only entities and interfaces that are in scope of the work and/or are impacted by BB 2.

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.

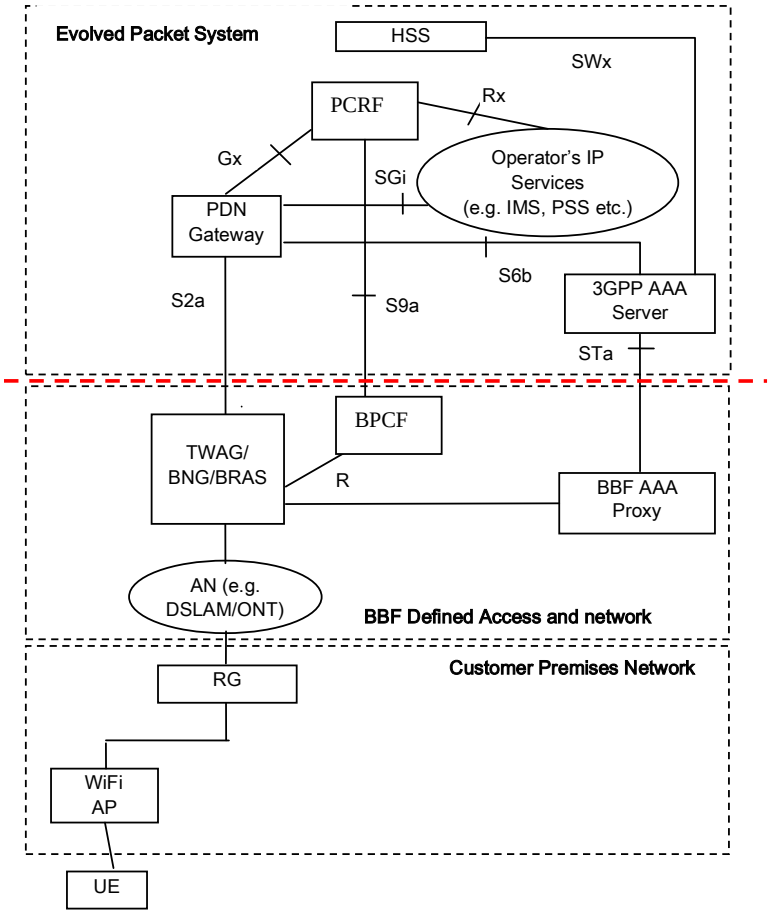


Figure 8.3.3.2-1: Non-Roaming Architecture for P4C_TI

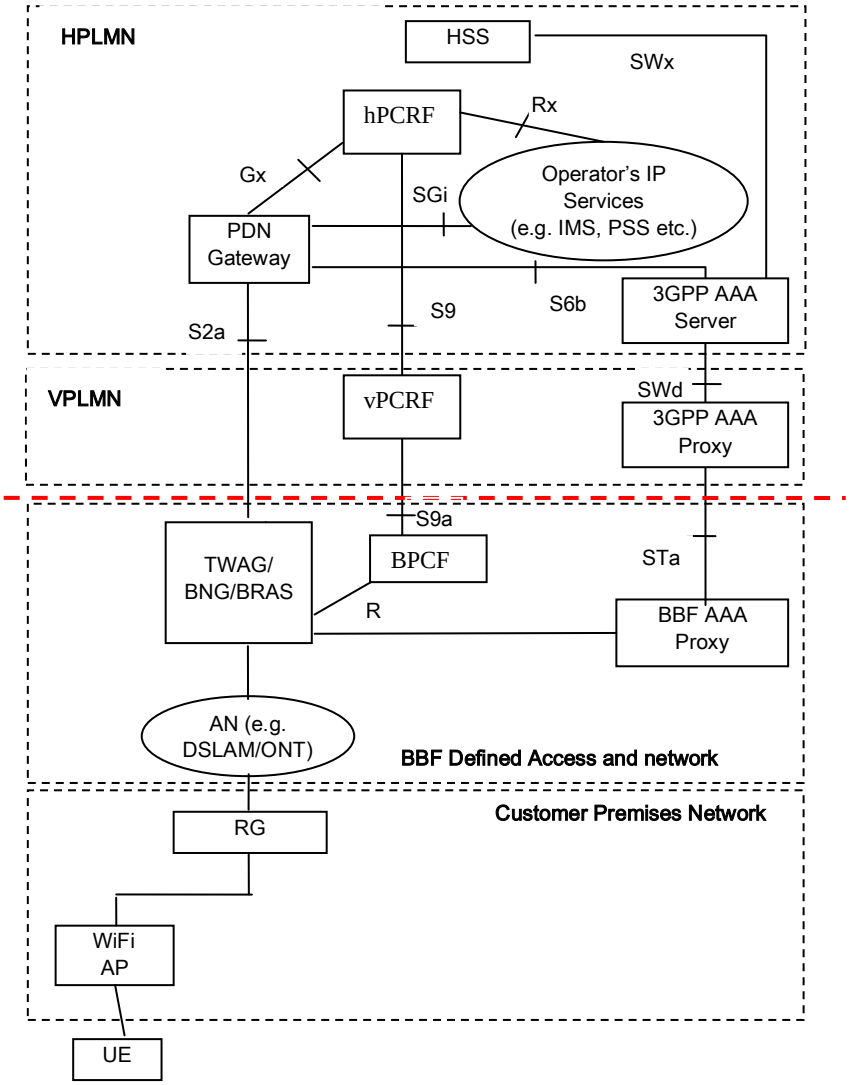


Figure 8.3.3.2-2: Roaming Architecture for P4C_TI- Home Routed

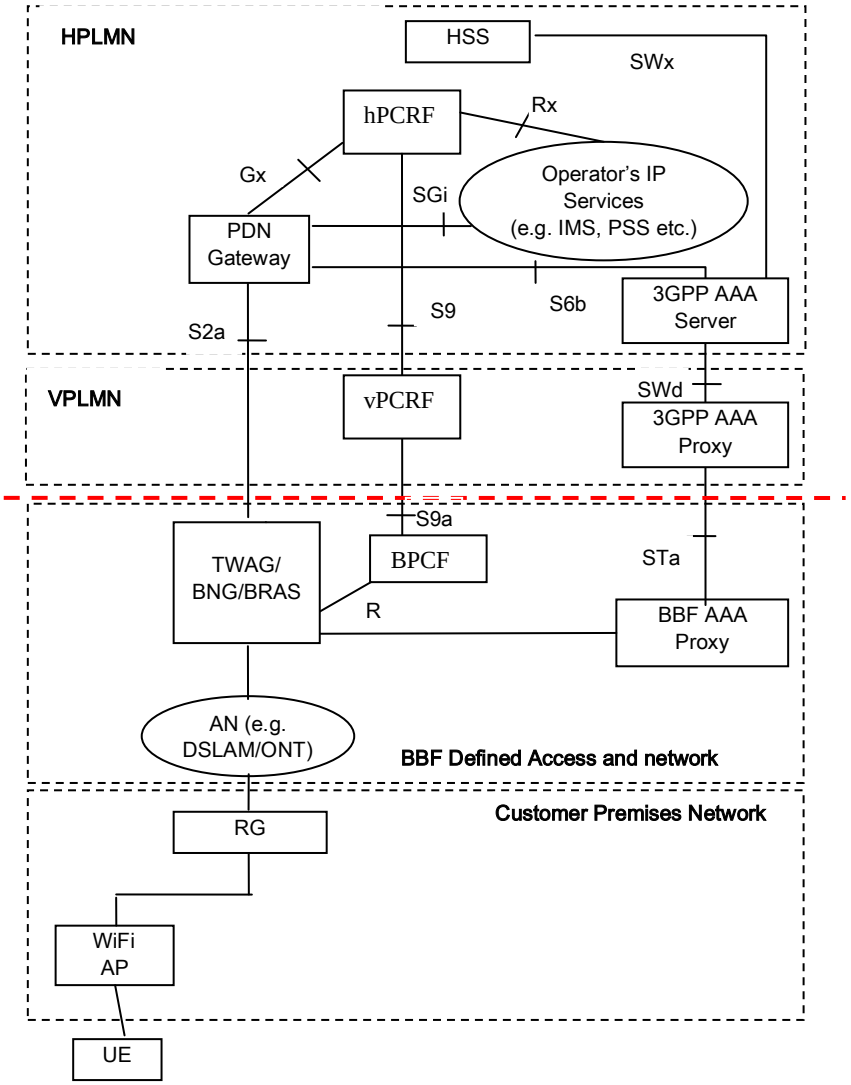


Figure 8.3.3.2-3: Roaming Architecture for P4C_TI- Local Break Out

Editor's note: TWAG may be integrated with BNG/BRAS or standalone.

Editor's note: The figures above describe a single entity supporting the TWAG and the BNG/BRAS functions and one interface between this entity and the AAA Proxy. Further refinement on the architecture figures above will be provided when TWAG function is partitioned from the BNG/BRAS.

8.3.3.3 Reference points

S9a For the purpose of Interworking between 3GPP and BBF network it transfers QoS control policies from the Home PCRF to the BPCF in non-roaming scenario and from the Visited PCRF to the BPCF in roaming scenario. The detailed description can refer to TS 23.139, clause 5.2 - Reference Points.

