3GPP TR 23.852 V2.0.0 (2013-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on S2a Mobility based On GTP and WLAN access to EPC (SaMOG);
Stage 2
(Release 12)

Keywords

EPC, WLAN, GTP, S2a

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

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.

1 Scope

This Study item is to study:

1. The addition of a S2a based on GTP option. In particular this SID will develop the necessary stage 2 message flows to support S2a based on GTP and mobility between GTP-S5/S8 and GTP-S2a.
2. Supporting WLAN access to EPC through S2a via mechanisms:

   2.1 with no impact to the UE;

   2.2 with impact to the UE.

Solutions requiring modifications to non 3GPP link-layers will not be considered. It is expected that the result of this Study Item may be used by 3GPP-BBF interworking activities (BBAI).

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 41.101: ""Technical Specifications and Technical Reports for a GERAN-based 3GPP system".

[3] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

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

[5] IEEE Std 802.11-2007: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[6] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[7] 3GPP TS 29.273: "Evolved Packet System (EPS); 3GPP EPS AAA interfaces".

[8] IETF RFC 791: "Internet Protocol".

[9] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[10] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[11] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[12] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[13] IETF RFC 4436: "Detecting Network Attachment in IPv4 (DNAv4)".

[14] IETF RFC 6059: "Simple Procedures for Detecting Network Attachment in IPv6".

[15] IEEE Std 802.11n-2009: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Enhancements for Higher Throughput (Amendment 5)".

[16] IETF RFC 6085: " Address Mapping of IPv6 Multicast Packets on Ethernet".

[17] IETF RFC 5213: "Proxy Mobile IPv6".

[18] IETF RFC 5844: "IPv4 Support for Proxy Mobile IPv6".

[19] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[20] IEEE Std 802.1Q-2011: "IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks".

[21] IEEE Std 802.11u-2011: " IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Amendment 9: Interworking with External Networks".

[22] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[23] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[24] IETF RFC 3203: "DHCP reconfigure extension".

[25] IETF RFC 6085: "Address Mapping of IPv6 Multicast Packets on Ethernet".

[26] IEEE Std 802-2001: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".

[27] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[28] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[29] IETF RFC 6704: "Forcerenew Nonce Authentication".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] apply.

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].

ANQP	Access Network Query Protocol
CAPWAP	Control And Provisioning of Wireless Access Points
DHCPv4	Dynamic Host Configuration Protocol for IPv4
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DLNA	Digital Living Network Alliance
DNAv4	Detecting Network Attachment in IPv4
DNAv6	Detecting Network Attachment in IPv6
Femto	Femto is short for femtocell and is synonymous of HNB or HeNB in 3GPP.
FCS	Frame Checksum

GAS	Generic Advertisement Service
IAID	Identity Association Identifier
IPCP	Internet Protocol Control Protocol
IPv6CP	IPv6 Control Protocol
LCP	Link Control Protocol
LLC	Logical Link Control
LL-DAD	Logical Link Duplicate Address Detection
NSWO	Non-seamless WLAN Offload
OUI	Organization Unique Identifier
PPPoE	Point to Point Protocol Over Ethernet
SAP	Service Access Port
SLAAC	Stateless Address Auto-configuration
SNAP	Subnetwork Access Protocol
TNAP	Trusted non-3GPP Access Peers
TNSP	Trusted non-3GPP Signalling Peers
TWAG	Trusted WLAN Access Gateway
TWAP	Trusted Wireless Access Proxy
TWAN	Trusted WLAN AN
VMAC	Virtual MAC
WCS	WLAN Control Signalling
WLCP	WLAN Control Protocol

4 Scenarios

The decision on whether a non 3GPP access is considered trusted or un trusted is made by the HPLMN operator and is not a characteristic of the non 3GPP access network. More details on it are provided in clause 4.3.1.2 of TS 23.402 [3]. The HPMN operator however while making a decision on trust worthiness of a non 3GPP access can also take into consideration security aspects of the access network.

WLAN security was considered poor in both strength and ease of use, compared with that taken for granted in 3G networks and devices (UICC plus HSS, and GPRS encryption of data). Hence it made sense for the Mobile Network Operators (MNOs) to use their core network to add overlay security layers, i.e. the IKEv2 for Authentication and Authorization of the UE, and the IPSec between the UE and ePDG for the security of the user data.

Now, with the deployment of 802.1x, 802.11u, 802.11i and Hotspot 2.0, it may be considered by some operators that the security strength and ease of use (discovery and set up) is as acceptable as 3G/LTE security. For example, for the radio air link, the operator controlled hotspot with 802.11i could be treated as a secure Non-3GPP Access. As 802.11i (or WPA2 called by WFA) has been released for several years, many AP-s support it as a basic feature and lots of smart phones also have supported it.

WLAN can also be deployed integrated in a residential/enterprise device (e.g. femto). In such a scenario, protection mechanism for the traffic on the backhaul link between the residential/enterprise device and the EPC may be used. This protection of the backhaul may be leveraged to consider the WLAN security in terms of connectivity to the EPC.

The impact on the support of the following scenarios shall be used to evaluate the solutions that will be proposed in the study:

- Access to EPC resources/services with access control by the operator;
- Seamless mobility between 3GPP and WLAN for EPS services with IP address preservation;
- Non-seamless mobility services between 3GPP and WLAN for EPS services: no IP address preservation;
- Support of UEs with single PDN connection; support of UEs with multiple PDN connections;
- Access to EPC via WLAN simultaneously with non-seamless WLAN offload.

5 Architectural assumptions

Editor's note: This clause will identify the architectural assumptions.

5.1 Architectural assumptions for GTP based S2a

From a UE perspective, using S2a-GTP or S2a-PMIP shall be transparent.

The impacts to the existing functionalities and to the EPC shall be minimized. The protocol design on S2a should aim at keeping S2a GTP operations similar to those supported on GTP-based S5/S8 and GTP-based S2b as much as possible.

