TECHNICAL REPORT

TR-291

Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access

Issue: 1
Issue Date: March 2014

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER the Forum, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	3 March 2014	4 April 2014	Behcet Sarikaya, Huawei Roberto David Carnero Ros, Ericsson	Original

Comments or questions about this Broadband Forum Technical Report should be directed to help@broadband-forum.org.

Editor	Behcet Sarikaya	Huawei
	Roberto David Carnero Ros	Ericsson
E2EArchitecture WG Chairs	David Allan	Ericsson
	David Thorne	BT
Vice Chair	Sven Ooghe	Alcatel-Lucent

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

The Broadband Forum, in cooperation with 3GPP, is developing architecture and solutions for the interworking between wireline and wireless networks. TR-203 [7] defines the architectural framework for interworking, high level requirements for interworking solutions and a set of use cases that the solution should support.

TR-291 builds on the work done in TR-203 and provides the nodal requirements for solutions associated with the TR-203 interworking architecture and use cases.

1 Purpose and Scope

1.1 Purpose

Since the introduction of mobile devices that include Wi-Fi, there has been an increasing interest in coordination and interworking among wireless and wireline networks. The rise in the use of smartphones at public hotspots has accelerated this interest. As the popularity of smartphones, tablets, and mobility-enabled laptops continues to increase, an emerging ecosystem is taking shape where applications are developed largely independently of access types. There is increased desire to provide network capabilities that offer better user experiences and more efficient network utilization for these devices as they handoff, roam, tether, and attach to wireline locations. The interworking between fixed and mobile networks is becoming a requirement for operators that wish to provide superior user experiences.

The Broadband Forum has published an architectural framework for interworking between fixed access and 3GPP mobile accesses in TR-203 [7], *Interworking between Next Generation Fixed and 3GPP Wireless Access*. TR-203 defines business requirements, use cases, high-level functional architecture, and deployment options for interworking. Building on that, the purpose of TR-291 is to provide a system architecture at the nodal level and nodal requirements in support of the scope of TR-203.

1.2 Scope

TR-291 covers requirements on the regional access network and customer premises network in order to support interworking between BBF wireline access networks and 3GPP wireless networks to allow the attachment of 3GPP User Equipment (UE) to wireline networks. The network elements involved include: Residential Gateway (RG), Access Node (AN), Multi Service Broadband Network Gateway (MS-BNG), Broadband Policy Control Function (BPCF), Fixed Access Authentication Authorization Accounting Server (AAA), UE, Femto Access Point (Femto AP) and Wi-Fi AP. TR-291 depends on requirements that 3GPP Rel-11 has developed for elements like Policy and Charging Rules Function (PCRF), Packet Data Networks Gateway (PDN GW), evolved Packet Data Gateway (ePDG), and other 3GPP network elements.

TR-291 refers to TR-124i3 [2], TR-134 [3], TR-145 [4], TR-146 [5], WT-178 [6], TR-203 [7], and 3GPP Rel-11 specifications TS 23.139 [11], TS 23.203 [12] and TS 23.402 [14] as appropriate.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [26].

MUST This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.

MAY This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-101i2	*Migration to Ethernet-Based Broadband Aggregation*	Broadband Forum	2011
[2]	TR-124i3	*Functional Requirements for Broadband Residential Gateway Devices*	Broadband Forum	2012

[3]	TR-134	*Broadband Policy Control Framework (BPCF)*	Broadband Forum	2012
[4]	TR-145	*Multi-service Broadband Network Functional Modules and Architecture*	Broadband Forum	2012
[5]	TR-146	*Subscriber Sessions*	Broadband Forum	2013
[6]	WT-178	*Multi-service Broadband Network Architecture and Nodal Requirements*	Broadband Forum	WIP
[7]	TR-203	*Interworking between Next Generation Fixed and 3GPP Wireless Networks*	Broadband Forum	2012
[8]	TS 23.002	*Network architecture (Release 11)*	3GPP	2012
[9]	TS 23.003	*Numbering, addressing and identification (Release 11)*	3GPP	2012
[10]	TS 23.060	*General Packet Radio Service (GPRS); Service description; Stage 2 (Release 11)*	3GPP	2012
[11]	TS 23.139	*3GPP system - fixed broadband access network interworking; Stage 2 (Release 11)*	3GPP	2012
[12]	TS 23.203	*Policy and charging control architecture (Release 11)*	3GPP	2012
[13]	TS 23.401	*General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 11)*	3GPP	2012
[14]	TS 23.402	*Architecture enhancements for non-3GPP accesses (Release 11)*	3GPP	2012
[15]	TS 24.302	*Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access network; Stage 3 (Release 11)*	3GPP	2012
[16]	TS 29.215	*Policy and Charging Control (PCC) over S9 reference point; Stage 3 (Release 11)*	3GPP	2012
[17]	TS 29.273	*3GPP EPS AAA interfaces (Release 11)*	3GPP	2012
[18]	TS 29.274	*Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) (Release 11)*	3GPP	2012
[19]	TS 29.281	*General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U) (Release 11)*	3GPP	2012

[20]	TS 33.210	*3G security; Network Domain Security (NDS); IP network layer security (Release 11)*	3GPP	2012
[21]	TS 33.320	*Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Release 11)*	3GPP	2012
[22]	TS 33.402	*Security aspects of non-3GPP accesses (Release 11)*	3GPP	2012
[23]	IEEE 802.11	*Wireless LANs*	IEEE	2007
[24]	IEEE 802.1Q	*Virtual LANs*	IEEE	2011
[25]	IEEE 802.1X	*Port Based Network Access Control*	IEEE	2010
[26]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[27]	RFC 2784	*Generic Routing Encapsulation*	IETF	2000
[28]	RFC 3579	*RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*	IETF	2003
[29]	RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*	IETF	2003
[30]	RFC 3931	*Layer Two Tunneling Protocol - Version 3 (L2TPv3)*	IETF	2005
[31]	RFC 4284	*Identity Selection Hints for the Extensible Authentication Protocol (EAP)*	IETF	2006
[32]	RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*	IETF	2008
[33]	RFC 5844	*IPv4 Support for Proxy Mobile IPv6*	IETF	2010

2.3 Definitions

The following terminology is used throughout this Technical Report.

3GPP Access Authentication 3GPP based access authentication is executed across a SWa/STa reference point as depicted in the 3GPP Evolved Packet System (EPS) architecture.

3GPP Allocation and Retention Priority The 3GPP Quality of Service (QoS) parameter Allocation and Retention Priority contains information about the priority level, the pre-emption capability and the pre-emption vulnerability.

3GPP-BBF Interworking It occurs when a 3GPP UE accesses the internet and/or other services through the BBF access network – by femtocell or Wireless LAN (WLAN) connectivity. For such purpose, the BBF requests the 3GPP domain for authentication, authorization and policy parameters for the 3GPP UE, with the aim of either offloading traffic onto the local wireline network and/or routing it through the 3GPP domain.

3GPP Network-Based Mobility 3GPP Network Based Mobility occurs when the mobility management is supported by the trusted/non-trusted BBF domain which may consult the 3GPP domain in the setup process (e.g. request the IP address from the PDN GW).

3GPP PCC Rule A set of information enabling the detection of a 3GPP service data flow, defining its associated 3GPP QoS parameters and enabling charging differentiation. Please note that for BBF routed connectivity charging information is not applicable. The 3GPP Policy and Charging Control (PCC) rule is defined in 3GPP TS 23.203 [12].

3GPP QCI 3GPP QoS Class Identifier (QCI) is a scalar that is used as a reference to a node-specific set of parameters and values that control packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration) to be provided for a specific mobile service. This parameter is defined in the 3GPP TS 23.203 [12].

3GPP QoS Rule A set of information enabling the detection of a 3GPP service data flow and defining its associated 3GPP QoS parameters. The 3GPP QoS rules are defined in 3GPP TS 23.203 [12].

3GPP routed connectivity When a 3GPP-UE is attached to a WLAN or to a 3GPP femtocell, the IP traffic from the 3GPP UE (both transmitted from and received by the UE) is routed through the 3GPP domain, e.g. via ePDG and/or PDN GW, traversing the BBF network.

For 3GPP routed traffic, seamless IP connectivity is supported, since the anchor point for mobility is located in the 3GPP network.

NOTE: This scenario is similar to the roaming setup between two 3GPP operators, in particular to the Home routed scenario when traffic reaches a network element in Home Public Land Mobile Network (HPLMN).

3GPP Tunnel Authentication Tunnel Authentication refers to the procedure by which the UE and the ePDG/PDN GW perform mutual authentication during the IPsec tunnel establishment between the UE and the ePDG/PDN GW.

3GPP UE It is the end-user device that allows access to network services. The interface between the UE and the 3GPP network is the radio interface. The User Equipment consists of the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME). The UE is defined in the 3GPP TS 23.002 [8].

APN The Access Point Name (APN) is defined in 3GPP TS 23.003 [9]. It is typically a Fully Qualified Domain Name that resolves to a 3GPP Gateway GPRS Support Node (GGSN) or PDN GW for a given service as requested by the 3GPP UE.

It is composed of two parts:

1. The APN Network Identifier: this defines to which external network the GGSN/PDN GW is connected and optionally a requested service by the 3GPP UE. This part of the APN is mandatory.

2. The APN Operator Identifier: this defines in which Public Land Mobile Network (PLMN) GPRS/EPS backbone the GGSN/PDN GW is located. This part of the APN is optional.

BBF routed connectivity When a 3GPP-UE is attached to a WLAN, the IP traffic from the 3GPP UE (both transmitted from and received by the UE) is routed out to the fixed network services and/or to the Internet from the BBF network without traversing the 3GPP EPC.

Gateway Control Session An association between a BPCF and a PCRF used for transferring access specific parameters, BPCF events and QoS rules between the PCRF and BPCF. The Gateway Control Session is defined in 3GPP TS 23.139 [11] and 3GPP TS 23.203 [12].

Host-Based Mobility Host-Based Mobility occurs when the mobility management is performed directly by the 3GPP UE without intermediate BBF network intervention. In this mobility type, the 3GPP UE establishes a direct tunnel towards the 3GPP domain (PDN GW) which is used to forward all traffic to and from the user equipment. The fixed network proxies the entire authentication signaling towards the 3GPP domain and the PDN GW is responsible for assigning a virtual IP address to the tunnel during the setup process.

IMSI The International Mobile Subscriber Identity (IMSI) is a unique identification number, stored on a Subscriber Identity Module (SIM) inside the phone or mobile device, and used to identify a 3GPP subscriber. The IMSI is defined in 3GPP TS 23.003 [9].

IP-CAN Session The IP Connectivity Access Network (IP-CAN) Session is the association between a 3GPP UE and an IP network. The association is identified by one IPv4 address and/or an IPv6 prefix together with 3GPP UE identity information, if available, and a Packet Data Network (PDN) represented by a PDN ID (e.g. an APN). An IP-CAN session exists as long as 3GPP UE IP addresses/prefix are established and announced to the IP network. The IP-CAN Session is defined in the 3GPP TS 23.203 [12].

Network-Based Mobility Network-Based Mobility occurs when the mobility management is performed by the 3GPP network.

Regional Broadband Network As defined in Section 1.6/TR-101i2 [1], the Regional Broadband Network interconnects the service provider's networks and the access networks. Typically more than one access network is connected to a common regional network.

Roaming The ability of a 3GPP device to access services according to their user profile while moving outside of their subscribed home network, i.e. by using an access point of a visited network.

S2a Reference point between the Trusted WLAN Access Gateway (TWAG) and the 3GPP PDN GW. It is used for interworking between a Trusted BBF Access and 3GPP network and for supporting IP Network-Based Mobility. It conveys mobility and policy control from the 3GPP domain towards the TWAG.

S2b Reference point between the ePDG and the 3GPP PDN GW. It is used for interworking between Untrusted BBF and 3GPP networks and for supporting IP Network-Based Mobility. This reference point is intra 3GPP-domain

S2c Reference point between the 3GPP UE and the 3GPP PDN GW. It is used for interworking between BBF and 3GPP networks and for supporting Host-Based Mobility. It provides the user plane with related control and mobility support between the 3GPP UE and the 3GPP Gateway. This reference point is implemented over Trusted and/or Untrusted BBF Access and/or 3GPP Access.

S9a The reference point between the BPCF and the 3GPP PCRF. It is intended to support interworking between BBF and 3GPP networks, providing transfer of dynamic QoS control policies from the PCRF towards the BPCF for host-based mobility (S2c), network-based mobility (S2b) and BBF routed traffic.

STa/SWa Reference point between the Fixed Access AAA Server and the 3GPP HSS/AAA. It is used for transporting access authentication, authorization, mobility parameters and accounting information.

Subscriber Session As defined in Section 2.3/TR-146 [5], a Subscriber Session can be a Point-to-Point Protocol (PPP) Session, an IP Session, or an Ethernet Session. Subscriber sessions are used to represent all traffic that is associated with that subscriber by a given service provider in order to provide a context for policy enforcement.

Trusted Access An Access network is considered trusted by the Home 3GPP Network service provider when it fulfills all the security features deemed necessary by the Home 3GPP Network service provider. The Home 3GPP Network service provider owns the 3GPP device subscription. This is also the case where the non-3GPP and 3GPP wireless network service providers have a business agreement to permit the 3GPP UE to access non-3GPP network services like Internet and localized services.

In a BBF Trusted access, the 3GPP UE authentication signaling is provided by the fixed broadband network which may also query the Home 3GPP Home Subscriber Server (HSS)/AAA.

TWAG The TWAG is the logical entity responsible for the 3GPP UE IP mobility service on the data plane between a Trusted BBF Access and 3GPP network.

TWAN The Trusted WLAN Access Network (TWAN) is the construct from which the 3GPP systems (UE and core) accept trusted Wi-Fi traffic from a non-3GPP network. The TWAN is defined in 3GPP TS 23.402 [14]

TWAP The Trusted WLAN AAA Proxy (TWAP) is a logical AAA element that binds the UE's subscription data held by its 3GPP provider, to the Media Access Control (MAC) Address seen by the WLAN Access Network. It provides the TWAG with such information together with L2 attach/detach events when needed as triggers

Untrusted Access An Access Network is considered untrusted by Home 3GPP network when it does not fulfill the security features required by the Home 3GPP Network service provider.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization & Accounting
AN	Access Node
AP	Access Point
APN	Access Point Name
ARP	Address Resolution Protocol
BPCF	Broadband Policy Control Function
BSSID	Basic Service Set Identifier
CoA	Change of Authorization
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
H(e)NB	Home evolved Node B
HESSID	Homogenous Extended Service Set Identifier
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IKEv2	Internet Key Exchange version 2
IMSI	International Mobile Subscriber Identity
IP-CAN	IP Connectivity Access Network
IPMM	IP Mobility Mode
L2TPv3	Layer 2 Tunneling Protocol version 3
LIPA	Local IP access

MAC	Media Access Control
ME	Mobile Equipment
MME	Mobility Management Entity
MS-BNG	Multi Service Broadband Network Gateway
NAI	Network Access Identifier
NA(P)T	Network Address (Port) Translation
NSWO-APN	Non-Seamless WLAN Offload - APN
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Networks
PDN GW	Packet Data Networks Gateway
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PPP	Point-to-Point Protocol
QCI	QoS Class Identifier
QoS	Quality of Server
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RBN	Regional Broadband Network
RG	Residential Gateway
RS	Router Solicitation
SeGW	Security Gateway
SIM	Subscriber Identity Module
SIPTO	Selected IP Traffic Offload
SSID	Service Set Identifier
TDF	Traffic Detection Function
TR	Technical Report
TWAG	Trusted WLAN Access Gateway
TWAN	Trusted WLAN Access Network
TWAP	Trusted WLAN AAA Proxy
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
VLAN	Virtual Local Area Network
VPLMN	Visited Public Land Mobile Network
WAN	WLAN Access Network
WG	Working Group
WLAN	Wireless Local Area Network.
WT	Working Text

3 Technical Report Impact

3.1 Energy Efficiency

TR-291 has no impact on Energy Efficiency.

3.2 IPv6

IPv6 is covered in TR-291. There are nodal requirements which cover the cases of both wireline and wireless networks being IPv6 and both being IPv4. However, the case where/when one network is IPv4 and the other IPv6 is not covered.

3.3 Security

Most aspects of security for 3GPP and Fixed Broadband interworking are already defined in 3GPP TS 33.402 [22] (security architecture between non-3GPP accesses, including fixed broadband access, and 3GPP EPC) and 3GPP TS 33.210 [20] (security architecture for network domain IP based control planes).

Security aspects in particular L2 isolation on P2P links are covered in Section 7.5.

3.4 Privacy

Because TR-291 describes interworking between 2 operators, privacy concerns will need to encompass the privacy statements and policies of both operators. Customers may need to be told the differences they can expect in the privacy of their communications based on the selection of protocols and technologies by the interworking operators.

4 Introduction

This section provides an overview of the interworking principles described by TR-203 [7] for trusted and un-trusted interworking.

A UE whose traffic is crossing a BBF network should still benefit from a certain degree of mobility, provided that the UE is equipped with a Wi-Fi or a 3GPP interface, and that the required 3GPP mechanisms are present in the network. These mechanisms can either remain confined to the 3GPP domain, or be entrusted to the BBF domain.