Editor's note: It is FFS whether S9a need enhancement or not.

Editor's note: Whether the Gateway control session over S9a for the EPC-routed traffic is initiated by PCRF or IP Edge is FFS.

8.3.3.4 Policy and QoS

Editor's note: This clause will identify the requirements and assumptions for Policy and QoS for alternative solution 3 in Building Block 2.

In this alternative solution, Policy and QoS are sent over S9a signalling, i.e. no additional requirements are imposed to FBB/BBF to define a signalling path to support either S2a-GTP or S2a-Gxa to provision QoS rules at the TWAN.

Assumptions for policy and QoS control via S9a:

- A common policy control interface is defined to support converged policy for the co-existence deployment for the NSWO and EPC-routed transport.
- This solution does not impact the existing QoS enforcement within the TWAN.
- The QoS parameters that are in-band to S2a-GTP will be ignored by TWAN as S9a is the common policy control interface to support policy control interworking for S2a over trusted WLAN access.

8.3.3.5 Procedures

Editor's note: This clause will identify the procedures for Policy and QoS in TS 23.402 [3] and/or TS 23.203 [4] style for Building Block 2.

8.3.3.5.1 General

The call flow figures in the subsequent clauses are based on subcaluse 16.2, TS 23.402 [3]. The home routed roaming, LBO and non-roaming scenarios are depicted. In the LBO case, 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 are not involved.

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

8.3.3.5.2 Initial Attach/Gateway control session establishment over S9a

This clause specifies the additional procedures at the UE's initial attachment to a Fixed Broadband access network via PMIPv6 or GTPv2 based S2a interface, for the UE to establish the first PDN connection over the Fixed Broadband Access with S2a.

Two possible alternatives are considered for triggering the gateway control session establishment over S9a: PCRF-initiated or BPCF-initiated.

Editor's note: The decision on which the alternative is to be adopted is FFS.

8.3.3.5.2.1 BPCF-initiated Gateway control session establishment over S9a

This procedure is triggered by BPCF to establish a gateway control session with the PCRF to request policy decisions for EPC routed traffic.