All functions of the existing PMIP-S2a option should also be supported by GTP-S2a, except for optimized handover.

5.2 Architectural assumptions for WLAN access to EPC through S2a

In order to support the scenarios described in clause 4, the following assumptions for WLAN access to EPC through S2a are taken and need to be investigated as part of the study:

- The UE and the EPC are assumed to mutually authenticate through the WLAN Access as defined in TS 23.402 [3], clause 4.9.1.

- It is assumed that UE traffic over the WLAN air link may be confidentiality and integrity protected as defined by IEEE 802.11 [5].

- It is assumed that there is a point-to-point link between UE and non-3GPP access GTP peer for the solutions with no impact to UE.

The backhaul, through which WLAN accesses to EPC, may be secured, e.g. through IPSec, to build a secure access to the EPC.

5.2.1 Assumptions for solutions with no Impact to the UE

The solutions that enable trusted WLAN access to EPC over S2a without any UE impact shall comply with the following architectural assumptions:

- There shall be no functionality added to a R11 UE with respect to a R10 or pre-R10 UE specifically for the support of trusted WLAN access to EPC over S2a.

- No additional 3GPP mechanisms (other than those already specified), layer 2 protocol modifications or layer 3 protocol modifications shall be required on the UE to allow a UE capable of WLAN connectivity to a trusted WLAN network to gain WLAN access to EPC through S2a.

- There shall be no impact to the UE for the indication of the APN of the PDN to be established upon attach or upon handover of a PDN connection from a 3GPP access to trusted WLAN through S2a. The network shall be capable of selecting the APN to be used for the PDN establishment upon attach, independently of whether one or more PDN connections with such APNs are active over a 3GPP access.

- There shall be no impact to the UE for the support of IP address preservation in case of mobility between a 3GPP access and WLAN.

- There shall be no impact to the UE for the establishment of more than one PDN connections over WLAN when attaching to WLAN access or when handing over PDN connections from a 3GPP access.

- There shall be no impact to the UE for the simultaneous support of IP connectivity to the EPC over WLAN and with non-seamless WLAN offload.

- SaMOG solution should co-exist with Release 11 and earlier UEs which may implement WLAN interworking related features including ANDSF and its extensions, SWu, S2c.

- Since an unmodified UE may support the Detecting Network Attachment (DNA) functions, solutions claiming no impacts to the UE shall work in presence of the following protocols:
  - For IPv4: IETF RFC 4436 [13].
  - For IPv6: IETF RFC 6059 [14].

The above list is non-exhaustive.

Only the following functions can be considered supported by an unmodified UE, i.e. solutions with no impacts to UE shall only expect the following functions in the UE:

- WLAN spec only restricted to PHY/MAC aspects in IEEE 802.11 [5] and IEEE 802.11n [15].
- 3GPP-based authentication as defined in TS 23.402 [3] over WLAN (i.e. access authentication towards EPC).
- IPv4 and/or IPv6 support:
  - For IPv4: IETF RFC791 [8], IETF RFC 2131 [9].
  - For IPv6: IETF RFC 2460 [10], IETF RFC 4861 [11], and IETF RFC 4862 [12].

6 Solutions for GTP based S2a

Editor's note: This clause will describe the solution(s) for the "access agnostic" GTP-S2a, which is basically similar to PMIPv6-S2a in TS 23.402 [3]. For WLAN Access, the additional considerations including the potential UE impacts are studied in clause 7.

6.1 Solution 1

6.1.1 Architecture

The same architecture reference models as those defined in TS 23.402 [3] can be applied to GTP based S2a, with the following differences:

- BBERF is not required with GTP based S2a;
- Gxa interface is not required between the PCRF (or vPCRF) and the Trusted Non-3GPP Access;
- vPCRF (and S9 interface) is not required for roaming with Home Routed traffic (i.e. non-LBO traffic).

NOTE 1: The Chained case is not proposed to be supported in this release.Figures 6.1.1-1 to 6.1.1-3 show the baseline architecture reference model for GTP based S2a in the non roaming and roaming cases.