- When the mechanisms are confined to the 3GPP domain, the BBF network is said to be UNTRUSTED (by the subscriber 3GPP operator). The interworking solution in the BBF network may be able to assist the 3GPP network in controlling the UEs' traffic.
    - The femtocell traffic of a UE is backhauled by means of a 3GPP HeNB establishing a secured tunnel to a 3GPP core over the BBF network.
    - The Wi-Fi traffic of a UE is forwarded over the BBF network and goes through a secure tunnel.
- When the mechanisms are entrusted to the BBF domain, the BBF network is said to be TRUSTED (by the subscriber 3GPP operator), and UEs' Wi-Fi traffic is forwarded and controlled by the interworking solution in the BBF network.

This Technical Report considers the interworking mechanisms for UE traffic. This includes both:

- 3GPP routed connectivity (a.k.a. "EPC-routed" in 3GPP) where traffic requiring mobility support is routed via the 3GPP domain.
- BBF routed connectivity (a.k.a. "NSWO" for "non-seamless WLAN offload" in 3GPP), where traffic is routed across the BBF domain. This typically occurs when the mobility service is not required or not achievable.

The terms 3GPP routed connectivity and BBF routed connectivity can be applied to traffic on a per Subscriber Session basis (as defined in TR-146 [5]) or on a per APN basis (a.k.a. Selected IP Traffic Offload (SIPTO) in 3GPP). 3GPP routed connectivity is applicable for both trusted and untrusted scenarios, while BBF routed connectivity is only applicable for trusted scenario.

TR-291 does not provide any requirement for routing in the untrusted scenario and relies on requirements defined by 3GPP TS 23.139 [11].

For the trusted scenario, the possible decision points for traffic routing are the UE, the RG and the MS-BNG. Requirements for addressing routing in the trusted scenario are addressed in Section 7 and Section 9.

Regarding mobility, this specification covers IP network-based mobility, but it is agnostic to IP host-based mobility and application mobility. Hence, throughout this Technical Report, mobility pertains to 3GPP routed traffic only. The seamless aspects of mobility are out of scope; the only role of the fixed network being to fulfill S2a (trusted case) or the secured tunnel between a 3GPP device in the subscriber network and a 3GPP network (untrusted case).

5 Fundamental architectures and topologies

This section describes 3GPP-BBF interworking architecture principles for host-based (S2c) and network based (S2b and S2a) mobility management in the context of WT-178 [6].

5.1 Host-based mobility (S2c scenarios)

The figure below depicts 3GPP-BBF interworking in host-based mobility scenarios in the context of WT-178 [6] architecture. It should be noted, however, that a UE could alternately or simultaneously participate in the networks and services provided by the wireline access. This traffic is not shown in the figure.

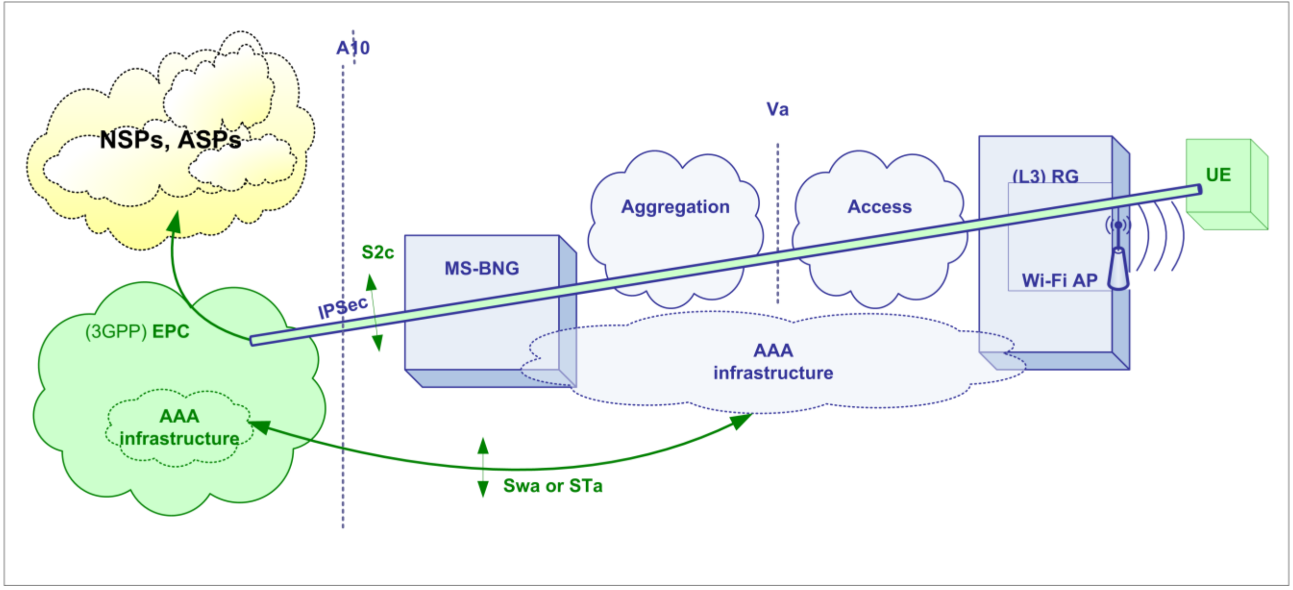

Figure 1 – Interworking for trusted S2c and untrusted S2c scenarios

Note: In trusted S2c there is a tunnel for mobility signaling. In untrusted case there are 2 tunnels: one for mobility signaling, one for user plane.

Whenever “host-based mobility” is required, the UE establishes an IPsec tunnel through the BBF network to a given 3GPP EPC. This doesn’t require any special treatment from the BBF network to support the traffic, but the scenarios are documented in TR-203 [7]. Due to that, there is no S2c specific procedure included in Section 11.

However, requirements on interworking between the fixed and mobile control planes do exist, especially for policy control. They are described in TR-203 [7], and the associated nodal requirements are in Section 8. Once these are added to the base S2c architecture (Figure 1), the resulting architecture looks like Figure 2.

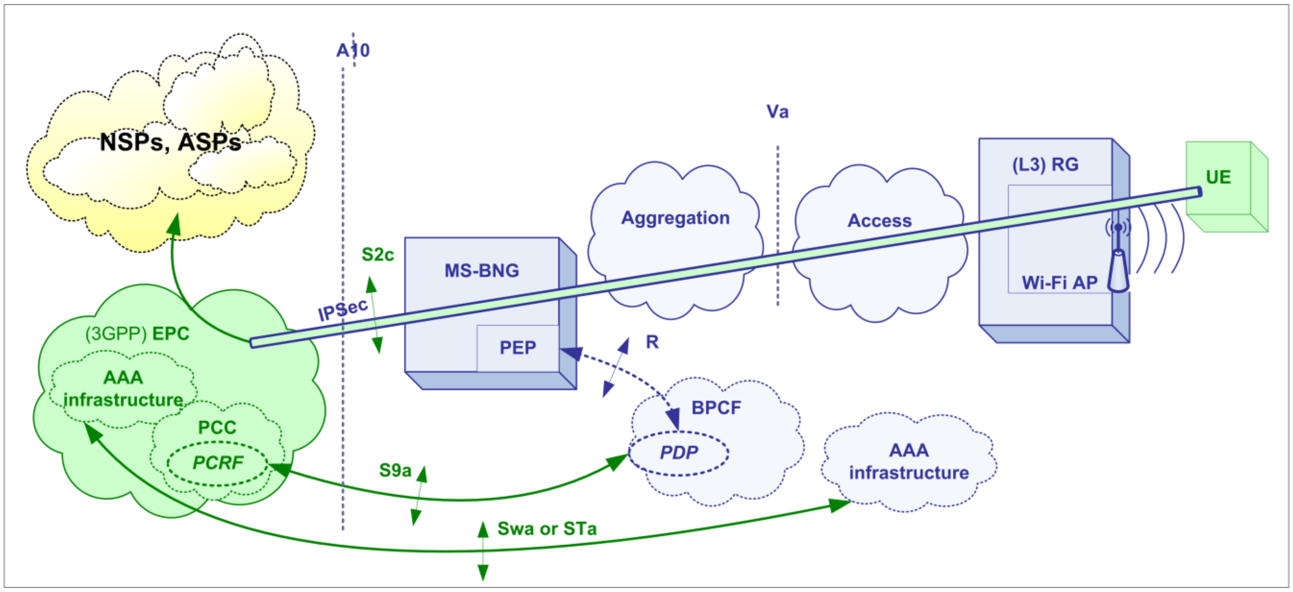

Figure 2 – S2c scenarios with interworking between policy control systems

5.2 3GPP Network-based mobility (S2b)

Figure 3 shows interworking in the context of the WT-178 [6] architecture, for network-based mobility scenarios where the fixed network is untrusted. Note as before that the UE can also natively receive service from the BBF network.

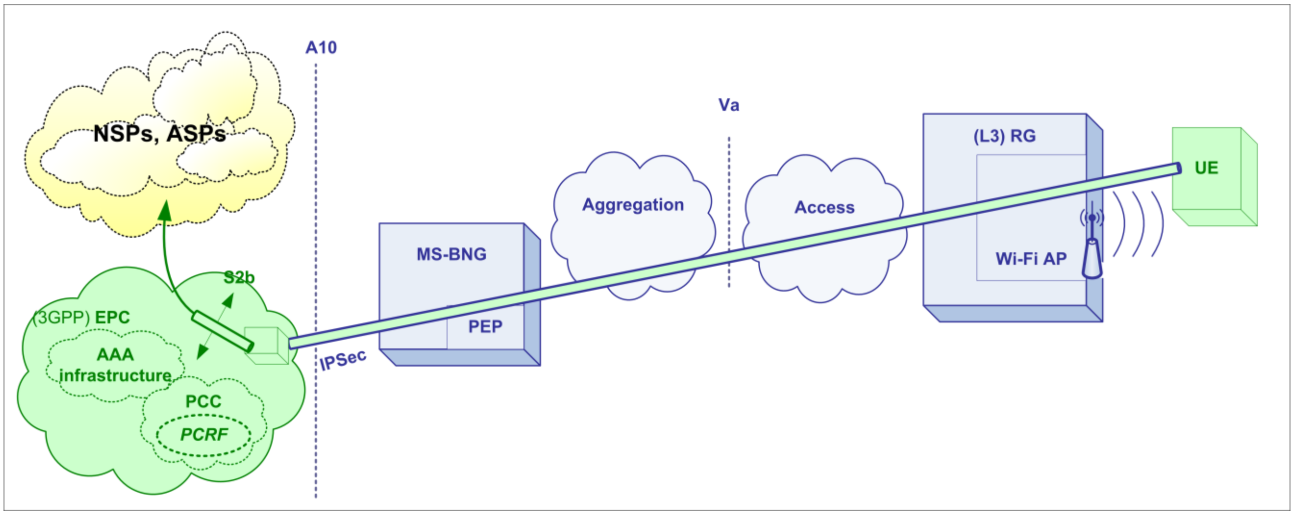

Figure 3 – Interworking for untrusted S2b scenario

In this scenario the gateway providing mobility is located in the 3GPP network because the BBF network is untrusted. The UE establishes an IPsec tunnel to the targeted 3GPP network in order to build a secure point-to-point link between the UE and the mobility gateway.

Figure 4 depicts the collaboration options between fixed and mobile policy control and AAA infrastructure. They are described in TR-203 [7], and the associated nodal requirements are in Section 8.

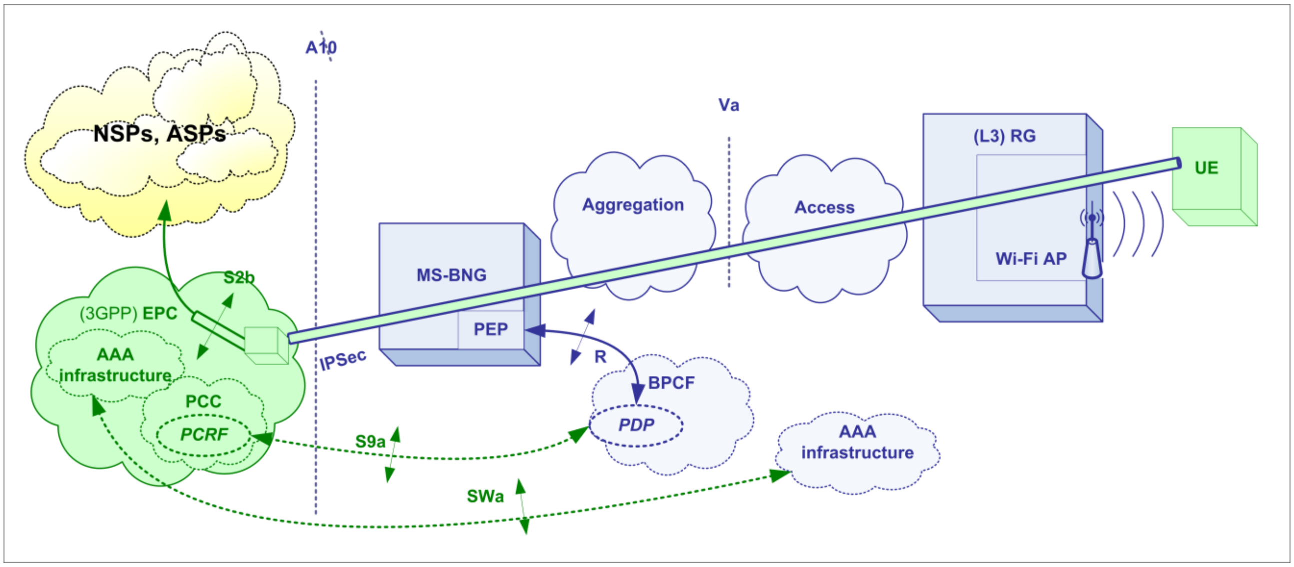

Figure 4 – S2b scenario with interworking between policy control systems

5.3 3GPP Network-based mobility (S2a)

5.3.1 The Trusted WLAN Access Network (TWAN) concept

The TWAN is defined in Section 16/3GPP TS 23.402 [14], and can be seen as a set of requirements to achieve S2a interworking between non-3GPP and 3GPP networks. The TWAN is the construct whereby the 3GPP systems (UE and 3GPP EPC) accept traffic from a trusted BBF network.

- SWw is the reference point providing the link between UE and a Wi-Fi access point.
- STa is the reference point that securely conveys the AAA and mobility information between the 3GPP HSS/AAA server (or proxy in the case of roaming) and the WLAN Access Network.
- S2a is the reference point providing the user and control planes between TWAG and 3GPP Network. It conveys mobility control, QoS Information and subscriber data.

The functions between these interfaces are respectively called: WLAN Access Network, TWAP, and TWAG. Point-to-point user plane connectivity between UE and TWAG is described in Section 7.5.

- The WLAN Access Network (WAN) is the set of APs, one of which terminates the UE’s 802.11 link. It provides forced-forwarding between the UE's 802.11 association and the TWAG in both directions.

- The TWAP is an AAA element that binds the UE’s subscription data held by its 3GPP provider to the MAC Address seen by the WAN. The TWAP provides the TWAG with such information, together with L2 attach/detach events when needed as triggers.

- The TWAG is a GPRS Tunneling Protocol (GTP) peer for the S2a reference point. It also acts as the default router for the UE on its access link, and as a Dynamic Host Configuration Protocol (DHCP) server for the UE. When the TWAN provides access to the 3GPP EPC for the UE, it forwards packets between the UE-TWAG point-to-point link and the S2a tunnel for that UE. The association in the TWAN between the UE the TWAG point-to-point link and the S2a tunnel is based on the UE MAC Address.

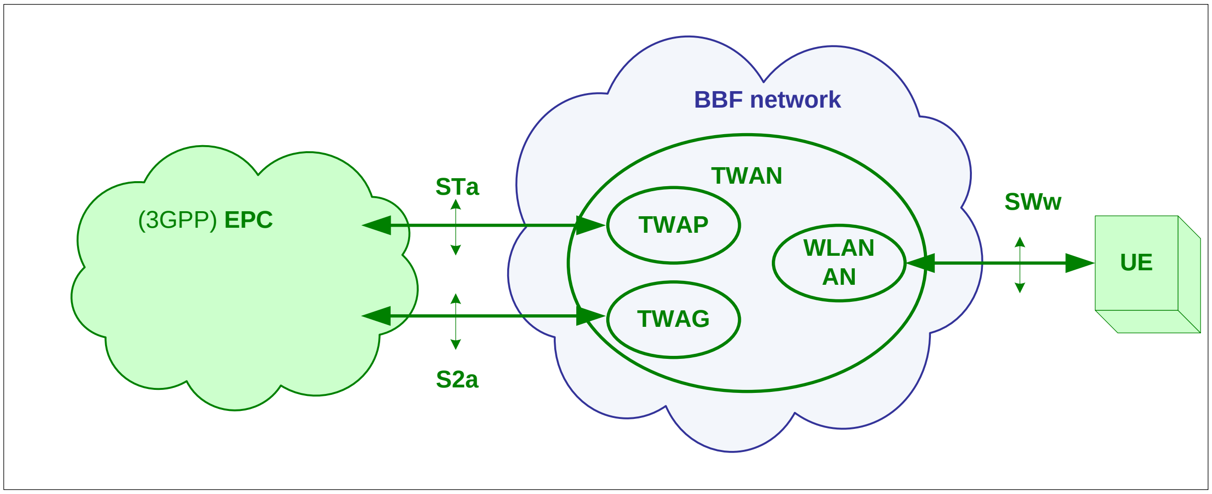

Figure 5 – Interworking for S2a scenario: the TWAN

For 3GPP network based mobility and trusted scenario, the interworking solution supports a non 3GPP TWAN and exposes the SWw, STa and S2a interfaces.