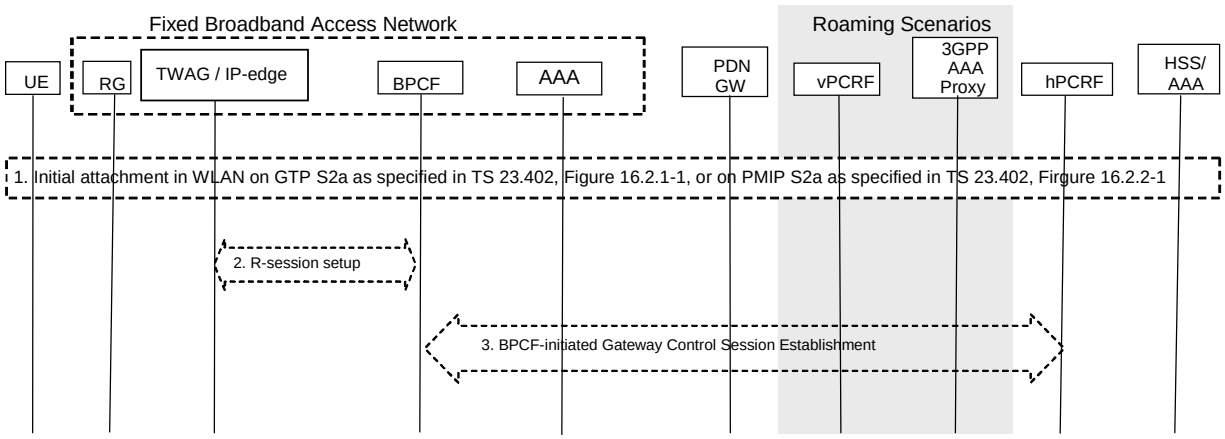


Figure 8.3.3.5.2.1-1: BPCF-initiated Gateway control session establishment over S9a

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 local policies.

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.

1. The description of the attachment procedure is the same as for steps 1-15 in TS 23.402 [3], clause 16.2.1 or 16,2,2.

2. Triggered by the successful authentication in step 8 of clause 16.2.1 or 16.2.2 in TS 23.402 [3] as referred by step 1 above, the BPCF is informed about the UE accessing over Fixed Broadband Access. The local policy session (R session) is established. How this is done is out of 3GPP scope.

Editor's note: How the BPCF is triggered by the IP-edge to initiate the Gateway Control Session towards the PCRF in the case of standalone or integrated TWAG scenario is FFS

3. Triggered by step 2, the BPCF initiates the Gateway Control Session establishment request over S9a with the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case). IMSI and APN needs to be included in the Gateway Control Session Establishment request message over S9a.

   After the hPCRF established the Gateway control session over S9a, the hPCRF will link it to the IP-CAN session over Gx interface, which is established in step 1.

8.3.3.5.2.2 PCRF-initiated Gateway control session establishment over S9a

This procedure is triggered by PCRF to establish a gateway control session with BPCF to provision policy decisions for EPC routed traffic. The PCRF initiated approach is the same as the existing S2b/c support except with the additional signaling parameter over S9a and is described in more details as follows.