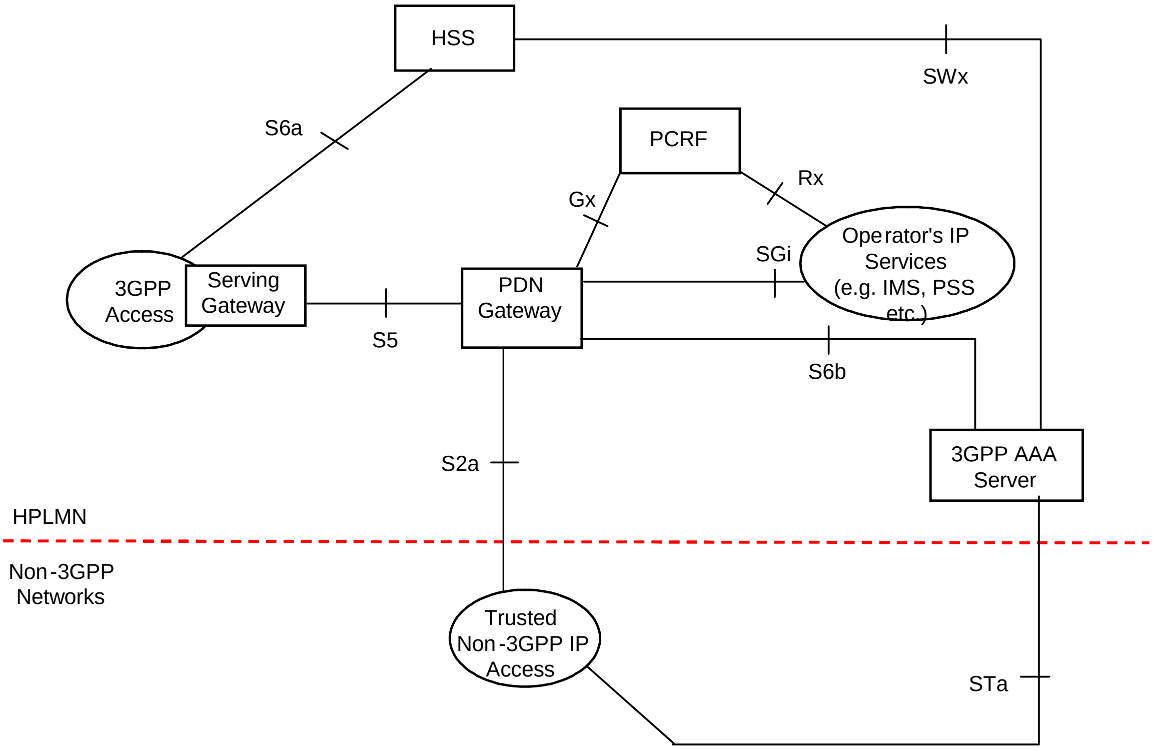


Figure 6.1.1-1: Non-Roaming Architecture within EPS using GTP based S5, S2a

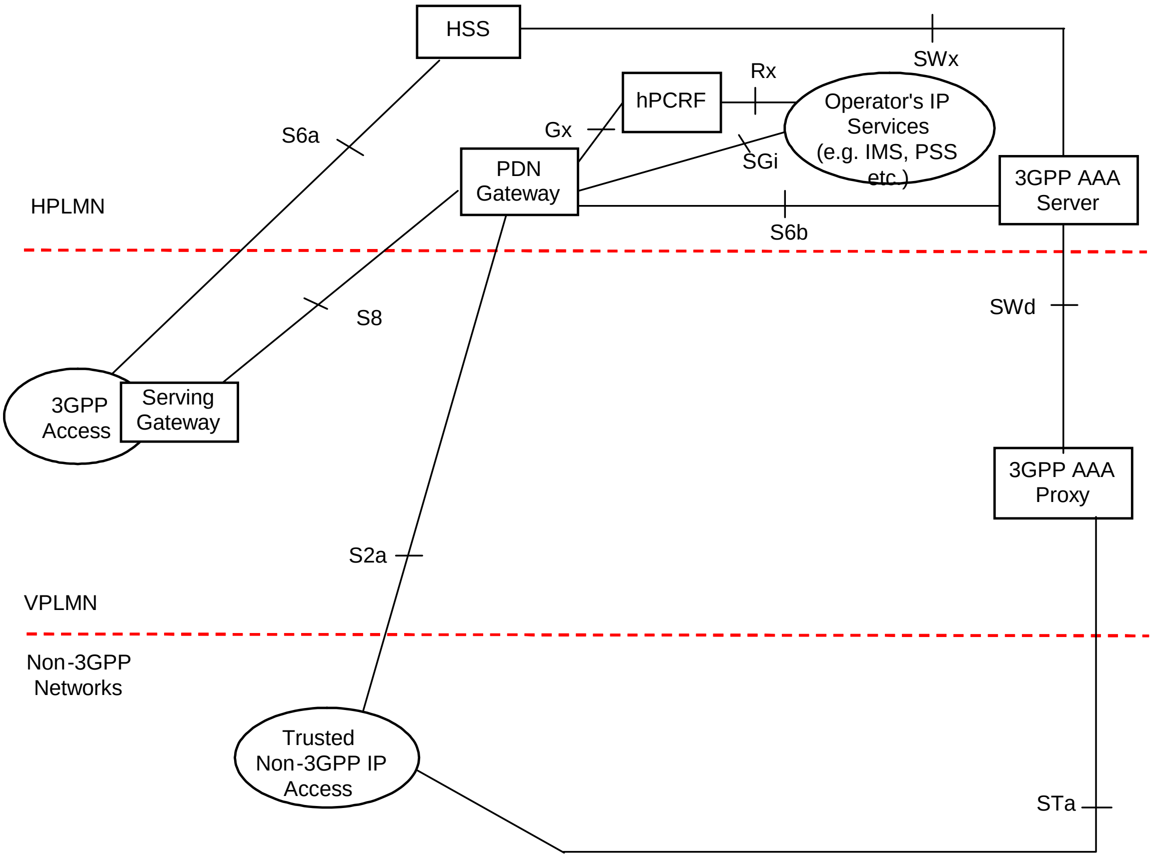


Figure 6.1.1-2: Roaming Architecture for EPS using GTP based S8, S2a - Home Routed