5.3.2 TWAN distribution in WT-178 nodal architecture

5.3.2.1 WLAN Access Network (WAN)

By definition, the TWAN function called WAN can only be located on the Wi-Fi AP.

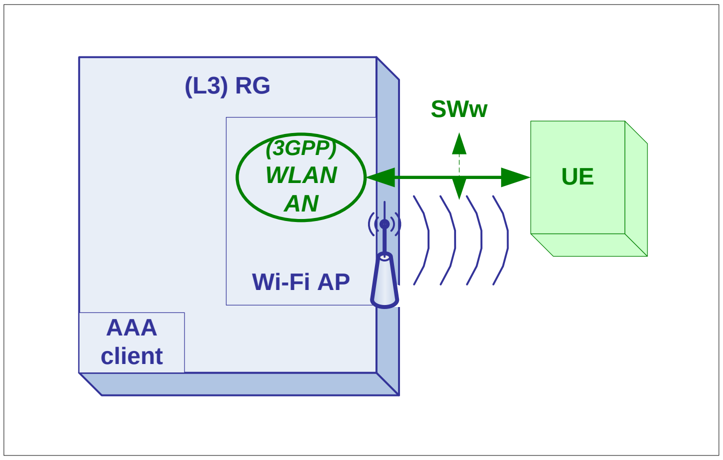

Figure 6 – Location of WLAN Access Network

5.3.2.2 TWAG

The TWAG must be located on a router acting as IP edge for 3GPP routed traffic. This will be one of the following:

- The MS-BNG.
- A dedicated router.
- A mobility service platform beyond A10.

TR-291 only considers the cases where the TWAG is located either on the MS-BNG, or on a dedicated router – which is a Nested BNG devoted to Wi-Fi traffic (dedicated Service Edge router described in WT-178 [6] as part of the MS-BNG concept). Having the mobility service platform beyond A10 is out of scope.

Moreover, for the TWAG located in a dedicated router, the L3 hierarchical MS-BNG architecture is also out of scope.

5.3.2.3 TWAP

The TWAP is part of the control plane.

5.3.3 3GPP Network-based mobility (S2a) architecture options

5.3.3.1 Deployment option 1: MS-BNG acting as a TWAG

Figure 7 shows the case where the MS-BNG acts as a TWAG. This node encompasses at least an AAA client, which could be an AAA proxy.

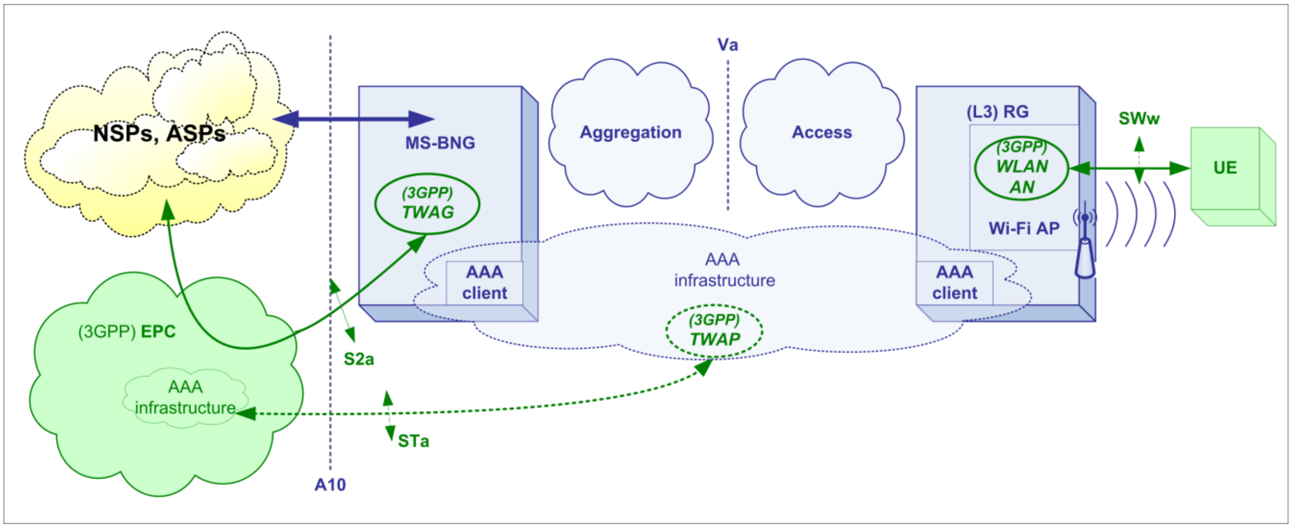

Figure 7 – Trusted scenario with TWAG on MS-BNG

The blue arrow crossing A10 represents possible BBF routed traffic pertaining to the same UE. The node on which forking occurs depends on the mechanism used.

The requirements for deploying the TWAG on MS-BNG architecture are given in Section 7.1.

Policy information is provided through the S2a-GTP and may require an admission control step in the MS-BNG.

5.3.3.2 Deployment option 2: Dedicated Router as TWAG & TWAP

Figure 8 depicts the case where a Dedicated Router is used to achieving both the TWAG and the TWAP functions.

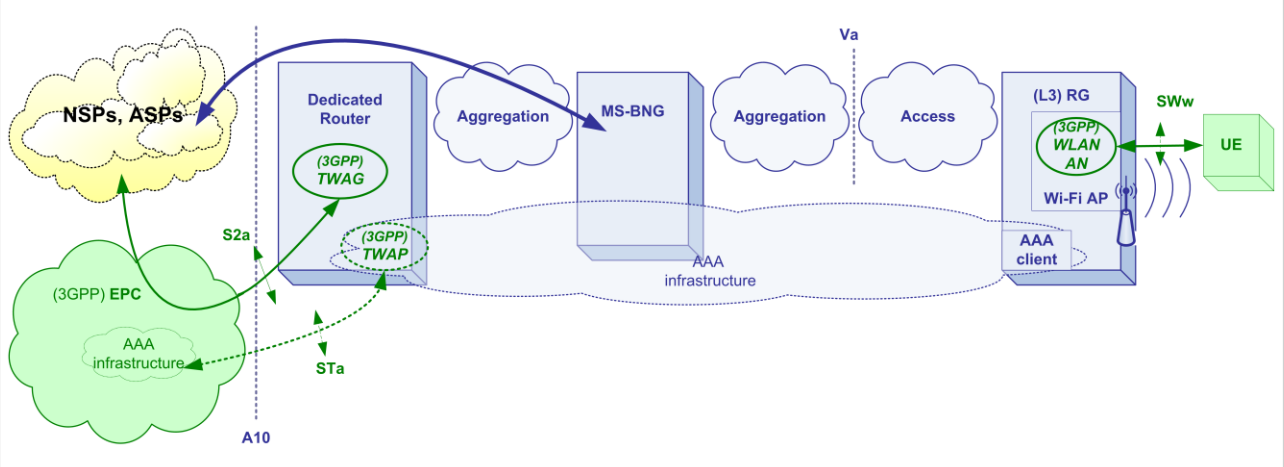

Figure 8 – Trusted scenario with TWAG on Dedicated Router

Policy information is provided through the S2a-GTP and may require an admission control step in the TWAG.

5.4 Mobility in the Femto scenario

TR-203 [7] includes use cases and requirements where a 3GPP UE requests services from the 3GPP network via a Home evolved Node B (H(e)NB) that connects to the BBF access network. Figure 9 shows interworking in the context of WT-178 [6] architecture, for H(e)NB based mobility scenarios.

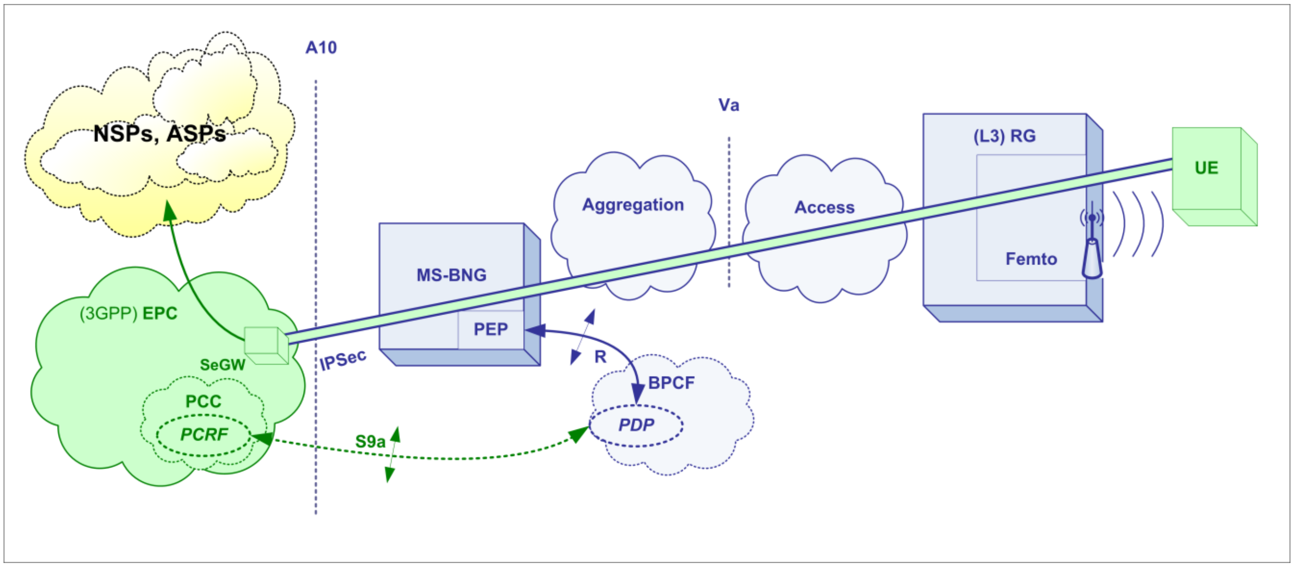

Figure 9 – H(e)NB scenario

Note: Local IP Access (LIPA) is not covered in TR-291 as it is fully described in Section 4.3.16/3GPP TS 23.401 [13], Section 4.4.9/3GPP TS 23.401[13], and Section 5.3.14/3GPP TS 23.060.

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

Note 1: The IPsec tunnel establishment between the H(e)NB (standalone and RG integrated) is per 3GPP TS 33.320 [21].

Note 2: The connection between the MS-BNG and the Security Gateway (SeGW) is IP transport.

Note 3: When the 3GPP and Fixed Broadband access networks belong to different service providers, security arrangements for the PCRF – BPCF connection are the same as for the Fixed Access AAA Server – 3GPP HSS/AAA connection in S2a and S2b scenarios.

Note 4: For non-LIPA traffic from all UEs connected to the Femto is routed to the 3GPP EPC.

Note 5: The UE identity and IP address are not known to the BBF network.

Note 6: Multiple PCRFs may initiate the S9a session.

6 Common nodal requirements for 3GPP trusted (S2a) and untrusted (S2b) network-based mobility, and host-based mobility (S2c)

6.1 RG Requirements

This section provides a set of requirements the RG must meet to support of the architecture described in TR-203 [7].

As per TR-124i3 [2], the RG can be operated in two different modes: bridged or routed. Whenever requirements depend on whether bridged or routed mode is used, this is explicitly indicated in this section.

The role of the RG depends on multiple deployment scenario criteria such as whether Femto access or Wi-Fi access is used, which IP Mobility Mode (IPMM) is used, the 3GPP trust mode and on whether 3GPP UE authentication is used. Section 6.1.2.1 provides an overview of the applicable combinations within the scope of TR-291.

6.1.1 General Requirements

Common requirements include the way the RG prioritizes packets exchanged between the 3GPP core network and the UE inside the customer premises network. The level of granularity of the rules defining the prioritization method depends on how deep the RG can inspect packets. While in most cases, the RG just acts as a router or bridge transporting tunnels on top of the IP protocol, in the S2a case (as can be seen below), the RG has more granular means as it can "see" the plain IP packets without tunnel headers and encryption preventing it from doing so. The following requirements apply per UE.

[R-1] The RG MUST be able to prioritize IP packets exchanged between UE and 3GPP network in both, uplink and downlink direction in the case where IP-based tunnels are used to carry the UE's traffic.

[R-2] The RG MUST be able to prioritize IP packets in both, uplink and downlink direction in the case where no IP-based tunnel is used to carry the UE's traffic.

[R-3] The RG MUST support IP packet prioritization based on pre-configured policies.

[R-4] The RG MUST be able to generate local prioritization rules based on the result of a successful access authentication procedure for that UE.

[R-5] The RG MUST be able to receive prioritization rules from the Fixed Access AAA Server in case UE authentication is applied.

6.1.2 Wi-Fi Access Requirements

6.1.2.1 3GPP modes

In interworking scenarios, the role of the network nodes depends on the 3GPP IPMM used, the trust level and whether the UE is to be authenticated during network attachment. 3GPP TS 24.302 [15] specifies how the IPMM is selected. While UE authentication is mandatory for S2a trusted access, it is optional for other access cases since in these cases a tunnel authentication is always executed.

Table 1 – Overview of combinations of 3GPP mobility modes, trust relationship and UE authentication in BBF network

IPMM	**Trust relationship between BBF and 3GPP network**	**UE authentication in BBF network with 3GPP Identity**
S2a (GTP)	Trusted	Mandatory
S2b (PMIP/GTP)	Untrusted	Optional
S2c (client-based, DSMIPv6)	Trusted	Optional
S2c (client-based, DSMIPv6)	Untrusted	Optional

For the S2a case, there is no IP-based tunnel specified by the 3GPP between UE and TWAG. Thus, the BBF network must provide a means to transport these IP flows between UE and TWAG although they do not use UE IP addresses that can be routed inside the BBF network. The BBF network elements such as RG and TWAG transport plane IP packets and are thus able to apply more granular policies to the UE’s traffic.

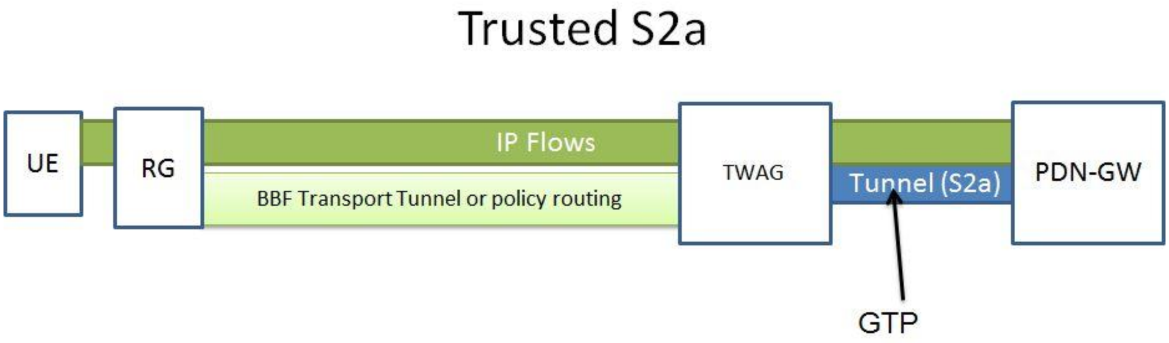

Figure 10 – S2a: RG is only aware of UE’s plain IP packets

From the RG viewpoint, the S2b and S2c modes run “over the top”. The RG just routes IP packets that transport the tunneled traffic towards the 3GPP core. If UE access authentication is applied, the RG can be dynamically made aware of the tunnels.

The following figure depicts this situation for S2b and S2c. The end-to-end IP traffic to and from the UE is encapsulated inside one or more IP-based tunnels. The RG will only be able to detect the outer headers of these tunnels. The tunneled IP traffic uses IP addresses from the 3GPP core network's address space.