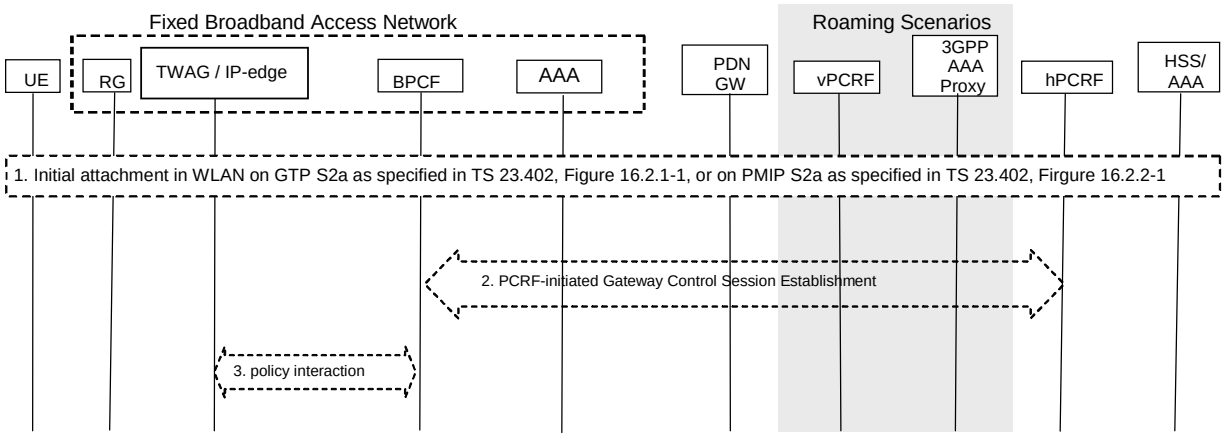


Figure 8.3.3.5.2.2-1: PCRF-initiated Gateway control session establishment over S9a

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 local policies.

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.

1. The description of the attachment procedure is the same as for steps 1-15 in TS 23.402 [3], clause 16.2.1 and clause 16.2.2 with the following additions: Fixed Broadband access network information (e.g. IP address of the IP-edge) are also forwarded to P-GW, then to PCRF.

   Such Fixed Broadband access network information is necessary for PCRF to identify the appropriate BPCF and IP-edge for the given UE when the gateway control session establishment is initiated by the PCRF towards the BPCF over S9a.

Editor's note: The details on how P-GW obtains the Fixed Broadband access network information and the details of the information for both integrated and standalone scenarios of TWAG is FFS.

2. Triggered by the step 4, the completion of the IP-CAN session establishment procedure, in clause 16.2.1 or 16.2.2 in TS 23.402 [3] as referred by step 1 above, 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 needs to be included in the Gateway Control Session Establishment request message over S9a.

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

8.3.3.5.3 Detach or PDN disconnection / PCRF initiated Gateway control session termination procedure over S9a

This clause specifies the additional procedures at the UE's Detach or PDN disconnection from Fixed Broadband access network via PMIPv6 or GTPv2 based S2a interface.

This procedure terminates the gateway control session between the BPCF and the PCRF for EPC routed traffic.

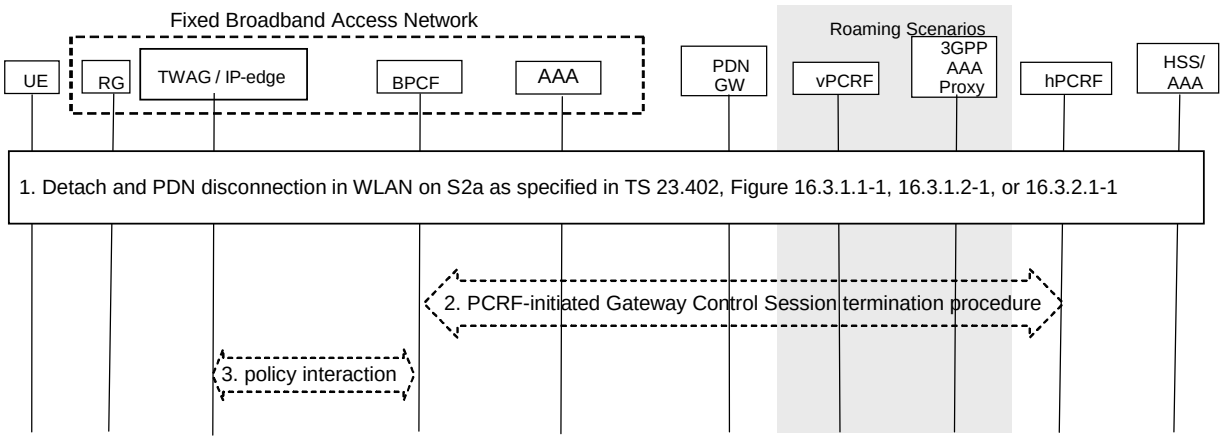


Figure 8.3.3.5.3-1: Detach or PDN disconnection and PCRF initiated Gateway control session termination procedure over S9a

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 local policies.

The IP-CAN session for the PDN Connection is terminated via Gx procedures which is specified in TS 23.402 [3]. In addition, the Gateway Control Session termination is initiated by PCRF.