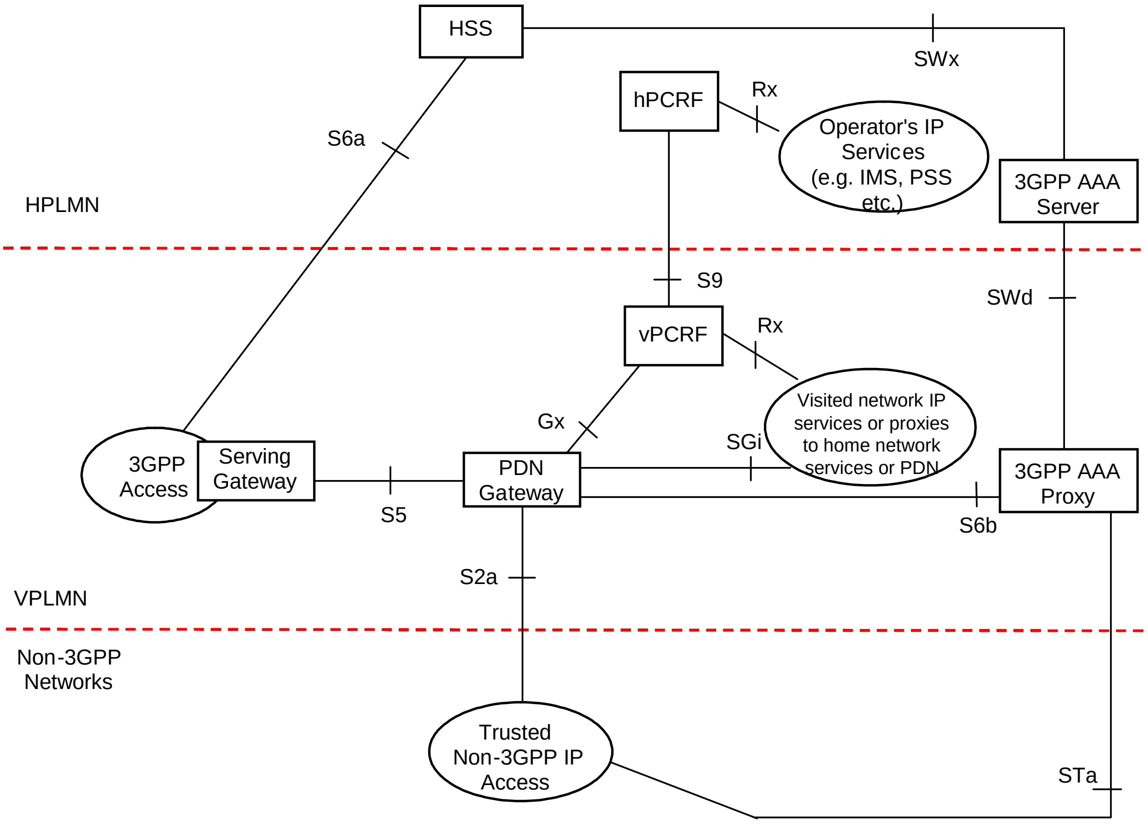

HSS
SWx
hPCRF
Rx
Operator's IP Services (e.g. IMS, PSS etc.)
S6a
3GPP AAA Server
HPLMN
S9
SWd
vPCRF
Rx
Visited network IP services or proxies to home network services or PDN
Gx
SGi
3GPP Access
Serving Gateway
PDN Gateway
3GPP AAA Proxy
S5
S6b
S2a
VPLMN
Non-3GPP Networks
Trusted Non-3GPP IP Access
STa

Figure 6.1.1-3: Roaming Architecture for EPS using GTP based S5, S2a - Local Breakout

NOTE 2: A GTP peer is assumed in the Trusted Non-3GPP IP Access for this GTP based S2a. Moreover it is assumed that the GTP peer acts as first hop router in a similar way as the MAG when PMIP is used over S2a. When deferred IPv4 address allocation is supported, it is assumed that the GTP peer supports DHCPv4 relay functionality.

6.1.2 Functional description

Editor's note: This clause will contain the functional description for S2a mobility based on GTP.

6.1.2.1 Bearer model for a PDN connection

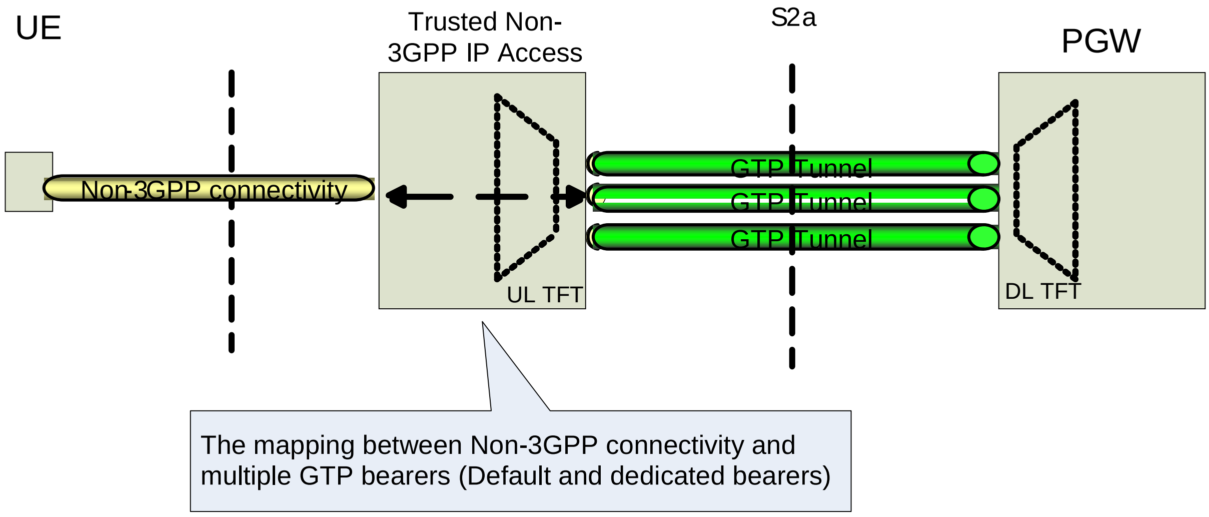

UE
Trusted Non-3GPP IP Access
S2a
PGW
Non-3GPP connectivity
GTP Tunnel
GTP Tunnel
GTP Tunnel
UL TFT
DL TFT
The mapping between Non-3GPP connectivity and multiple GTP bearers (Default and dedicated bearers)

Figure 6.1.2.1-1: Bearer model on GTP based S2a

NOTE: The mapping between Non-3GPP connectivity and multiple GTP bearers in the Trusted Non-3GPP IP Access is out of 3GPP scope.

For Trusted non-3GPP access to the EPC, the PDN connectivity is made up of the concatenation of Non-3GPP connectivity (between the UE and the Trusted Non-3GPP access) and of GTP bearer(s) over S2a.

The GTP based S2a interface is similar to GTP-S5/S8 and GTP-S2b. The Trusted Non 3GPP access handles the UL TFT received from the PGW over GTP with the same way as an ePDG terminating GTP based S2b handles the UL TFT received from the PGW.