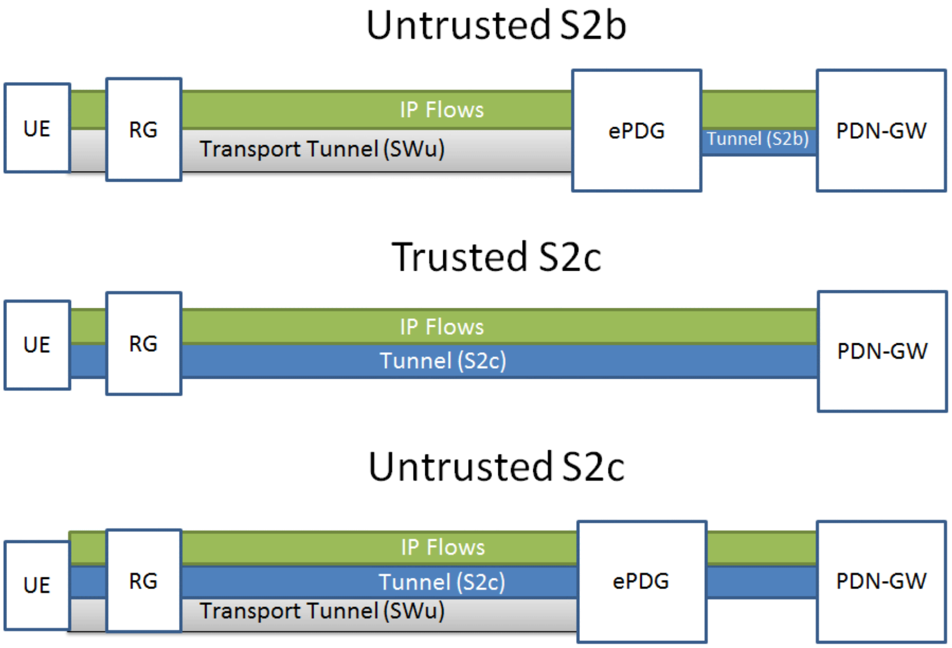

Figure 11 – S2c and S2b: RG is only aware of tunnels over IP

6.1.2.2 UE Authentication Support

S2a-based interworking requires IEEE 802.1X-based UE authentication where the RG acts as authenticator. In general, UE authentication enables the RG to learn that a 3GPP UE attaches to the customer premises network even where it later uses an over-the-top tunnel to connect to the 3GPP network. Thus, this procedure may also be used for S2b and S2c.

During authentication (for instance, steps 1 to 8 in Section 11.1.1.1), the UE attaches to the network and the RG sends an EAP-ID request over the Wi-Fi interface to the UE. The UE will reply with an EAP-ID response message containing its identity. The subsequent backend messages sent and received by the RG from the Fixed Access AAA Server are transported using RADIUS. The Fixed Access AAA Server itself will query the 3GPP HSS/AAA server via the RADIUS/Diameter translation function.

Upon successful authentication, the RADIUS EAP success will be received by the RG and delivery to the UE. The UE can then start acquiring an IP address from the 3GPP network domain. This is the IP address assignment process (for instance, steps 9 to 12 in Section 11.1.1.1), where the RG proxies a DHCP request to either MS-BNG or TWAG.

During regular user plane traffic, the UE will exchange IP packets using the address space from the 3GPP network via the PDN GW. During this operation, upon events generated by the network or user interaction additional policies can be evoked/installed on the RG using the RADIUS Change-of-Authorization (CoA) procedure.

[R-6] For S2a support, the RG MUST be able to act as an 802.1X authenticator using a RADIUS client connected to a Fixed Access AAA Server.

[R-7] For S2a support, the RG MUST support proxying EAP-AKA/EAP-AKA’ messages over RADIUS (RFC 3579 [28]), using an internal RADIUS client.

[R-8] The Fixed Access AAA Server MUST insert the ANID AVP (defined in 3GPP TS 33.402 [22]) set to WLAN on the STa interface for EAP-AKA’ authentication received from a RADIUS client in the RG.

[R-9] For supporting the untrusted scenario (S2b and S2c), the RG SHOULD support UE authentication based on IEEE 802.1X as authenticator using a RADIUS client connected to a Fixed Access AAA Server.

Within the RADIUS Access Accept message or using subsequent RADIUS CoA messages, the RG may be instructed to install policies, e.g. rules to prioritize traffic, firewall rules accounting policies, enable local traffic offloading, grant access to local or remote services, add Layer 2 tunnel headers on the uplink, etc.

[R-10] The RG MUST be able to receive policies from the Fixed Access AAA Server during UE authentication and during an ongoing session using RADIUS CoA as per RFC 5176 [32].

[R-11] The RG MUST be able to have pre-configured policies to handle UE traffic or to download such policies via RADIUS from the Fixed Access AAA Server during authentication or by using RADIUS CoA.

6.2 Fixed Access AAA Server Requirements

This section provides a set of requirements the Fixed Access AAA Server must fulfill in support of the architecture described in TR-203 [7].

[R-12] The Fixed Access AAA Server MUST support proxying the authentication signaling to the AAA server in 3GPP network for the 3GPP UE.

[R-13] The Fixed Access AAA Server MUST support the Translation Agent function as defined in R-62/TR-203 [7] when STa is terminated in the Fixed Access AAA Server.

[R-14] The Translation Agent MUST support Diameter on STa reference point as specified in 3GPP TS 29.273 [17].

[R-15] During the 3GPP Access Authentication process, and at the reception of the authentication confirmation from the 3GPP HSS/AAA including the 3GPP IMSI (as described in R-59/TR-203 [7]), the Fixed Access AAA Server MUST report the received 3GPP IMSI to the TWAG.

[R-16] If the S2a tunnel set-up fails, the Fixed Access AAA Server MUST report it to the 3GPP HSS/AAA.

[R-17] The Fixed Access AAA Server MUST be able to forward the accounting packets received for the 3GPP UE to the 3GPP HSS/AAA server via the STa/SWa reference point.

[R-18] If BBF routed traffic is allowed as part of inter-operator agreements, the Fixed Access AAA Server MUST indicate this to the MS-BNG via the Non-Seamless WLAN Offload – Access Point Name (NSWO-APN).

[R-19] The Fixed Access AAA Server MUST instruct the TWAG to disconnect the UE from the Fixed Broadband network upon receipt from 3GPP HSS/AAA of an indication to terminate the UE connection (e.g. the UE has run out of credit).

[R-20] The Fixed Access AAA Server MUST send a response indicating the result of disconnection procedure described in [R-19].

[R-21] The Fixed Access AAA Server MUST be able to receive the following from 3GPP HSS/AAA via STa reference point:

- Whether access to EPC is allowed for the UE on the TWAN;
- When the UE is allowed to access EPC via TWAN, the default APN to be associated with the user for EPC access;
- The subscriber MSISDN.

[R-22] The Fixed Access AAA Server MUST be able to forward the information received per requirement [R-21] to the TWAG.

6.3 BPCF Requirements

Note: BPCF and S9a are not involved in 3GPP trusted Network-based mobility (S2a).

[R-23] The BPCF MUST support the S9a interface as per 3GPP specifications in 3GPP TS 29.215 [16].

[R-24] The BPCF MUST be able to accept the PCRF-triggered Gateway Control Session establishment.

[R-25] The BPCF MUST be able to establish the S9a Gateway Control Session in response to the trigger in [R-24].

[R-26] For S9a Gateway Control Session establishment triggered from the PCRF, the BPCF MUST be able to associate the S9a Gateway Control session with the corresponding session over the R-interface based on the Local IP address of the IPsec tunnel (i.e. the RG's IP address) it receives from the PCRF.

[R-27] When an S9a Gateway Control Session Termination or an IP-CAN Session Termination request from the PCRF is received, the BPCF MUST inform the MS-BNG of the request for session termination.

[R-28] The BPCF MUST support the PCRF initiated S9a IP-CAN session termination procedure.

[R-29] When a request for 3GPP UE session termination is received from the MS-BNG over the R-interface, the BPCF MUST report the corresponding session termination to the PCRF using S9a IP-CAN Session Termination procedures.

[R-30] The BPCF MUST ignore the Service Data Flow Templates provided by the PCRF for the 3GPP Routed traffic as indicated in Annex P/3GPP TS 23.203 [12].

[R-31] The BPCF MUST be able to map PCC rules and/or QoS Rules received over the S9a interface into equivalent BBF policy parameters defined in TR-134 [3].

[R-32] If the MS-BNG reports an available QoS to the BPCF, the BPCF MUST be able to report it to the 3GPP PCRF via S9a interface.

[R-33] For admission control purposes, the BPCF MUST be able to receive a resource reservation request from 3GPP PCRF with the requested QoS parameters (i.e. UL/DL bandwidth, QCI and Allocation and Retention Priority). The resource reservation request is part of the S9a Gateway Control Session Modification procedure described in 3GPP TS 23.139 [11].

[R-34] The BPCF MUST be able to authorize the request for resources from the PCRF by using service policy rules defined by the network operator.

[R-35] If the BPCF receives packet filters for admitted flows from the PCRF over S9a interface, then the BPCF MUST provide them to the MS-BNG.

6.4 Access Node Requirements

TR-291 has no impact on ANs.

6.5 Visited Public Land Mobile Network (VPLMN) information at the 3GPP UE

VPLMN information may be gathered in the BBF domain via 3GPP access authentication. Support for RFC 4284 [31] provides the 3GPP UE with information to facilitate network selection (e.g. a list of roaming partners of the access network). This list can be provided to the RG in a RADIUS EAP-

Request/Identity message during the RG authentication process, or by local configuration at the RG. Subsequently, this information is provided to the UE via a RADIUS EAP-Request/Identity message.

[R-36] The Fixed Access AAA Server MUST be able to be configured to provide the list of available VPLMNs (VPLMN Identifiers list) to the 3GPP UE in EAP message during the EAP-based authentication.

[R-37] The Fixed Access AAA Server MUST provide the VPLMN Identifier selected during the 3GPP UE authentication phase to the MS-BNG (if the MS-BNG does not proxy RADIUS messages).

[R-38] The MS-BNG MUST provide the VPLMN Identifier to the BPCF over the R reference point when IP-CAN Session establishment for the 3GPP UE is requested.

[R-39] When the BPCF receives a VPLMN Identifier, the BPCF MUST use it at IP-CAN Session Establishment in order to address the V-PCRF in the VPLMN.

7 Nodal requirements for 3GPP trusted Network-based mobility (S2a)

7.1 TWAG Requirements

[R-40] The TWAG MUST support binding the UE MAC Address (obtained from RADIUS) and IMSI of the 3GPP UE to support IP address allocation of the UE.

[R-41] The TWAG MUST trigger the establishment of GTP session with the PDN GW on S2a reference point using the 3GPP subscription attributes obtained through the authentication process ([R-21] and [R-22]).

[R-42] The TWAG MUST support binding the UE MAC Address (obtained from RADIUS) and IP address of the 3GPP UE in order to forward the downstream traffic.

[R-43] When the S2a tunnel set-up is based on a layer 2 trigger (as described in Section 11.1.1), and the TWAG and the TWAP are not collocated, the TWAG MUST support a RADIUS proxy.

[R-44] When the subscriber session is terminated as defined in Section 5.7/TR-146 [5], the TWAG MUST trigger the PDN disconnection procedure on S2a by sending a GTP Delete Session Request message to the PDN GW.

[R-45] When the subscriber session is terminated as defined in Section 5.7/TR-146 [5], the TWAG MUST stop the accounting session for the UE.

[R-46] The TWAG MUST trigger the PDN Disconnection procedure on S2a by sending a GTP Delete Session Request message to the PDN GW when it receives indication from the TWAP to terminate the UE connection (e.g. the UE has run out of credit).

[R-47] The TWAG MUST remove the UE session from the Fixed Broadband network when it receives an appropriate AAA request from the EPC network.

[R-48] The TWAG MUST support the GTPv2 protocol as specified for control plane by 3GPP TS 29.274 [18] and for user plane by 3GPP TS 29.281 [19]. The GTP-C control messages applicable to TWAG are listed in Table 6.1-1/3GPP TS 29.274 [18].

[R-49] When the TWAG receives a GTP Delete Bearer Request message via S2a, the TWAG MUST initiate the release of the resource on BBF access associate with the 3GPP EPC Bearer.

[R-50] When the resources are released per requirement [R-49], the TWAG MUST send a GTP Delete Bearer Response message to PDN GW via S2a reference point with the result of the procedure.

[R-51] The TWAG MUST use the default APN received from Fixed Access AAA Server per requirement [R-21] to establish the PDN connection with the PDN GW in GTP tunnel on S2a reference point.

[R-52] The TWAG MUST send a response to the Fixed Access AAA Server indicating the result of disconnection procedure requested by the Fixed Access AAA Server in requirement [R-19].

[R-53] The TWAG MUST be able to obtain the Basic Service Set Identifier (BSSID) and the Service Set Identifier (SSID) from the TWAP if the TWAG doesn't proxy the authentication messages during 3GPP UE access authentication.

[R-54] If the TWAG proxies the RADIUS authentication messages during 3GPP UE access authentication, the TWAG MUST be able to extract the BSSID and the SSID from such RADIUS authentication messages.

[R-55] The TWAG MUST be able to provide the BSSID and the SSID to the PDN GW via S2a.

[R-56] The TWAG MUST be able to map between QoS parameters provided by 3GPP via S2a reference point (i.e. transported by GTPv2-C protocol) and the QoS parameters defined by the BBF.

7.2 TWAP requirements

[R-57] The TWAP MUST support binding the UE MAC Address (obtained from RADIUS) and IMSI of the 3GPP UE to support IP address allocation of the UE.

[R-58] The TWAP MUST be able to run Diameter on STa and RADIUS on B and towards RGs.

7.3 MS-BNG requirements

[R-59] The MS-BNG MUST be able to proxy the RADIUS authentication messages of the 3GPP UE to the TWAG based on Network Access Identifier (NAI) when the MS-BNG and the TWAG are separated.

[R-60] The MS-BNG MUST be able to map between core facing outer IP traffic classes and the Ethernet priority field for packets in the access network.

7.4 RG requirements

The BBF network needs to ensure that IP packets can be forwarded between RG and TWAG even when their IP address belong to a different domain.

[R-61] The RG MUST support routing policies to forward packets for 3GPP UEs.

[R-62] The RG MUST be able to insert the MAC Address of the 3GPP UE into the Calling-Station-Id attribute of the RADIUS authentication messages during 3GPP UE access authentication.

[R-63] The RG MUST be able to insert the Homogenous Extended Service Set Identifier (HESSID) – when there is only one Access Point, the HESSID is the BBSID, i.e. the MAC Address of the AP – and the SSID used by the 3GPP UE to access the EPC into RADIUS the authentication message during the 3GPP UE access authentication.

Note: RFC 3580 [29] provides support to BSSID and SSID information on RADIUS messages.

[R-64] The RG MUST support a dedicated WAN-side logical interface for carrying the UEs traffic.

[R-65] The RG MUST be able to bind a UE to an 3GPP routed Virtual Local Area Network (VLAN)/Tunnel or BBF routed VLAN based on AAA indication and/or local configuration.

[R-66] The RG MUST be able to stop the L2 session between the UE and RG based on IEEE 802.11 dissociation message from the UE.

[R-67] The RG MUST be able to terminate IP session as described in Section 5.7/TR-146 [5].

7.5 BBF transport tunnel implementation between UE and TWAG in S2a scenario

For 3GPP Routed traffic, the UE-TWAG connectivity is point-to-point. The point-to-point link is used for forwarding packets from the UE to TWAG and packets from the TWAG to the UE.

7.5.1 General requirements

In the case where UEs on the same subnet need to communicate via IPv4, they will send an ARP request to resolve the IP address of their correspondent (see Section 3.2.4/RFC 5844 [33]).

[R-68] The UE traffic MUST be bridged along the path between UE and TWAG in both directions.

[R-69] The TWAG MUST be able to act as an Address Resolution Protocol (ARP) proxy for 3GPP UE IPv4 addresses and for Default Gateway IPv4 address within the IPv4 subnet advertised via DHCP.

A UE’s HPLMN allocates only one prefix per UE for mobility support.

[R-70] The TWAG MUST advertise the prefix allocated from its HPLMN to IPv6 3GPP UE.

Note: In the 3GPP roaming scenario, the prefix is allocated by the VPLMN for supporting traffic terminated in the VPLMN.

Unsolicited RAs sent by the TWAG may contain prefixes meant for other devices:

[R-71] The TWAG MUST support sending periodic and solicited multicast RA messages to the unicast MAC Address of the 3GPP UE learnt during 3GPP UE authentication.

[R-72] The TWAG MUST forward traffic received from the UE onto the specific S2a tunnel for the UE selected on the basis of the UE's MAC Address.

[R-73] The TWAG MUST be able to forward traffic received from the S2a tunnel to the 3GPP UE, by mapping the IP packet to the Ethernet frames and then encapsulating or tagging the Ethernet frames with the destination MAC Address set to that of the 3GPP UE into the P2P tunnel between RG and TWAG.

[R-74] The TWAG MUST support bridged Generic Routing Encapsulation (GRE) encapsulation on the access side as defined in RFC 2784 [27].

[R-75] The TWAG SHOULD support bridged Layer 2 Tunneling Protocol version 3 (L2TPv3) encapsulation on the access side as defined in RFC 3931 [30].

[R-76] The TWAG SHOULD support VLAN encapsulation on the access side as defined in IEEE 802.1Q [24].

[R-77] The RG MUST support bridged GRE encapsulation on the WAN side as defined in RFC 2784 [27].

[R-78] The RG SHOULD support bridged L2TPv3 encapsulation on the WAN side as defined in RFC 3931 [30].

[R-79] The RG SHOULD support VLAN encapsulation on the WAN side as defined in IEEE 802.1Q [24].