1. The description of the Detach or PDN disconnection is the same as for clause 16.3.1 and clause 16.3.2 in TS 23.402 [3].

2. As referred by step 1 above, either step 1 in clause 16.3.1.1 or step 1 in clause 16.3.2.1 in TS 23.402 [3], the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case) initiates Gateway Control Session termination over S9a with the BPCF.

3. The BPCF may interact with the IP-edge, e.g. to release the local policy session, as defined by Fixed Broadband Access Policy Framework specifications BBF WT-134 [11] and BBF WT-203 [6]. This step is out of 3GPP scope.

8.3.3.5.4 PCRF initiated Gateway control and QoS rule provisioning procedure over S9a

This clause specifies the additional procedures at the PDN GW initiated resource allocation deactivation specified in clause 16.4, dedicated bearer activation specified in clause 16.5, and PDN GW Initiated Bearer Modification specified in clause 16.6.1, in TS 23.402 [3].

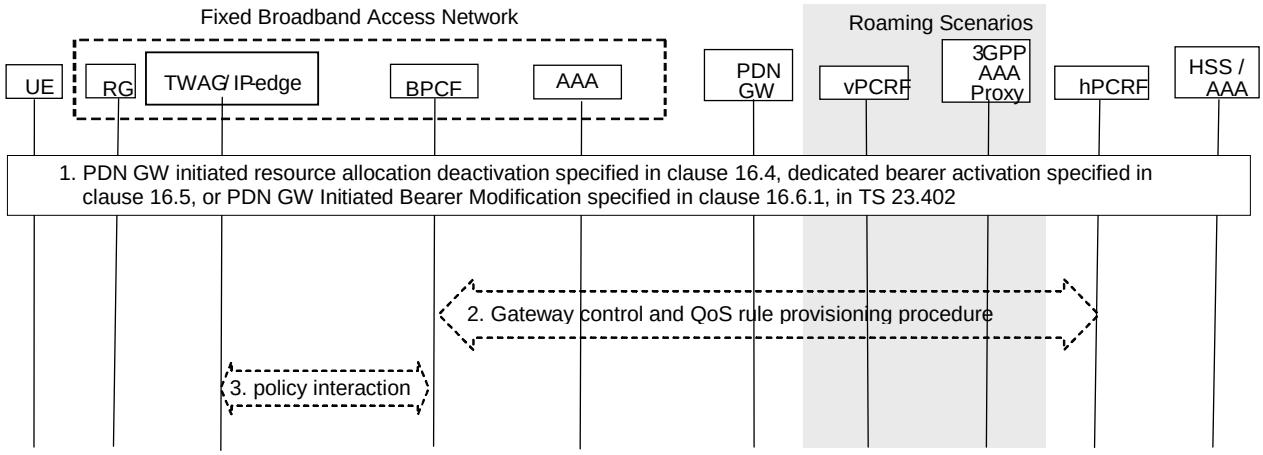


Figure 8.3.3.5.4-1: PCRF initiated Gateway control and QoS rule provisioning procedure over S9a

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 local policies.

The IP-CAN session for the PDN Connection is modified via Gx procedures which are specified in TS 23.402 [3]. In addition, the Gateway Control Session modification is initiated by PCRF.

1. The description of PDN GW initiated resource allocation deactivation is specified in clause 16.4, dedicated bearer activation is specified in clause 16.5, and PDN GW Initiated Bearer Modification is specified in clause 16.6.1, in TS 23.402 [3].

2. As referred by step 1 above, triggered bystep 3 in clause 16.4, or step 3 in clause 16.5, or step 3 in clause 16.6.1 in TS 23.402 [3], the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case) initiates gateway control and QoS rule provisioning procedure over S9a with the BPCF. 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.

3. The BPCF may interact with the IP-edge, e.g. to modify the local policy session, as defined by Fixed Broadband Access Policy Framework specifications BBF WT-134 [11] and BBF WT-203 [6]. This step is out of 3GPP scope.