Whether GTP or PMIP is used in the network for S2a is transparent to the UE.

6.1.3 Information flows

6.1.3.1 Initial Attach Procedure with GTP on S2a and Anchoring in PDN GW

NOTE 1: The exact list of parameters signalled in GTP S2a information flows will be defined during normative work.

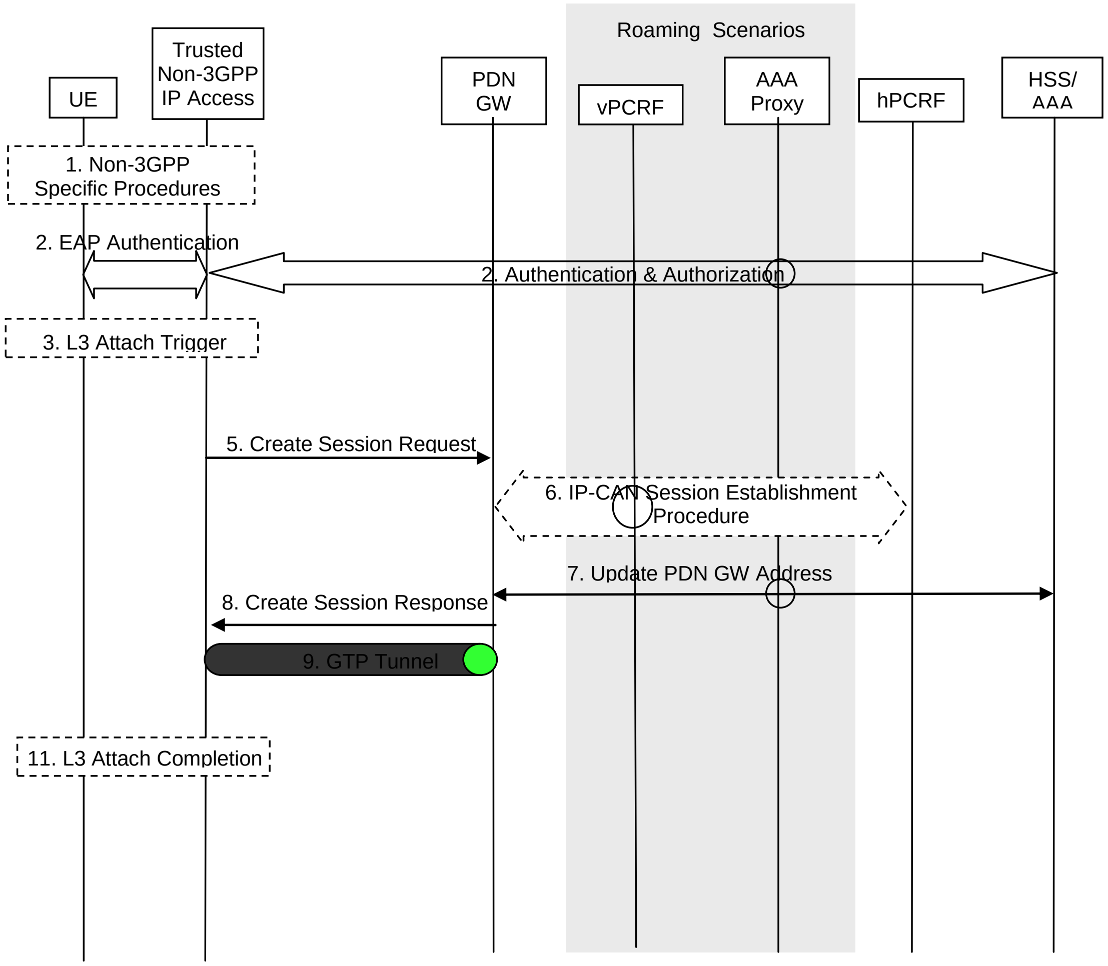

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. L3 Attach Trigger
5. Create Session Request
6. IP-CAN Session Establishment Procedure
7. Update PDN GW Address
8. Create Session Response
9. GTP Tunnel
11. L3 Attach Completion

Figure 6.1.3.1-1: Initial attachment with Network-based MM mechanism over S2a for roaming, LBO and non-roaming scenarios

Principles are similar to those specified for the PMIPv6 S2a call flow in clause 6.2.1 of TS 23.402 [3], but with GTP signalling and following differences:

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 6.1.3.1-1.

- 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 home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy are not involved, except for the authentication and authorization in step 2.

1) As for step 1 of clause 6.2.1 of TS 23.402 [3].

2) As for step 2 of clause 6.2.1 of TS 23.402 [3], with the following additions:

   - Upon successful authorization, the 3GPP AAA server downloads authorization (subscription) data to the Trusted non-3GPP Access. This information is used at step 5.

   - The Trusted non 3GPP IP Access selects the S2a protocol variant (GTP vs PMIP). The Trusted non 3GPP IP Access may be configured with the S2a protocol variant(s) on a per HPLMN granularity, or may retrieve information regarding the S2a protocol variants supported by the PDN GW (PMIP or/and GTP) from the Domain Name Service function.

   - The Trusted non-3GPP IP Access selects the PGW as per the existing PGW selection procedure; if the Trusted non-3GPP IP Access receives a PGW Identity under the form of a FQDN, it shall derive it to an IP address according to the selected mobility management protocol (here GTP).

NOTE 2: As per existing principles, to support separate PDN GW addresses at a PDN GW for different mobility protocols (e.g. PMIP, MIPv4 or GTPv2), the PDN GW Selection function takes mobility protocol type into account when deriving PDN GW address by using the Domain Name Service function.

3) As for step 3 of clause 6.2.1 of TS 23.402 [3].

NOTE 3: Only when IPv4, the L3 trigger may be relayed to the PDN GW after the GTP tunnel has been setup in step 9 using deferred IPv4 address mechanism.

4) Step 4 of clause 6.2.1 of TS 23.402 [3] is skipped.