[R-80] The RG MUST be able to relay traffic between the 3GPP UE and the TWAG, using one of the encapsulations defined in [R-77], [R-78] or [R-79].

7.5.2 Layer 2 Point-to-Point connectivity between UE and TWAG based on dedicated tunnels, RG in Bridge mode

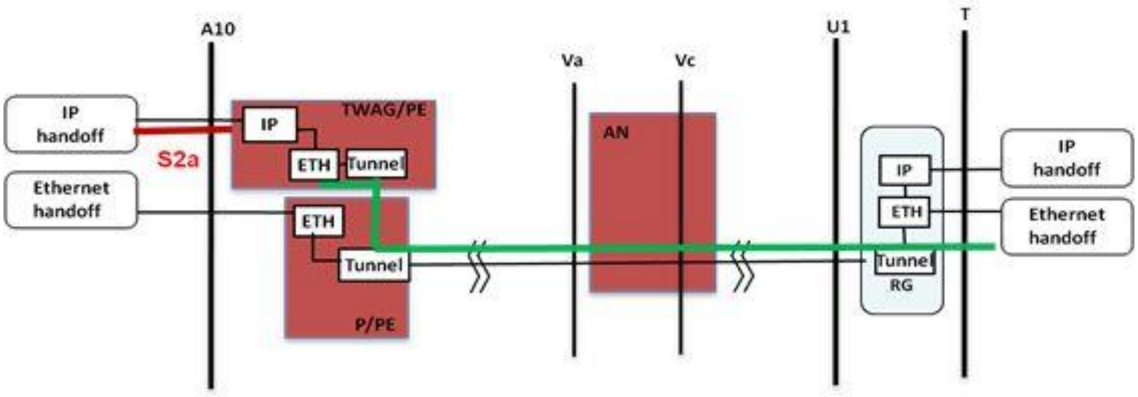

Figure 12 – Transport tunnel for Point to Point link

The procedure for traffic is as follows:

- The link between the UE and RG is layer 2. The UE’s MAC Address is embedded.
- The RG works in bridge mode and transmits the traffic between UE and TWAG.
- The TWAG can use the UE’s MAC Address to identify the UE and to associate the transport tunnel with the S2a tunnel. The TWAG selects the tunnel for the UE. So in order to guarantee a point-to-point link between UE and TWAG, the TWAG must select one specific tunnel for the UE. It could be achieved by binding the UE’s MAC Address to the tunnel identifier.

The traffic must be tunneled to the TWAG. The TWAG binds the transport tunnel to the S2a tunnel in both directions, based on UE’s MAC Address. The tunnel technology must preserve the L2 frame information, and so the following requirements apply.

[R-81] If the RG is the transport tunnel end point, the RG MUST bind the UE traffic to a specific transport tunnel on the basis of the UE’s MAC Address.

[R-82] If the RG is the Authenticator, the RG MUST be able to receive the 3GPP indication send by 3GPP HSS/AAA and forwarded by Fixed Access AAA Server during the authentication whether the traffic shall be 3GPP routed or BBF routed.

[R-83] RG MUST be able to distinguish the UE BBF routed traffic and the 3GPP routed traffic based on the 3GPP indication during authentication and to bind the traffic to a specific transport tunnel.

7.5.3 Layer 2 point-to-point connectivity between UE and TWAG based on Layer 2 isolation, RG in Bridge mode

A L2 point-to-point link between UE and TWAG can be achieved directly in the existing BBF infrastructure providing that L2 isolation is performed locally by each of the L2 forwarding devices. TR-101i2 [1] says: "User isolation means that the user/subscriber does not have direct bi-directional connectivity at the Ethernet MAC layer to any other user/subscriber in the RBN. This needs to be enforced in all nodes between the U interface and the MS-BNG(s)."

[R-84] The underlying infrastructure between RG and TWAG MUST comply with TR-101i2's requirements for L2 traffic isolation.

[R-85] The RG MUST be able to achieve user isolation for 3GPP UEs on its ingress Wi-Fi interfaces.

[R-86] The TWAG MUST be able to cope with potential duplicate IPv6 link-local-addresses for distinct 3GPP IPv6 UEs in one of the following ways:

- The TWAG MUST support a mechanism that allows sending distinct IPv6 messages to distinct UEs with the same link-local address based on using the unicast MAC Address of the UE as learned during authentication phase.
- The TWAG MUST support a mechanism to prevent more than one subscriber in the same broadcast domain from using the same link-local address.

The choice of the mechanism is an implementation decision as it does not affect interoperability between the TWAG, RG and UE.

[R-87] The RG MUST be configurable to bind the traffic associated with an SSID to the appropriate logical WAN interface.

7.5.4 P2P “tunnel over IP” establishment methods

7.5.4.1 Data plane triggered tunnel establishment

Once a UE is successfully authenticated, the first frame it sends is encapsulated and forwarded by the RG to the TWAG, using pre-provisioned parameters. Upon receiving this frame, the TWAG binds the UE MAC Address to the tunnel in order to properly forward packets in the other direction (and possibly to perform anti-spoofing).

[R-88] The RG MUST be able to be configured with a primary TWAG IP address and tunnel parameters.

[R-89] The RG SHOULD be able to be configured with a secondary TWAG IP address and tunnel parameters.

[R-90] The TWAG MUST create a binding between the UE MAC Address, the RG IP address and the tunnel parameters.

[R-91] The TWAG MUST manage the binding between the UE MAC Address, the RG IP address and the tunnel parameters.

7.5.4.2 Control plane triggered tunnel establishment

[R-92] If the tunnel establishment is done by the RG, the RG MUST insert its IP address, tunnel parameters into the RADIUS-Access-Request messages during the 3GPP UE access authentication.

[R-93] If the tunnel establishment is done by the TWAG, the TWAG MUST insert its IP address, tunnel parameters into the RADIUS-Access-Accept messages if the TWAG proxies the authentication messages during the 3GPP UE access authentication.

[R-94] If the tunnel establishment is done by the TWAG, the TWAG MUST be able to store a set of authorized RG IP address/prefixes with which it can configure a bridged GRE route if the TWAG doesn’t proxy the authentication messages during the 3GPP UE access authentication.

8 Nodal requirements for 3GPP untrusted Network-based mobility (S2b) and host-based mobility (S2c)

8.1 MS-BNG Requirements

This section provides a set of requirements the MS-BNG must fulfill in support of the architecture described in TR-203 [7].

[R-95] After a successful RADIUS Accounting establishment, the MS-BNG MUST provide the IMSI, the assigned local UE IP address and the APN (if available) to the BPCF over the R-reference point.

[R-96] The MS-BNG MUST perform the admission control based on the 3GPP UE requested resources – Uplink (UL)/Downlink (DL) bandwidth – indicated by the BPCF, and resource availability.

[R-97] If the MS-BNG does not accept the requested resource reservation, then the MS-BNG MUST be able to report the available QoS to the BPCF.

[R-98] If the MS-BNG cannot maintain the committed resource reservation, then the MS-BNG MUST be able to report the available QoS to the BPCF.

[R-99] For 3GPP Routed traffic, the MS-BNG MUST be able to schedule traffic based on the Differentiated Services Code Point (DSCP) markings of any packets that match the received packet filters from the BPCF.

[R-100] The MS-BNG MUST be able to apply local policies to any packets that don't match the received packet filters provided by the BPCF.

9 Nodal requirements for BBF routed connectivity support

9.1 MS-BNG Requirements

[R-101] The MS-BNG MUST perform admission control based on the 3GPP UE requested resources (UL/DL bandwidth) indicated by the BPCF and resource availability.

[R-102] In order to enable BBF routed traffic, the MS-BNG MUST provide the NSWO-APN, received previously from the Fixed Access AAA Server, to the BPCF over the R-reference point.

9.2 BPCF Requirements

[R-103] If BPCF configuration indicates that policy control for BBF Routed traffic needs to be provided, upon reception of a 3GPP UE IMSI and assigned local UE IP address the BPCF MUST initiate S9a IP-CAN session establishment with the 3GPP PCRF.

[R-104] At S9a IP-CAN session establishment (see [R-103]), the BPCF MUST provide the 3GPP UE IMSI, the local UE IP address and the NSWO-APN to the 3GPP PCRF.

[R-105] The BPCF MUST be able to find the PCRF based on identity parameters (e.g. IMSI, NSWO-APN, 3GPP UE's local IP address) provided by the MS-BNG once the 3GPP UE has been successfully authenticated.

[R-106] The BPCF MUST be able to send the IP address of the Traffic Detection Function (TDF) that performs packet inspection of the traffic for a given user as part of IP-CAN session establishment for BBF routed traffic over S9a based on local configuration.

Note: This requirement is only applicable when fixed and mobile domains are owned by the same operator.

10 Nodal requirements for Femto access

10.1 RG requirements

10.1.1 Downstream Packet Handling

For the H(e)NB case, the PDN GW in the 3GPP domain sets a per-flow DSCP marking on each packet outer header, as defined in 3GPP TS 23.401 [13].The SeGW copies the DSCP marking to the DSCP field of the outer header of the IPsec tunnel.

Note: DSCP remapping may be performed in the IP network that interconnects the 3GPP and BBF network domains.

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

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

[R-107] The RG MUST be able to prioritize IP packets exchanged with the 3GPP network in the downstream direction based on the DSCP code of the IPsec tunnel outer header.

[R-108] The RG MUST be able to perform the prioritization described in [R-107] based on policies that are preconfigured.

10.1.2 Upstream Packet Marking

DSCP marking for upstream packets is performed by the H(e)NB. The H(e)NB then copies the DSCP from the inner header to the outer header to ensure the correct QoS treatment in the tunnel.

[R-109] The RG MUST be able to prioritize IP packets exchanged with the 3GPP network in the upstream direction based on the DSCP code of the IPsec tunnel outer header.

10.2 MS-BNG Requirements

[R-110] The MS-BNG MUST be able to perform admission control based on the 3GPP UE authorized resources (UL/DL bandwidth, priority) received from the BPCF over the R-interface.

[R-111] The MS-BNG MUST be able to identify H(e)NB/Femto flows based on the Local IP address of the IPsec tunnel and source User Datagram Protocol (UDP) port it receives from the BPCF.

[R-112] The MS-BNG MUST be able to schedule H(e)NB/Femto EPC traffic based on the DSCP markings for the Femto IP flow received from the BPCF.

[R-113] The MS-BNG MUST terminate the RG subscriber IP session when it receives a RADIUS Disconnect message from the Fixed Access AAA Server.

10.3 BPCF Requirements

[R-114] The BPCF MUST support one and only one S9a session per H(e)NB.

11 Procedures and call flows for interworking between Next Generation Fixed and 3GPP Wireless networks

This section describes the procedures and signaling flows required for enabling wireline & wireless interworking.

11.1 Procedures for S2a based mobility

11.1.1 Initial attach based on layer 2 trigger

11.1.1.1 IPv4 address via DHCPv4

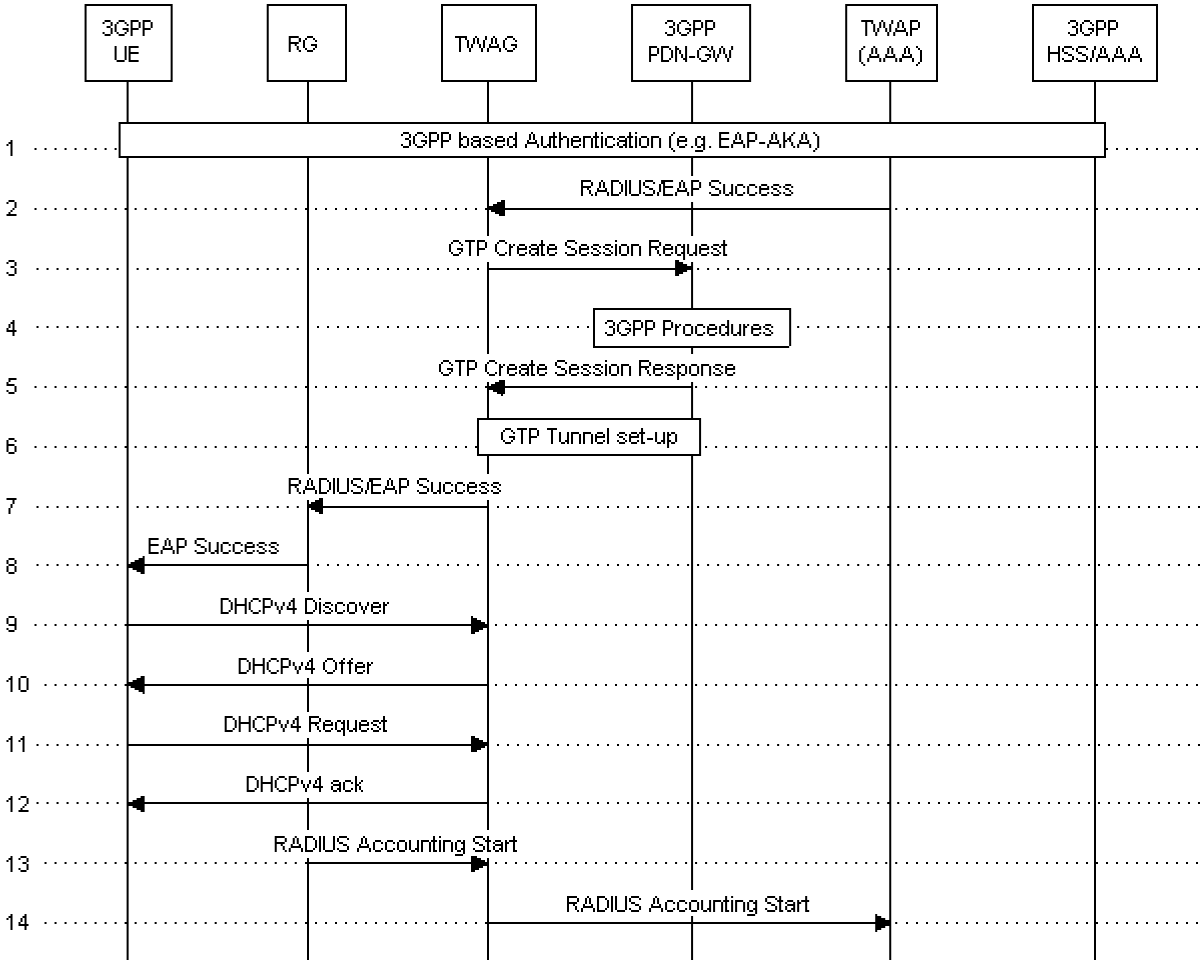

Figure 13 – Initial Attach on GTP S2a – IPv4 address via DHCPv4

1. The 3GPP UE attaches to the BBF access network, and initiates the EAP authentication process (see 3GPP TS 33.402 [22]). During the authentication phase, the RG acts as an

802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS Request message.

The TWAG is involved as an AAA proxy and DHCP server for the 3GPP UE.

When the TWAG is deployed in a dedicated router, the MS-BNG is involved as an AAA proxy and DHCP relay for the 3GPP UE, distinguishing 3GPP UE signaling from fixed device signaling based on NAI.

2. In the case of successful authentication (i.e. RADIUS EAP Accept received), the TWAP sends the RADIUS Accept message to the TWAG, including an indication as to whether it supports S2a, 3GPP UE IMSI and APN retrieved from the 3GPP Domain.

3. If the indication is to establish an S2a GTP tunnel, the TWAG sends a Create Session Request message to the PDN GW, including 3GPP UE IMSI.

4. 3GPP domain starts the IP-CAN Session Establishment procedure as defined by 3GPP TS 23.203 [12]. As a result of this procedure, an IP address is allocated to the UE.

5. The PDN GW returns a Create Session Response, including the IP address allocated for the 3GPP UE.

6. The GTP tunnel is set up between the TWAG and the PDN GW.

7. The TWAG proxies the RADIUS EAP Success message received at Step 2 to the RG.

8. The RG sends RADIUS EAP Success to the 3GPP UE. The 3GPP UE is now authenticated, and the BBF access is considered as trusted by the 3GPP Network.