8.3.3.5.5 BPCF initiated Gateway control and QoS rule request procedure over S9a

This clause specifies the additional procedures at HSS initiated bearer modification as specified in clause 16.6.2, in TS 23.402 [3]. And other triggers for BPCF initiated Gateway control and QoS rule request procedure may be defined in BBF network.

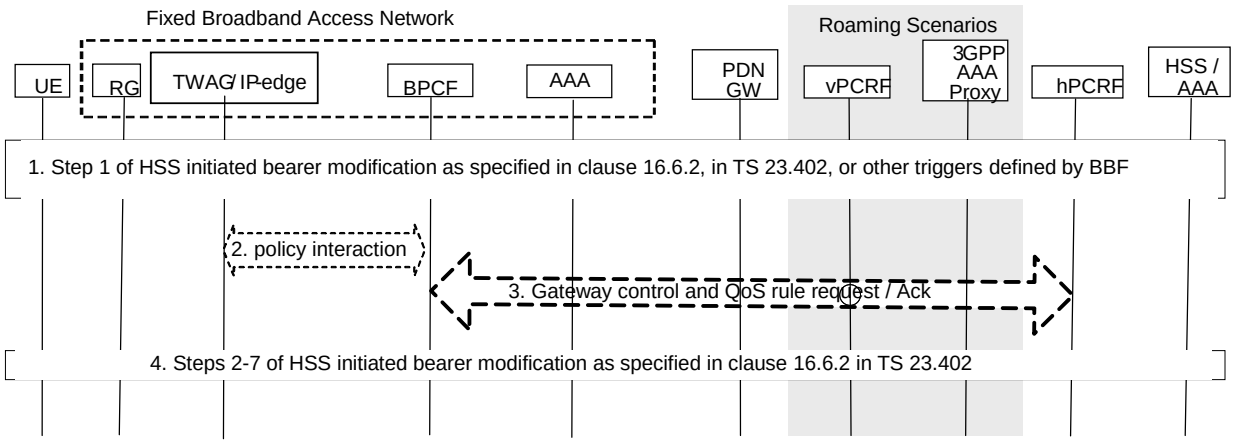


Figure 8.3.3.5.5-1: BPCF initiated Gateway control and QoS rule request procedure over S9a

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 local policies.

The IP-CAN session for the PDN Connection is modified via Gx procedures which are specified in TS 23.402 [3]. In addition, the Gateway Control Session modification is initiated by BPCF.

1. TWAN receives user's profile update as described in step 1 of HSS initiated bearer modification procedurein clause 16.6.2, in TS 23.402 [3].

2. Triggered by step 1 above, the IP-edge may interact with the BPCF, e.g. to modify the local policy session, as defined by Fixed Broadband Access Policy Framework specifications BBF WT-134 [11] and BBF WT-203 [6]. This step is out of 3GPP scope.

Editor's note: How the IP-edge obtains the updated user profile info from 3GPP AAA in order to convey the info to BPCF for either the standalone or integrated TWAG scenarios is FFS.

3. The BPCF initiates gateway control and QoS rule request procedure over S9a with the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming case). In roaming scenario, the BPCF will initiate the procedure over S9a towards the V-PCRF and the V-PCRF in turns initiates the procedure over S9 towards the H-PCRF.

4. The description for steps 2-7 of HSS initiated bearer modification is specified in clause 16.6.2, in TS 23.402 [3].

8.4 Evaluation of alternatives

Editor's note: This clause contains the evaluation of solutions for P4C Building Block 2 based on the objectives.

8.5 Conclusions

Alternative solution -1 (GTP-S2a) is fully specified in stage-2 and stage-3 specifications and as such is selected for P4C-TI in REL 12. No normative work for this solution is foreseen in Rel-12.