5) The Trusted non-3GPP IP Access sends a Create Session Request (IMSI, APN, RAT type, Trusted non-3GPP IP Access TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, Default EPS Bearer QoS, Trusted non-3GPP IP Access Address for the user plane, Trusted non-3GPP IP Access TEID of the user plane, APN-AMBR, Selection Mode, Dual Address Bearer Flag, Trace Information, Charging Characteristics, Protocol Configuration Options) message to the PGW. The RAT type indicates the non-3GPP IP access technology type. The PDN Type shall be set based on the requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach in TS 23.401 [6]. The Trusted non-3GPP IP Access Network shall set the Dual Address Bearer Flag when the PDN type is set to IPv4v6 and all SGSNs which the UE may be handed over to are Release 8 or above supporting dual addressing, which is determined based on node pre-configuration by the operator. The Trusted non-3GPP IP Access Network shall include Trace Information if PDN GW trace is activated.

   The PGW creates a new entry in its bearer context table and generates a Charging Id. The new entry allows the PGW to route user plane PDUs between the Trusted non-3GPP IP Access Network and the packet data network and to start charging.

NOTE 4: The EPS Bearer Identity and Default EPS Bearer QoS parameters convey the S2a bearer identity and the default S2a bearer QoS.

NOTE 5: As part of the access specific study it will be clarified whether step 5 (Create Session Request) is triggered by the completion of the authentication procedure (step 2) either/or by the reception of the L3 Attach trigger (step 3).

6) As for step 6 of clause 6.2.1 of TS 23.402 [3] except that there is no associated Gateway Control Sessions.

7) As for step 7 of clause 6.2.1 of TS 23.402 [3], with the following addition:

   - when informing the 3GPP AAA Server of the PDN GW identity, the selected PDN GW also indicates the selected S2a protocol variant (here GTP); this allows the option for the 3GPP AAA Server or 3GPP AAA Proxy not to return to the PDN GW PMIP specific parameters (e.g. static QoS Profile, Trace Information, APN-AMBR) if GTP is used over S2a; the PDN GW shall ignore those parameters if received from the 3GPP AAA Server or 3GPP AAA Proxy.

8) The PDN GW returns a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS

Bearer QoS, APN-AMBR, Protocol Configuration Options, Cause) message to the Trusted non-3GPP IP Access, including the IP address(es) allocated for the UE.

NOTE 6: If the L3 attach trigger is relayed to the PDN GW, the IP address will not be returned in the Create Session Response.

The PGW may initiate the creation of dedicated bearers on GTP based S2a (like it may do it on GTP based S5/S8 for an Attach on 3GPP access).

9) The GTP tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

NOTE 7: If the L3 Attach trigger is relayed to the PDN GW, the DCHP request is sent to the PDN GW in the established GTP tunnel.

10) Step 10 of clause 6.2.1 of TS 23.402 [3] is skipped.

11) As for step 11 of clause 6.2.1 of TS 23.402 [3].

6.1.3.2 Detach and PDN Disconnection with GTP on S2a

6.1.3.2.1 UE/Trusted Non-3GPP IP Access Network Initiated Detach and UE/Trusted Non-3GPP IP Access requested PDN Disconnection Procedure with GTP on S2a