9. The 3GPP UE sends a DHCP Discover message.

10. The TWAG sends a DHCP Offer including the IPv4 Address allocated by the PDN GW to the 3GPP UE.

11. The 3GPP UE responds by sending a DHCP Request message upstream to the TWAG.

12. The TWAG responds with a DHCP Ack.

13. The RG sends a RADIUS Accounting Start.

14. The TWAG proxies the RADIUS Accounting Start message to the TWAP for the 3GPP UE.

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

11.1.1.2 IPv6 prefix via SLAAC

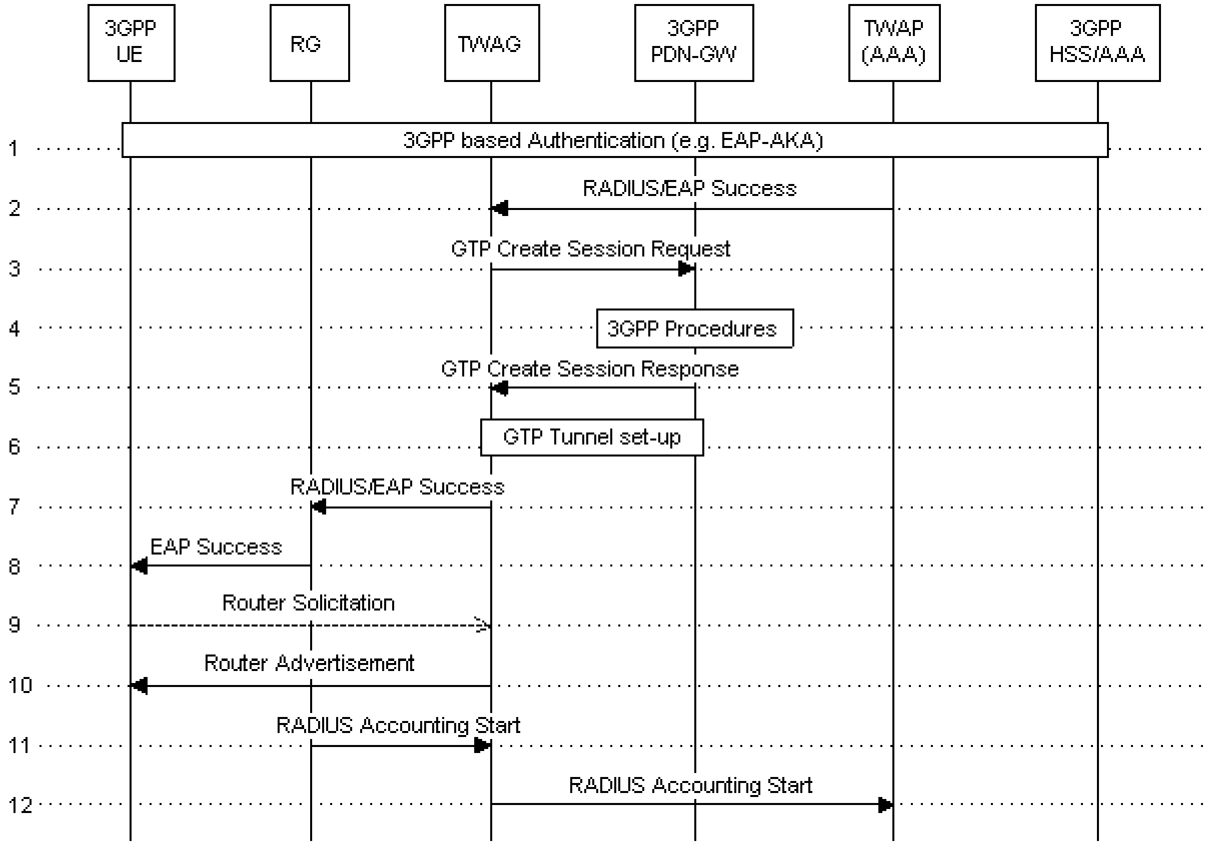

Figure 14 – Initial Attach on GTP S2a – IPv6 prefix via SLAAC

Steps 1 to 8 are the same as Steps 1 to 8 in Section 11.1.1.1. However, step 4 in Figure 14 implies the assignment of an IPv6 prefix by the 3GPP domain.

9. The 3GPP UE sends a Router Solicitation (RS) message to the TWAG.

10. The TWAG responds with a Router Advertisement (RA) with an IPv6 Prefix, retrieved from the 3GPP Domain in Step 4, based on a unicast RA.

Steps 11 and 12 are the same as Step 13 and 14 in Section 11.1.1.1.

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

11.1.2 Initial attach based on layer 3 trigger

11.1.2.1 DHCPv4

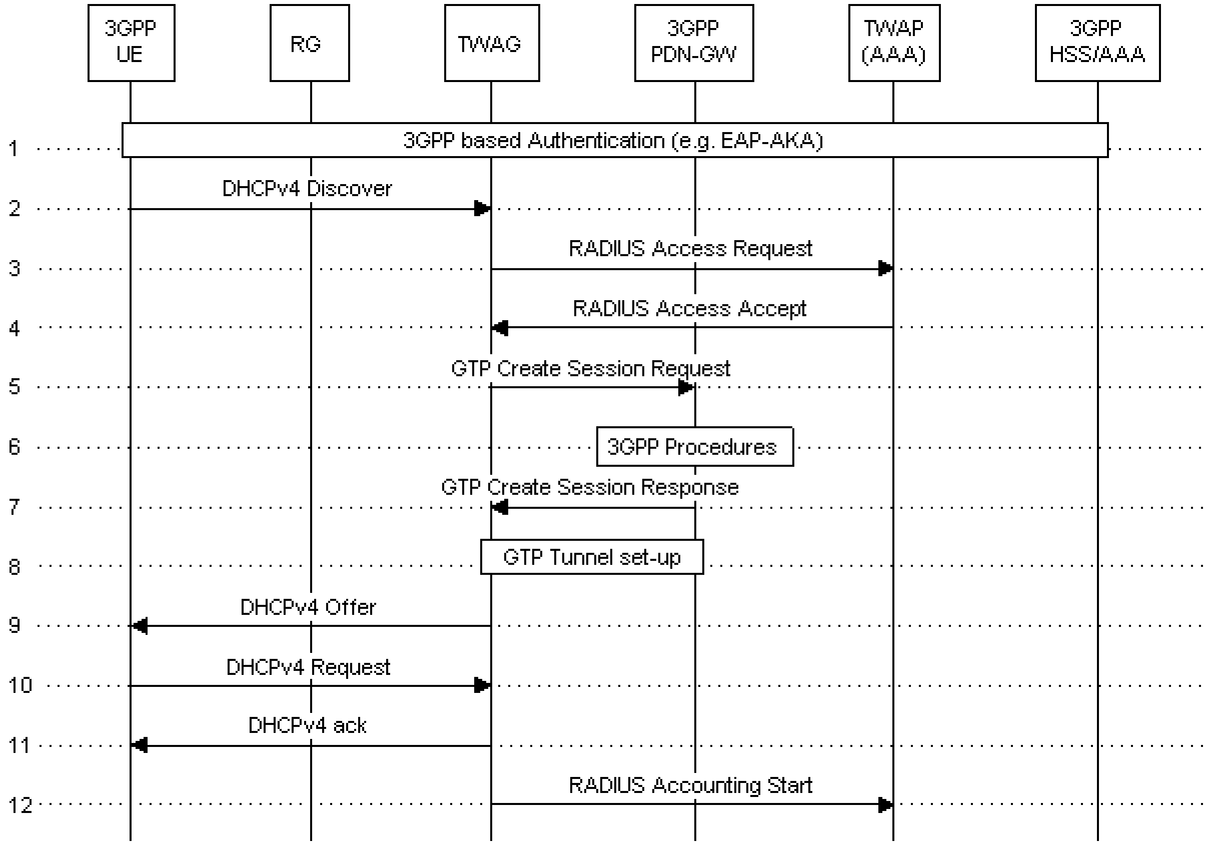

Figure 15 – Initial Attach on GTP S2a – Layer 3 trigger

1. 3GPP UE authentication is performed. 3GPP UE authentication is based on EAP authentication methods, and described in 3GPP TS 23.402 [14]. During the authentication phase, the RG acts as an 802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS Request message.

2. The 3GPP UE sends a DHCP Discover message including the MAC Address. The RG Relays the DHCP Discover message to the TWAG.

3. The TWAG sends a RADIUS Access Request to the TWAP, including the MAC Address. The TWAP makes use of the MAC Address, which is stored during the authentication phase of the 3GPP UE, for correlating the information obtained from the 3GPP Domain during the authentication phase (Step 1) with the IP session.

4. The TWAP responds with a RADIUS Access Accept to the TWAG, including an indication of the need to establish an S2a connection between the TWAG and the 3GPP PDN GW. The

TWAP also provides information retrieved from the 3GPP Domain at Step 1, such as the APN, the selected PLMN Id and the 3GPP IMSI.

Note: Steps 3 and 4 may be avoided if the TWAG is a RADIUS proxy during the 3GPP UE authentication performed during Step 1.

5. The TWAG decides to start an S2a GTP tunnel set-up procedure. For such purpose, the TWAG sends a GTP Create Session Request (as defined in 3GPP TS 23.402 [14]) to the 3GPP PDN GW, including the 3GPP IMSI. The TWAG finds the applicable 3GPP PDN GW based on the APN provided in Step 4.

6. 3GPP domain starts the IP-CAN Session Establishment procedure as defined by 3GPP TS 23.203 [12]. As a result of this procedure, an IPv4 address is allocated to the UE.

7. The PDN GW sends a GTP Create Session Response, including the IPv4 address allocated for the UE. How 3GPP PDN GW acquires such an IP address is out of BBF scope.

8. The S2a-GTP tunnel is set up between the TWAG and the PDN GW.

9. The TWAG sends a DHCP Offer containing the IPv4 Address allocated by the 3GPP domain to the end device that is relayed by the RG.

10. The end device responds by sending a DHCP Request message upstream to the TWAG.

11. The TWAG responds with a DHCP Ask and the IP Session is established.

12. The TWAG sends a RADIUS Accounting Start message to the TWAP for the 3GPP UE.

Note: The procedure for accounting message exchange used for charging purposes is not included in this flow.

11.1.3 Session termination based on a Layer 2 trigger

11.1.3.1 TWAG not supporting a RADIUS proxy

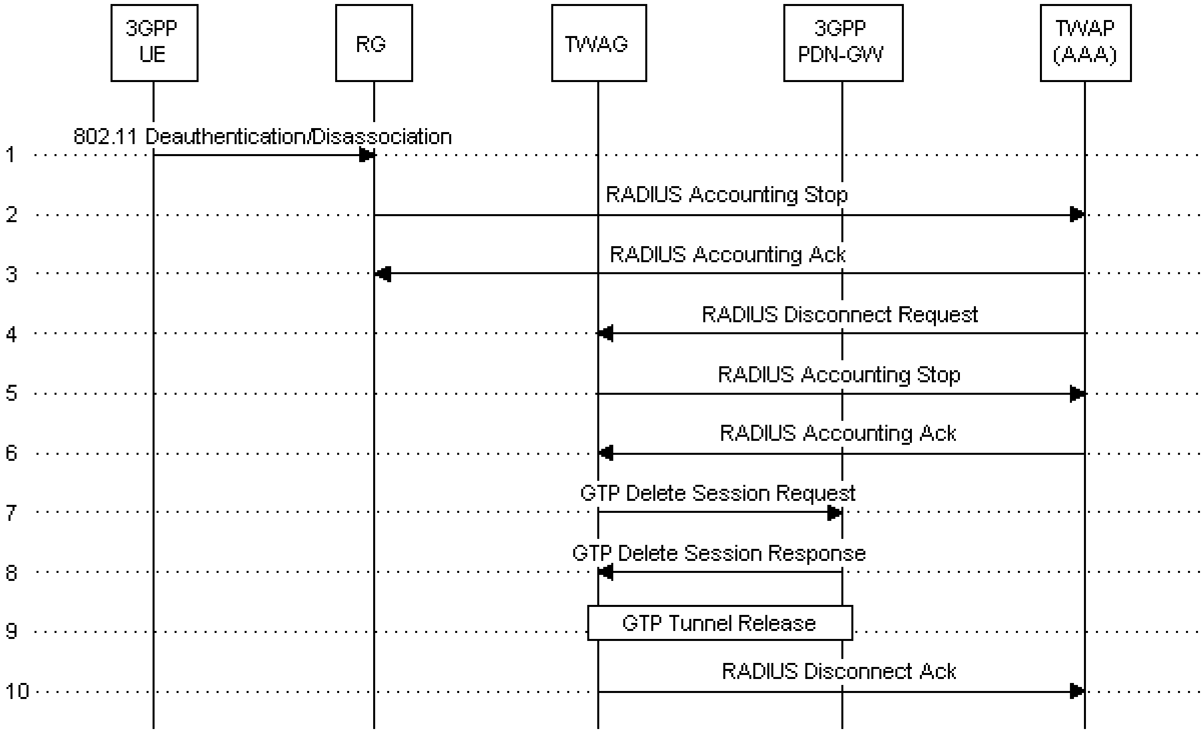

Figure 16 – Layer 2 S2a tunnel release - TWAG not supporting a RADIUS proxy

1. The RG decides to stop the L2 session. This decision could be based on 802.11 disassociation (out of BBF scope), or some internal RG event.

2. The RG sends a RADIUS Accounting-Stop to the TWAP.

3. The TWAP acknowledges the RADIUS Accounting-Stop.

4. Upon receiving the RADIUS Accounting-Stop from the RG, the TWAP sends a Disconnect Request to the TWAG.

5. The TWAG sends a RADIUS Accounting-Stop to the TWAP.

6. The TWAP acknowledges the RADIUS Accounting-Stop.

7. The TWAG requests termination of the S2a GTP tunnel. It sends a GTP Delete Session Request (as defined in 3GPP TS 23.402 [14]) to the 3GPP PDN GW.

8. The PDN GW sends a GTP Delete Session Response.

9. The S2a GTP tunnel is released.

10. The TWAG acknowledges the Disconnect Request to the TWAP.

11.1.3.2 TWAG supporting a RADIUS proxy

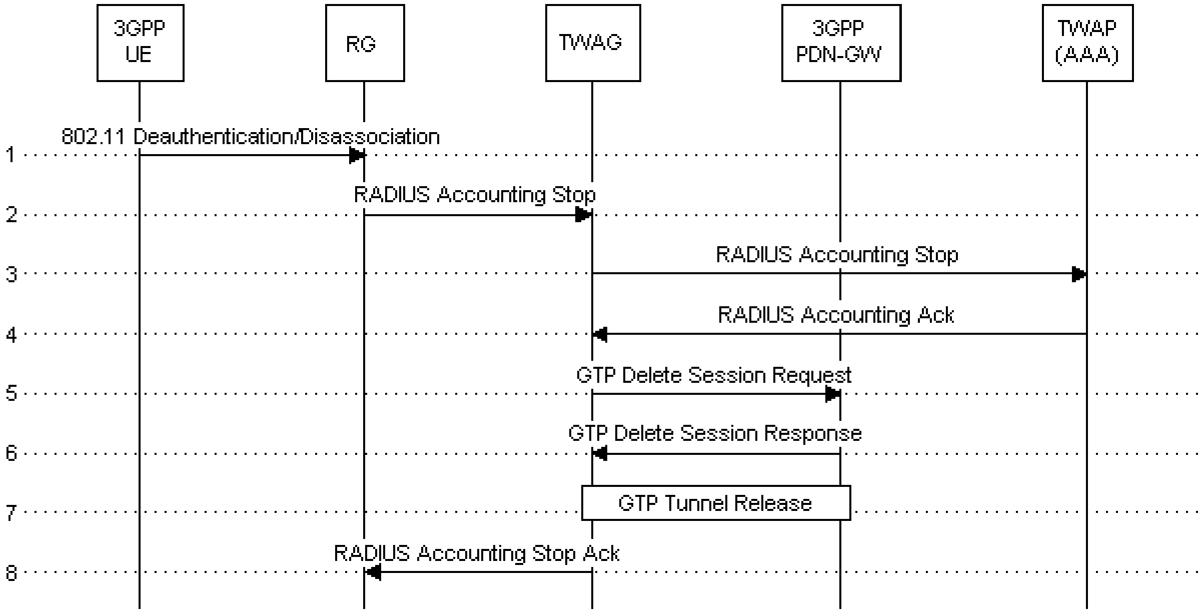

Figure 17 – Layer 2 S2a tunnel release - TWAG supporting a RADIUS proxy

1. The RG decides to stop the L2 session. That decision could be based on 802.11 disassociation or some internal RG event.

2. The RG sends a RADIUS Accounting-Stop to the TWAG (RADIUS Proxy).

3. The TWAG sends a RADIUS Accounting-Stop to the TWAP.

4. The TWAP acknowledges the RADIUS Accounting-Stop to the TWAG.

5. The TWAG requests the termination of the S2a GTP tunnel. It sends a GTP Delete Session Request (as defined in TS 23.402 [14]) to the 3GPP PDN GW.