No further work is expected on P4C-TI in Rel-12.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2010-05	SA2#79				Initial TR skeleton approved at SA2#79 (S2-102860)		0.0.0
2010-05	SA2#79				Included approved tdocs from SA2#79: S2-102461, S2-102861, S2-103027, S2-103028, S2-102865, S2-103022, S2-102464, S2-103024	0.0.0	0.1.0
2010-05	SA2#79				Corrected editorial mistake in Figure 5.2.2.2.4-2	0.1.0	0.1.1
2010-09	SA2#80				Included approved tdocs from SA2#80: S2-103417, S2-103557, S2-104192, S2-104327, S2-104328, S2-104330, S2-104332, S2-104340, S2-104341, S2-104387	0.1.1	0.2.0
2010-10	SA2#81				Included approved tdocs from SA2#81: S2-104714, S2-105158, S2-105186, S2-105223, S2-105227, S2-105229, S2-105230, S2-105286	0.2.0	0.3.0
2010-11	SA2#82				Included approved tdocs from SA2#82: S2-105379, S2-105412, S2-105662, S2-105827, S2-105921, S2-105923, S2-105924, S2-105925, S2-105926, S2-105995, S2-105998, S2-106002, S2-106003, S2-106004	0.3.0	0.4.0
2011-02	SA2#83				Included approved tdocs from SA2#83: S2-110665, S2-111029, S2-111127, S2-111131, S2-111132, S2-111133, S2-111134, S2-111172, S2-111216, S2-111254, S2-111260	0.4.0	0.5.0
2011-04	SA2#84				Included approved tdocs from SA2#84: S2-112028, S2-112029, S2-112111, S2-112116, S2-112159, S2-112110, S2-112032, S2-112160	0.5.0	0.6.0
2011-05	SA2#85				Included approved tdocs from SA2#85: S2-11797, S2-112798, S2-112800, S2-112885	0.6.0	0.7.0
2011-06	SP-52	SP-100353	-	-	MCC update for presentation to TSG SA for information	0.7.0	1.0.0
2011-06	SA2#85				Included approved tdoc from SA2#85: S2-112799	1.0.0	1.1.0
2011-07	SA2#86				Included approved tdoc from SA2#86; S2-113277 endorse S9* rename, S2-113278, S2-113280, S2-113782, S2-113583	1.1.0	1.2.0
2011-10	SA2#87				Included tdoc SA2-4483 (Revision of architecture for BB2), S2-114461 (revision of scope for BB2 and BB3), S2-114470 (clarification on Policy for BB2), S2-114695 (assumptions for BB3), S2-114696 (reference architecture for BB3)	1.2.0	1.3.0
2011-11	SA2#88				Included approved tdoc from SA2#88: S2-114962, S2-115261, S2-115263, S2-115276, S2-115277, S2-115282, S2-115386, S2-115387, S2-115388, S2-115389, S2-115390, S2-115281, S2-115280, S2-115447, S2-115448	1.3.0	1.4.0
2011-06	SP-54	SP-100754	-	-	Presentation to TSG SA for information	1.4.0	1.4.1
2012-02	SA2#89				Included approved tdoc from SA2#88:s2-120882, S2-121124	1.4.1	1.5.0
2012-07	SA2#92				Included approved tdoc from SA2#92:s2-123316, S2-123428, S2-123429, S2-123430	1.5.0	1.6.0
2012-09	SA2#92				Editorial correction of numbering of sub clauses in 8.3.1 and 8.3.3. Correction of numbering of figure in clause 8.3.3	1.6.0	1.6.1
2012-10	SA2#93				Included approved tdoc from SA2#93: S2-123978, S2-123980, S2-123981, S2-123982 For Tdoc S2-123980, S2-1239801, S2-123982 yellow highlights removed .	1.6.1	1.7.0
2013-01	SA2#95				Included following document:S2-130594	1.7.0	1.8.0
2013-01	SA2#95				Corrected title of section 8.3.2	1.8.0	1.9.0
2013-05	SA2#96				Included S2-131445	1.9.0	1.10.0
2013-06	SP-60	SP-130233	-	-	MCC Editorial update for presentation to TSG SA for approval	1.10.0	2.0.0