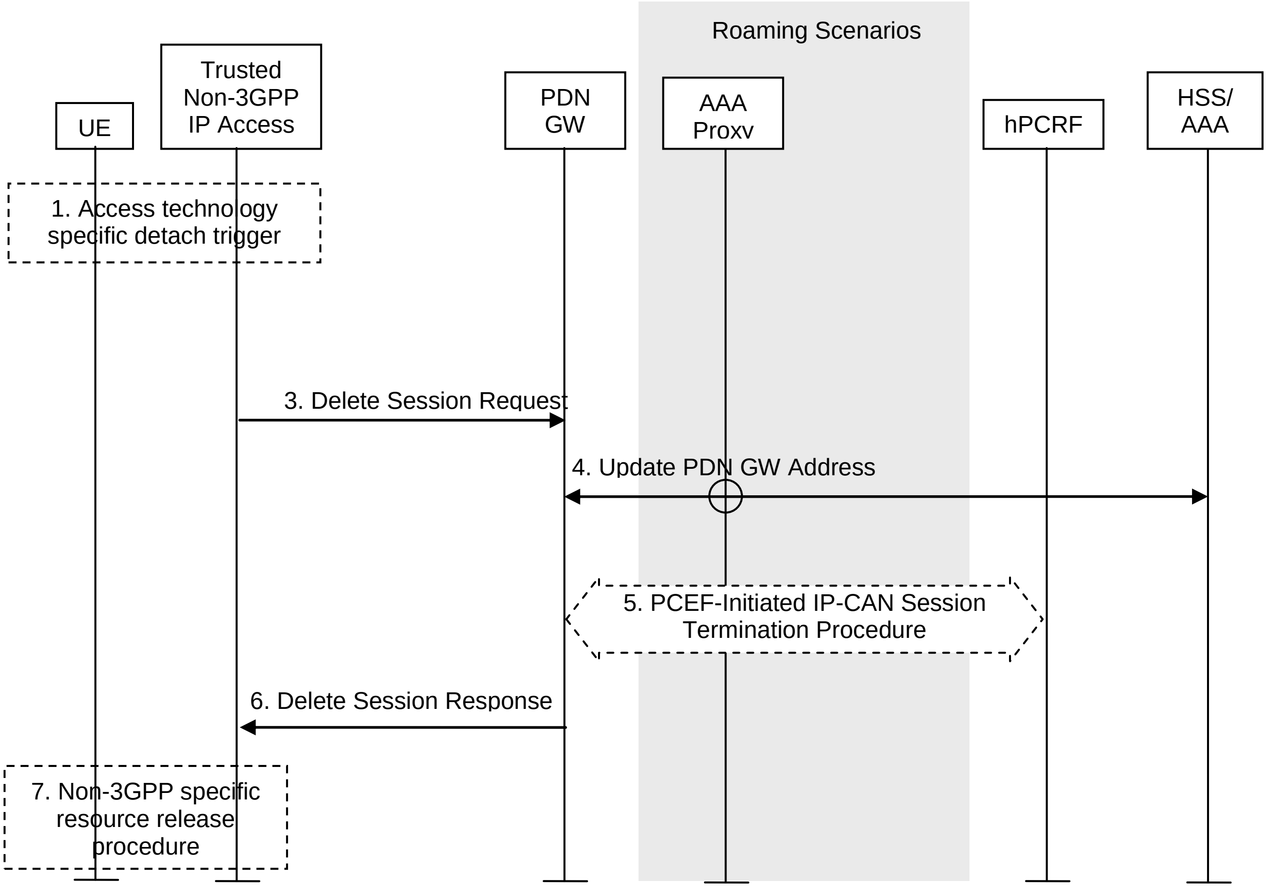

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
PDN GW
AAA Proxv
hPCRF
HSS/ AAA
1. Access technology specific detach trigger
3. Delete Session Request
4. Update PDN GW Address
5. PCEF-Initiated IP-CAN Session Termination Procedure
6. Delete Session Response
7. Non-3GPP specific resource release procedure

Figure 6.1.3.2.1-1: UE/Trusted Non-3GPP Access Network initiated detach procedure or PDN-disconnection with GTP on S2a

Principles are similar to those specified for the PMIP S2a call flow in clause 6.4.1.1 of TS 23.402 [3], but with GTP signalling:

1) as for step 1 of clause 6.4.1.1 of TS 23.402 [3].

2) step 2 of clause 6.4.1.1 of TS 23.402 [3] is skipped.

3) The active Bearer(s) Trusted non-3GPP IP Access regarding this particular UE and PDN connection are deactivated by the Trusted non-3GPP IP Access sending a Delete Session Request (Linked EPS Bearer ID) to the PGW for the related PDN connection.

4 to 5) as for steps 4 to 5 of clause 6.4.1.1 of TS 23.402 [3].

6) The PDN GW acknowledges with Delete Session Response (Cause).

7) as for step 7 of clause 6.4.1.1 of TS 23.402 [3].

6.1.3.2.2 HSS/AAA Initiated Detach Procedure with GTP on S2a

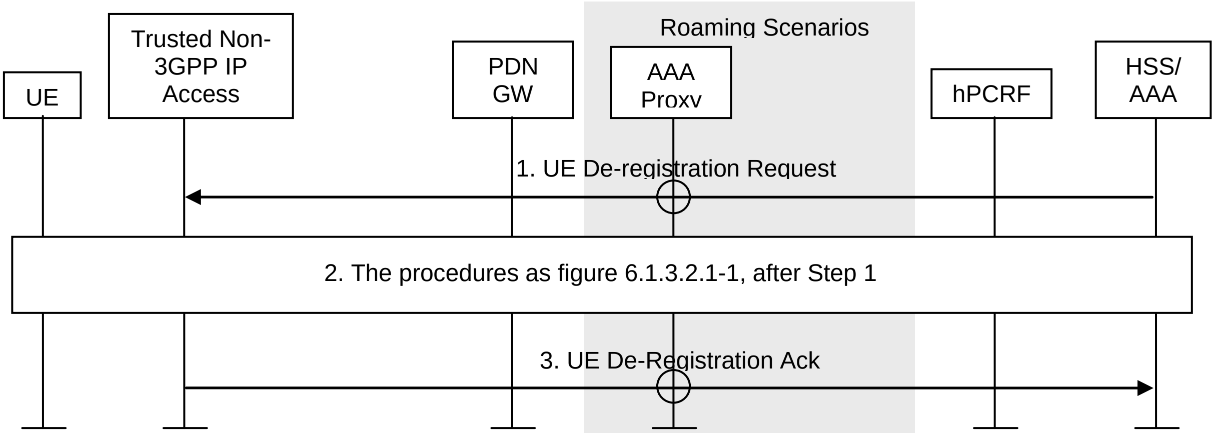

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
PDN GW
AAA Proxy
hPCRF
HSS/ AAA
1. UE De-registration Request
2. The procedures as figure 6.1.3.2.1-1, after Step 1
3. UE De-Registration Ack

Figure 6.1.3.2.2-1: HSS/AAA-initiated detach procedure with GTP on S2a

Principles are similar to those specified for the PMIP S2a call flow in clause 6.4.2.1 of TS 23.402 [3], but with GTP signalling:

1) As for step 1 of clause 6.4.2.1 of TS 23.402 [3].

2) This includes the procedures after step 1 as for Figure 6.1.3.2.1-1.

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

3) As for step 3 of clause 6.4.2.1 of TS 23.402 [3].

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the GTP tunnels on S2a, since the Trusted non-3GPP IP Access is responsible for removing those tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the HSS/AAA.

6.1.3.3 UE-initiated Connectivity to Additional PDN with GTP on S2a

Establishment of connectivity to an additional PDN over Trusted Non-3GPP IP Access with S2a is supported only for the accesses that support such feature and the UEs that have such capability.

During the establishment of a new PDN connection, the Trusted Non-3GPP IP Access allocates and sends a default EPS bearer ID to the PDN GW. The default EPS bearer ID is unique in the scope of the UE within an Trusted Non-3GPP IP Access, i.e. the IMSI and the default EPS bearer ID together identify a PDN connection within an Trusted Non-3GPP IP Access. In order to be able to identify a specific established PDN connection, both the Trusted Non-3GPP IP Access and the PDN GW shall store the default EPS bearer ID.

For network supporting multiple mobility protocols, the AAA/HSS enforces the same IPMS decision for each additional PDN connection as for initial attach.