6. The PDN GW sends a GTP Delete Session Response.

7. The S2a GTP tunnel is released.

8. The TWAG acknowledges the RADIUS Accounting-Stop to the RG.

11.1.4 Session termination based on a Layer 3 trigger

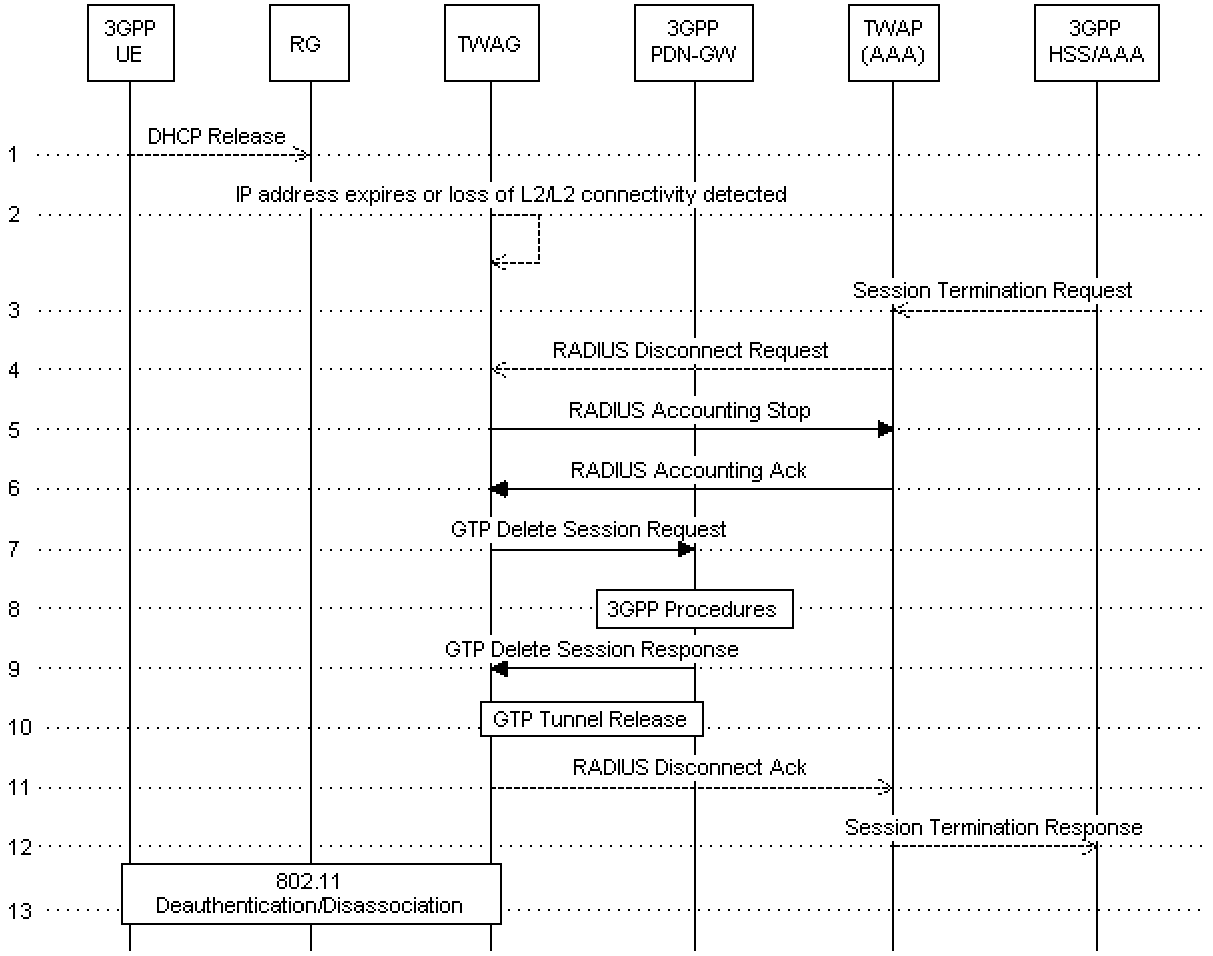
3GPP UE
RG
TWAG
3GPP PDN-GW
TWAP (AAA)
3GPP HSS/AAA
1
DHCP Release
2
IP address expires or loss of L2/L2 connectivity detected
3
Session Termination Request
4
RADIUS Disconnect Request
5
RADIUS Accounting Stop
6
RADIUS Accounting Ack
7
GTP Delete Session Request
8
3GPP Procedures
9
GTP Delete Session Response
10
GTP Tunnel Release
11
RADIUS Disconnect Ack
12
Session Termination Response
13
802.11 Deauthentication/Disassociation

Figure 18 – Layer 3 S2a tunnel release

1. The 3GPP UE may send a DHCP Release in order to indicate IP session termination authentication is performed. The response to the DHCP Release is not shown in the picture.

2. Alternatively, the TWAG may detect loss of L2 or L3 connectivity, or DHCP lease time-out, or a session keep-alive protocol failure event happens (see TR-146 [5]).

3. Alternatively, the 3GPP HSS/AAA may request a session termination request to detach a specific 3GPP UE.

4. Based on the received session termination request from the 3GPP HSS/AAA, the TWAP sends a Disconnect request to the TWAG.

5. The TWAG sends a RADIUS Accounting Stop to the TWAP.

6. The TWAP acknowledges the RADIUS Accounting Stop.

7. The TWAG requests the termination of the S2a GTP tunnel. For such purpose, the TWAG sends a GTP Delete Session Request (as defined in TS 23.402 [14]) to the 3GPP PDN GW.

8. The 3GPP domain starts the PCEF-initiated IP-CAN Session Termination procedure as defined by 3GPP TS 23.203 [12]. This part is out of BBF scope.

9. The PDN GW sends a GTP Delete Session Response.

10. The S2a-GTP tunnel is released.

11. In the case where the procedure was initiated based on a Disconnect request (Steps 3-4), the TWAG acknowledges it to the TWAP.

12. The TWAP reports the Session termination to the 3GPP HSS/AAA.

13. The TWAG locally removes the UE context and de-authenticates and disassociates the UE at Layer 2 according to IEEE 802.11 [23].

Note: For dual stack, Steps 5-10 are triggered by IPv4 address released or Session Termination Request from the 3GPP domain (Steps 3 and 4).

11.2 Procedures for S2b based mobility and BBF routed traffic

11.2.1Initial attach

Note: This scenario is depicted for a non-NAT scenario. Although the procedure is described for DHCPv4, a similar procedure will apply to DHCPv6.

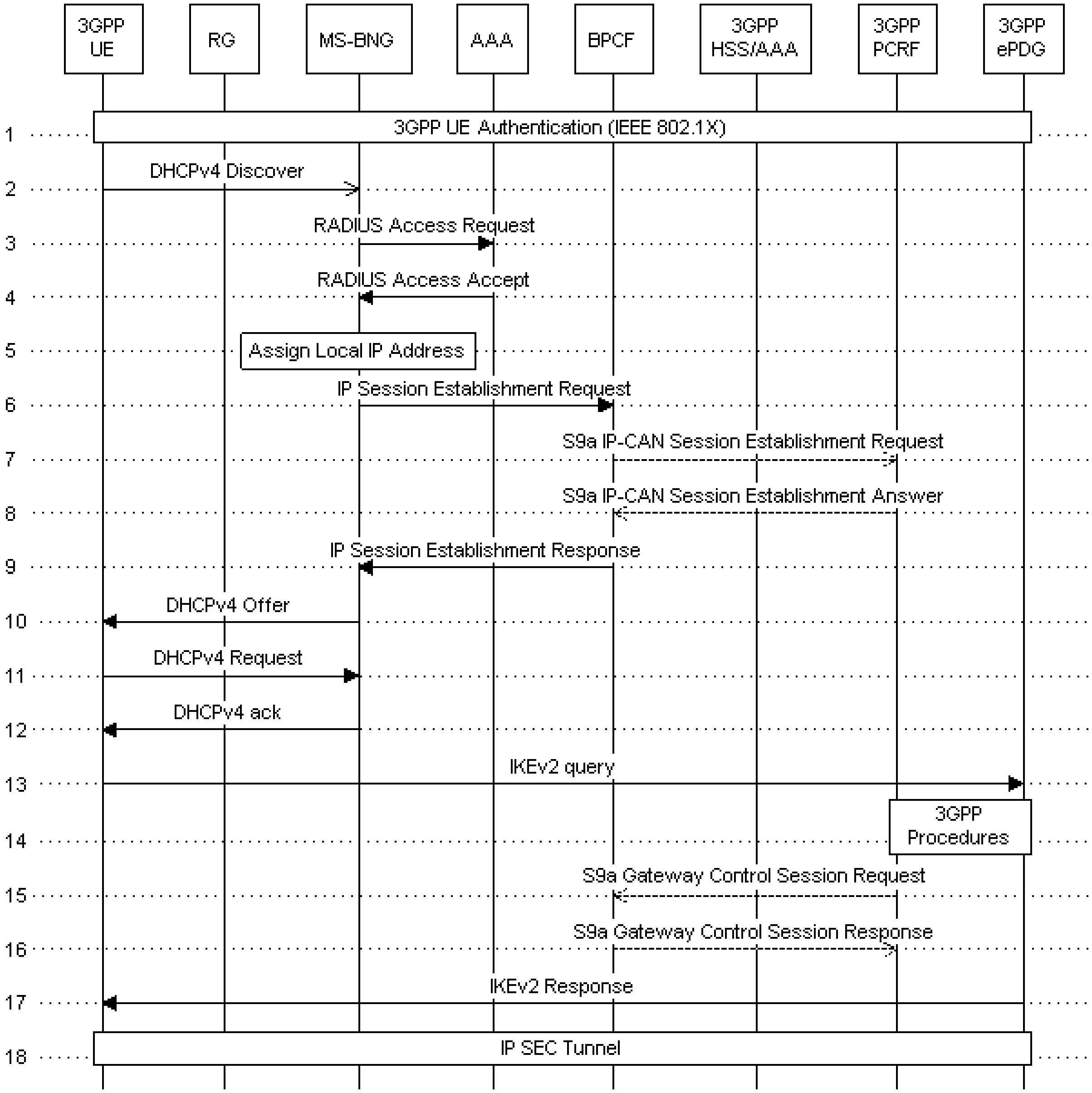
3GPP UE
RG
MS-BNG
AAA
BPCF
3GPP HSS/AAA
3GPP PCRF
3GPP ePDG
1
3GPP UE Authentication (IEEE 802.1X)
2
DHCPv4 Discover
3
RADIUS Access Request
4
RADIUS Access Accept
5
Assign Local IP Address
6
IP Session Establishment Request
7
S9a IP-CAN Session Establishment Request
8
S9a IP-CAN Session Establishment Answer
9
IP Session Establishment Response
10
DHCPv4 Offer
11
DHCPv4 Request
12
DHCPv4 ack
13
IKEv2 query
14
3GPP Procedures
15
S9a Gateway Control Session Request
16
S9a Gateway Control Session Response
17
IKEv2 Response
18
IP SEC Tunnel

Figure 19 – S2b Tunnel establishment

1. For BBF routed traffic, the 3GPP UE authentication step must be performed. Otherwise, for 3GPP Routed traffic, the 3GPP UE authentication step is optional.

   3GPP UE authentication is based on EAP authentication methods, and described in 3GPP TS 23.402 [14]. During the authentication phase, the RG acts as an 802.1X authenticator, and adds the MAC Address of the 3GPP UE to the RADIUS Request message.

2. The 3GPP UE sends a DHCP Discover message including the MAC Address. The RG proxies the DHCP Discover message to the MS-BNG.

3. The MS-BNG sends a RADIUS Access Request to the Fixed Access AAA Server, including the MAC Address. The Fixed Access AAA Server makes use of the MAC Address, which is stored during the authentication phase of the 3GPP UE, for correlating the information obtained from the 3GPP Domain during the authentication phase (Step 1) with the IP session (if applicable).

4. The Fixed Access AAA Server responds with a RADIUS Access Accept to the MS-BNG, including an indication of the need to establish an S2b connection between the ePDG and the 3GPP PDN GW. The Fixed Access AAA Server also provides information retrieved from the 3GPP Domain at Step 1, like the NSWO-APN, the selected PLMN Id and the 3GPP IMSI (if applicable).

5. The UE is assigned a local IP address from the BBF network.

6. The MS-BNG sends an IP Session Establishment request for the BPCF, including the UE's locally assigned IP Address in Step 5.

7. For BBF routed traffic, if local policies indicate that policy control for BBF routed traffic is provided for subscribers from that PLMN, the BPCF relays this information to the 3GPP PCRF in an IP-CAN Session Establishment by the S9a reference point. In the request, the BPCF includes the IMSI, UE local IP address and NSWO-APN indication (if obtained in Step 1).

8. The PCRF acknowledges the S9a session establishment and provisions the PCC Rules to the BPCF if policy control is enabled.

9. The BPCF acknowledges the session establishment request. If Steps 7 and 8 were performed, policy control is enabled and PCC Rules were received from the PCRF, the BPCF will map the PCC Rules to QoS Rules and forward these to the MS-BNG as part of the response.

10. The MS-BNG sends a DHCP Offer containing the BBF domain locally assigned IP Address (in Step 5) to the end device that is relayed by the RG.

11. The end device responds by sending a DHCP Request message upstream to the MS-BNG.

12. The MS-BNG responds with a DHCP Ask and the IP Session is established.

13. The UE terminal starts the Internet Key Exchange version 2 (IKEv2) tunnel establishment. The ePDG IP address to which the UE needs to form the IPsec tunnel is discovered via a DNS query performed by the UE, as specified in the 3GPP TS 23.402 [14].

14. 3GPP procedures take place between the ePDG, the PDN GW and the PCRF to establish the 3GPP IP-CAN Session and the GTP/PMIP tunnel between ePDG and PDN GW. These procedures are outside the scope of BBF.

15. For 3GPP Routed traffic, the PCRF starts the S9a session establishment procedure by sending a Gateway Control Session Request message towards the BPCF for admission control as specified in the 3GPP TS 23.139 [11].

16. The BPCF binds the S9a Gateway Control session with the corresponding IP session over the R-interface created at Step 6. The BPCF maps the 3GPP QoS rules received from the PCRF into BBF QoS parameters. An example of a mapping table is given in Appendix III/TR-203 [7]. The BPCF acknowledges the request sending the Gateway Control Session Response message back to the PCRF.

17. The ePDG sends an IKEv2 response with the 3GPP allocated IP address in the IKEv2 configuration payloads.

18. The IP connectivity from the UE to the PDN GW is now setup.

Any packet in the uplink direction is tunneled to the ePDG by the UE using the IPsec tunnel. The ePDG will tunnel any BBF-domain received packet to the 3GPP domain via the established GTP/PMIPS tunnel. In the downlink direction, the ePDG will tunnel any received packet to the UE via the proper IPsec tunnel.

11.2.23GPP initiated detach

Note: This scenario is depicted for a bridged RG.

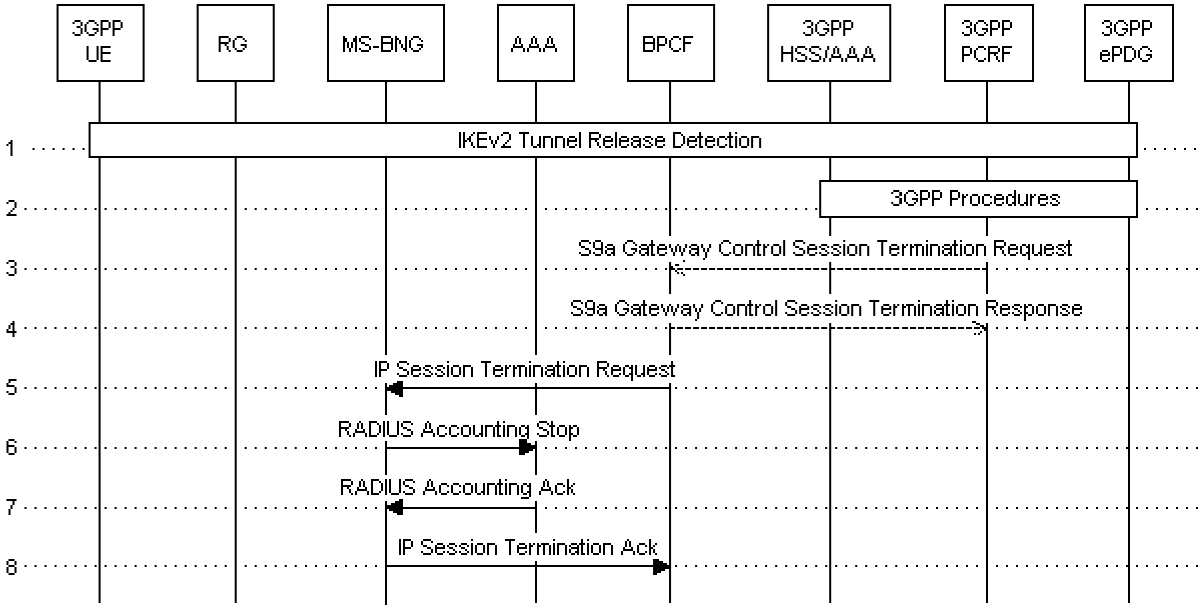
3GPP UE
RG
MS-BNG
AAA
BPCF
3GPP HSS/AAA
3GPP PCRF
3GPP ePDG
1
IKEv2 Tunnel Release Detection
2
3GPP Procedures
3
S9a Gateway Control Session Termination Request
4
S9a Gateway Control Session Termination Response
5
IP Session Termination Request
6
RADIUS Accounting Stop
7
RADIUS Accounting Ack
8
IP Session Termination Ack

Figure 20 – S2b tunnel release – 3GPP Initiated

1. IKEv2 tunnel release detection. This procedure can be initiated by the UE (e.g. when the UE is powered off) or by the ePDG due to an administration reason.

2. The IKEv2 tunnel release triggers 3GPP procedures for S2b Tunnel release. These procedures are out of BBF scope.

3. The PCRF executes a Gateway Control Session Termination procedure with the BPCF.

4. The BPCF acknowledges this with the Gateway Control Session Termination Response.

5. The previous step triggers the BPCF to send an IP Session Termination Request to the MS-BNG.

6. The MS-BNG sends a RADIUS Accounting Stop to the Fixed Access AAA Server.

7. The Fixed Access AAA Server acknowledges with a RADIUS Accounting Stop.

8. The MS-BNG acknowledges the IP Session Termination.

11.2.3 UE / BBF Initiated detach

Note: This scenario is depicted for a bridged RG.

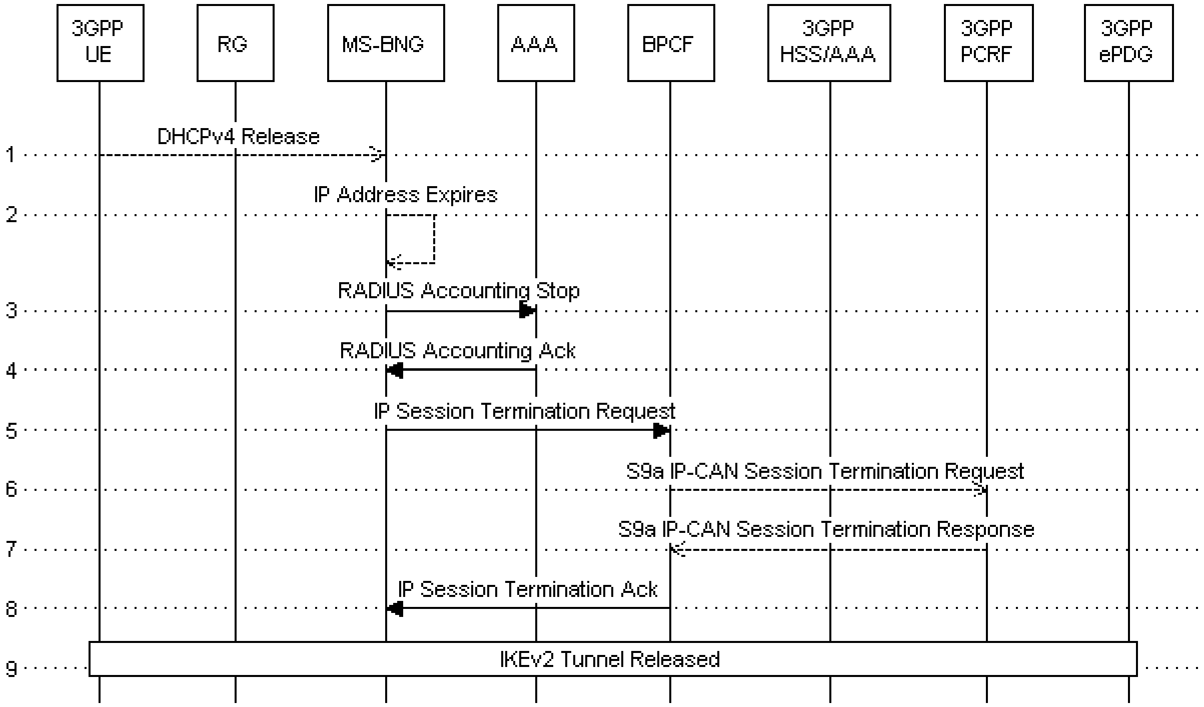

Figure 21 – S2b tunnel release – UE/MS-BNG Initiated

1. The 3GPP UE may send a DHCP Release in order to indicate IP session termination authentication is performed. The response to the DHCP Release is not shown in Figure 21.

2. Alternatively, the MS-BNG may detect loss of L2 or L3 connectivity, o DHCP lease time-out or a session keep-alive protocol failure event happens (according to TR-146 [5]).

3. The MS-BNG sends a RADIUS Accounting Stop to the Fixed Access AAA Server.

4. The Fixed Access AAA Server acknowledges this with a RADIUS Accounting Stop.

5. Step 1 or 2 triggers the MS-BNG to send an IP Session Termination Request to the BPCF.

6. The BPCF sends an indication of IP-CAN session termination to the PCRF.

7. The PCRF acknowledges receipt of the IP-CAN session termination request.

8. The BPCF acknowledges the IP Session Termination.

9. The IKEv2 tunnel is released. This step may occur in parallel with Steps 2-8.

11.3 Procedures for H(e)NB/Femto access

11.3.1PCRF triggered S9a Session Establishment

The S9a Session is triggered by the PCRF when the first mobile attaches to the network via the H(e)NB or the handover from the macro network to the H(e)NB occurs.

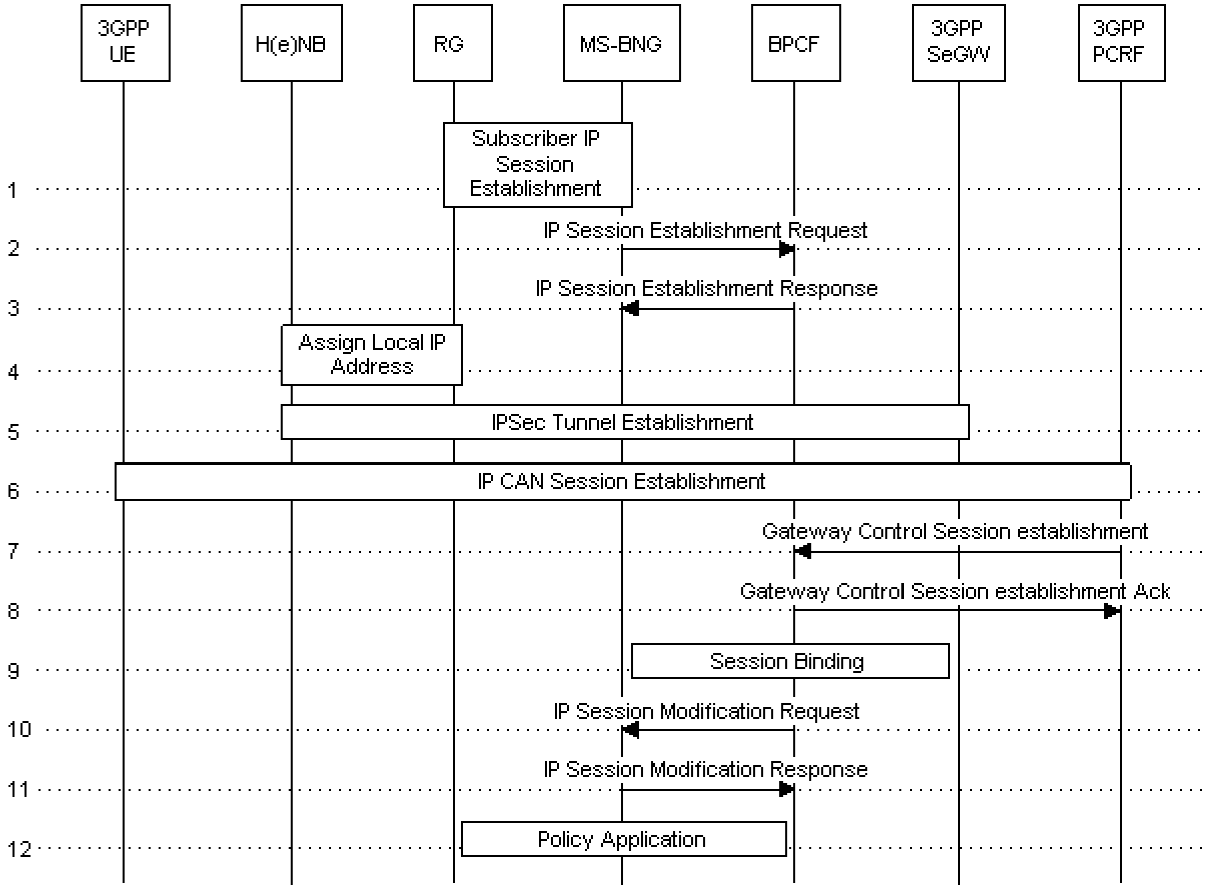
3GPP UE
H(e)NB
RG
MS-BNG
BPCF
3GPP SeGW
3GPP PCRF
1
Subscriber IP Session Establishment
2
IP Session Establishment Request
3
IP Session Establishment Response
4
Assign Local IP Address
5
IPSec Tunnel Establishment
6
IP CAN Session Establishment
7
Gateway Control Session establishment
8
Gateway Control Session establishment Ack
9
Session Binding
10
IP Session Modification Request
11
IP Session Modification Response
12
Policy Application

Figure 22 – H(e)NB Session Establishment

1. The RG establishes an IP session with the MS-BNG as per TR-146 [5].

2. The MS-BNG sends the IP session establishment request to the BPCF.

3. The BPCF acknowledges the IP session establishment.

4. The RG allocates a private IP address to the H(E)NB as per TR-124i3 [2].

5. IPsec tunnel set-up between the H(e)NB and the SeGW as per 3GPP TS 33.320 [21].

6. An event (defined by 3GPP) takes place that induces the PCRF to trigger the set-up of the S9a session. This may be, for example, an UE attaching to the network that is further described in 3GPP TS 23.139 [11] and Annex P/TS 23.203 [12].

7. The PCRF sends the Gateway Control Session establishment trigger message to the BPCF according to 3GPP TS 23.203 [12]. The message includes the IMSI, HeNB local IP address and UDP port if NA(P)T is detected.

8. The BPCF decides whether or not to accept the S9a session. It sends the Gateway Control Session establishment message to the PCRF according to 3GPP TS 23.203 [12]. The

message includes the IMSI, H(e)NB local IP address and UDP port if NAT/NA(P)T is detected. The PCRF acknowledges the S9a Gateway Control session establishment.

9. The BPCF binds the S9a session with the IP-session based on the H(e)NB local IP address it has received from the PCRF.

10. The BPCF initiates the IP session modification procedure.

Note: There are no QoS rules associated with this procedure. Nevertheless the PCRF may then update the S9a session with the relevant QoS rules per the PCRF initiated S9a Session Modification (see Section 11.3.3).

11. The MS-BNG acknowledges the IP session modification.

12. The MS-BNG applies the BPCF policies.

11.3.2 PCRF initiated S9a Session Termination

The PCRF initiates the S9a session termination when for the last UE connected to the H(e)NB the Gx session terminates or this UE moves out of the H(e)NB coverage.

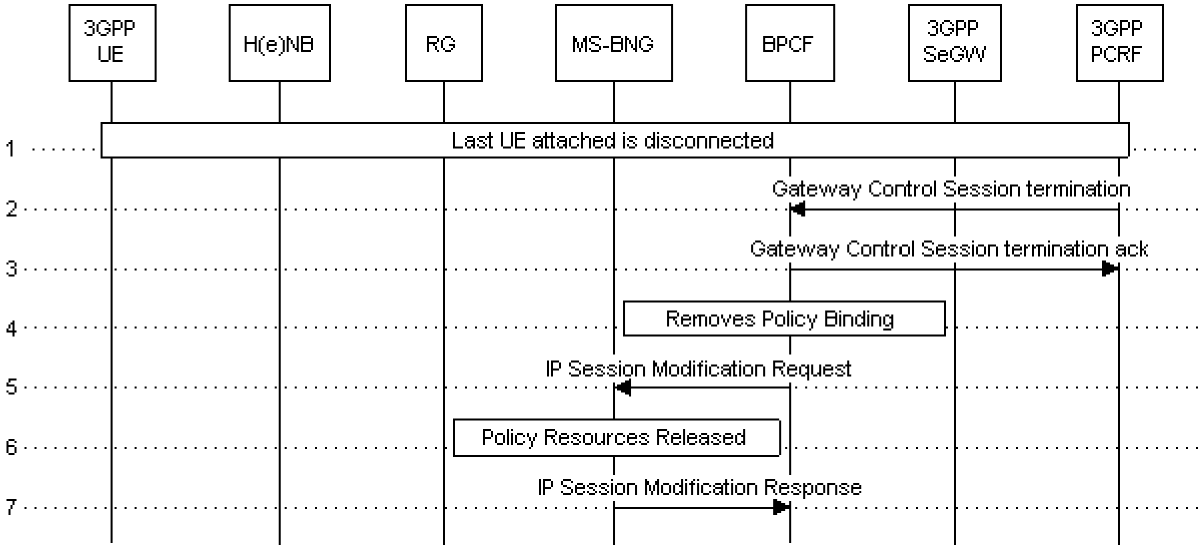
3GPP UE
H(e)NB
RG
MS-BNG
BPCF
3GPP SeGW
3GPP PCRF
1
Last UE attached is disconnected
2
Gateway Control Session termination
3
Gateway Control Session termination ack
4
Removes Policy Binding
5
IP Session Modification Request
6
Policy Resources Released
7
IP Session Modification Response

Figure 23 – H(e)NB PCRF initiated S9a Session Termination

1. The last UE connected to the H(e)NB terminates its IP session or this UE moves out of the H(e)NB coverage. This step is out of BBF scope

2. The PCRF determines that that there are no other UEs connected to the network via the H(e)NB and initiates the termination of S9a Gateway Control session per 3GPP TS 23.139 [11] and 3GPP TS 23.203 [12].

3. The BPCF acknowledges the termination of the S9a Gateway control Session.

4. The BPCF determines the QoS rules associated with the S9a session.

5. The BPCF initiates the IP session modification procedure that includes the QoS rules to be removed.

6. The MS-BNG removes the QoS rules identified by the BPCF.

7. The MS-BNG acknowledges the removal of the QoS rules to the BPCF.

11.3.3PCRF initiated S9a Session Modification

This procedure is initiated for example by the PCRF when a UE requests additional services that require allocation of QoS resources in the BBF network. This procedure is also initiated in order to free up QoS resources in the BBF network when a UE disconnects or moves out of coverage of the H(e)NB.

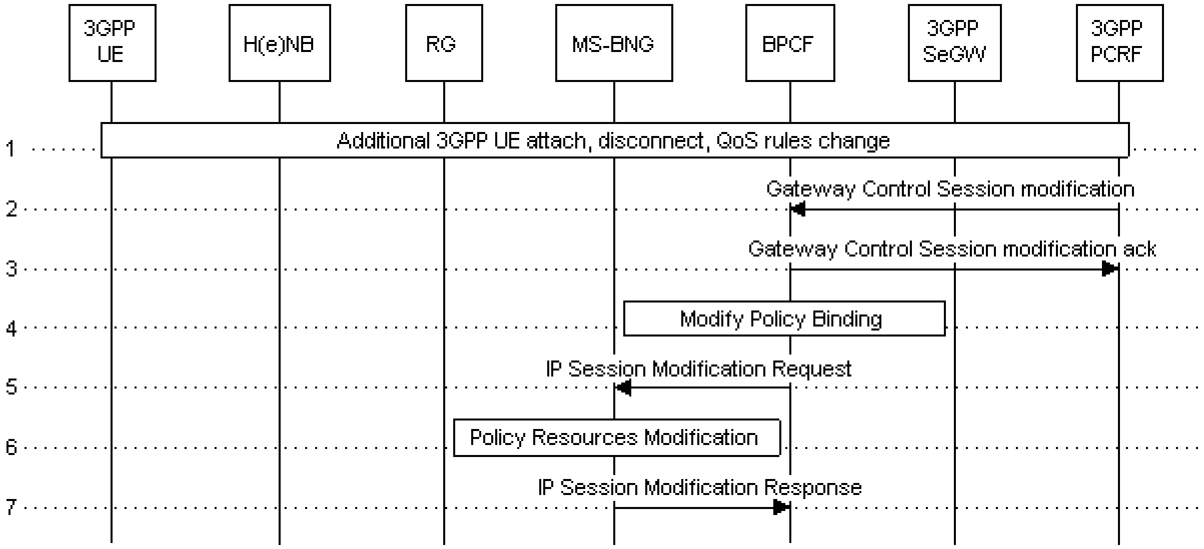
3GPP UE
H(e)NB
RG
MS-BNG
BPCF
3GPP SeGW
3GPP PCRF
1
Additional 3GPP UE attach, disconnect, QoS rules change
2
Gateway Control Session modification
3
Gateway Control Session modification ack
4
Modify Policy Binding
5
IP Session Modification Request
6
Policy Resources Modification
7
IP Session Modification Response

Figure 24 – H(e)NB PCRF initiated S9a Session Modification

1. The PCRF determines that the QoS requirements for an H(e)NB need a change in the policies enforced by the BBF access that connects this H(e)NB and thus decides that the S9a Session Modification has to be initiated. Examples of 3GPP procedures that may trigger this are:

    - An UE served by the H(e)NB initiates or releases a voice call thus requiring a change in the amount of bandwidth needing the high QoS.
    - As part of a Hand-Over procedure, a UE with a voice call enters or leaves the coverage of the H(e)NB.

2. The PCRF initiates the S9a Gateway Control Session Modification as per 3GPP TS 23.139 [11] and 3GPP TS 23.203 [12], and includes the QoS rules/QoS rule name as per 3GPP TS 23.139 [11], 3GPP TS 23.203 [12] and TR-203 [7].

3. The BPCF acknowledges the S9a Gateway Control Session Modification.

4. The BPCF maps the 3GPP QoS rules to BBF QoS parameters.

5. The BPCF provisions the new BBF QoS parameters at the MS-BNG by means of an IP Session Modification request.

6. The MS-BNG may perform admission control and installs the policy rules or removes existing rules as per the request from the BPCF.

7. The MS-BNG acknowledges the IP Session Modification performed.

End of Broadband Forum Technical Report TR-291