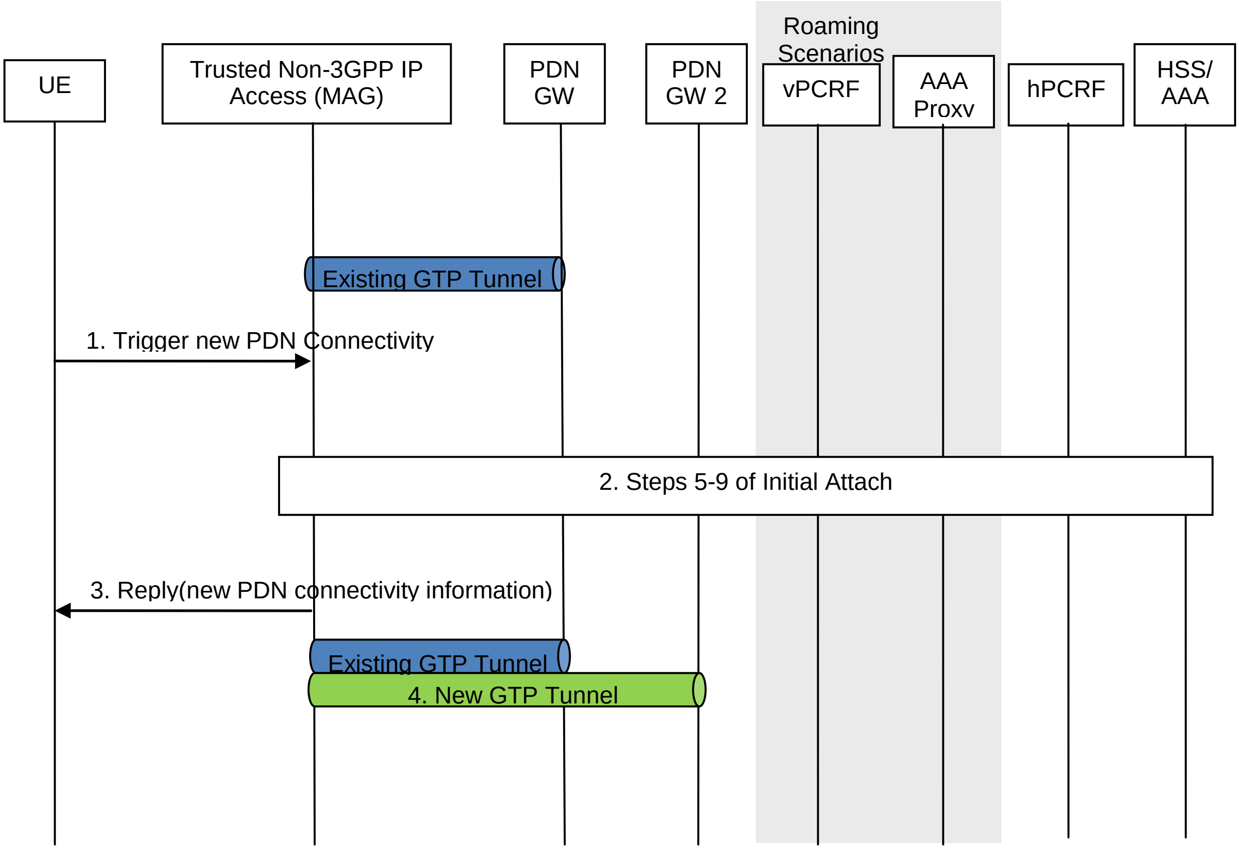

UE
Trusted Non-3GPP IP Access (MAG)
PDN GW
PDN GW 2
Roaming Scenarios
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Existing GTP Tunnel
1. Trigger new PDN Connectivity
2. Steps 5-9 of Initial Attach
3. Reply(new PDN connectivity information)
Existing GTP Tunnel
4. New GTP Tunnel

Figure 6.1.3.3-1: Additional PDN connectivity with GTP on S2a for non-roaming and roaming

The steps in the procedure which are marked as optional occur only if dynamic policy provisioning has been deployed.

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 6.1.3.3-1.

- 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 home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy are not involved.

1) When the UE wishes to connect to an additional PDN, it sends a trigger indicating that connectivity with that specific PDN is desired. The UE provides information about the new PDN by using an APN. When multiple PDN connections to a single APN are supported then some additional access specific mechanism is needed between the UE and the Trusted Non-3GPP IP Access to differentiate the PDN connections towards the same APN. If supported by the non-3GPP access, the UE may send Protocol Configuration Options in this step using access specific mechanisms. The Protocol Configuration Options provided by the UE may include the user credentials for PDN access authorization. The UE triggers the re-establishment of existing PDN connectivity after the handover by providing a Request Type indicating "Handover" on accesses that support the indication.

NOTE 1: The definition of the trigger that the UE provides to the access network is out of scope of 3GPP.

2) At this step the Trusted non-3GPP IP Access performs PDN GW selection as described in Steps 5 to 9 of Initial Attach procedure, while PDN GW2 is selected.

3) The Trusted non-3GPP IP Access sends the reply message to the UE with the allocated IP address from the PDN that the UE indicated at step 1. If supported by the non-3GPP access, the Protocol Configuration Options provided by the PDN GW2 in step 2 are returned to the UE in this step using access specific mechanisms. Since UE requested for additional PDN connectivity, the UE configures the IP address received from the Trusted Non-3GPP IP Access without deleting its configuration for connectivity with any other previously established PDN.

NOTE 2: The definition of the message used to carry the new connectivity information to the UE is out of scope of 3GPP.

4) The GTP tunnel is thus set up between the Trusted Non-3GPP IP Access and the PDN GW corresponding to the requested additional PDN while maintaining tunnels previously established for other PDNs.

6.1.3.4 Dedicated bearer activation with GTP on S2a

The dedicated bearer activation procedure for GTP based S2a is depicted in figure 6.1.3.4-1.

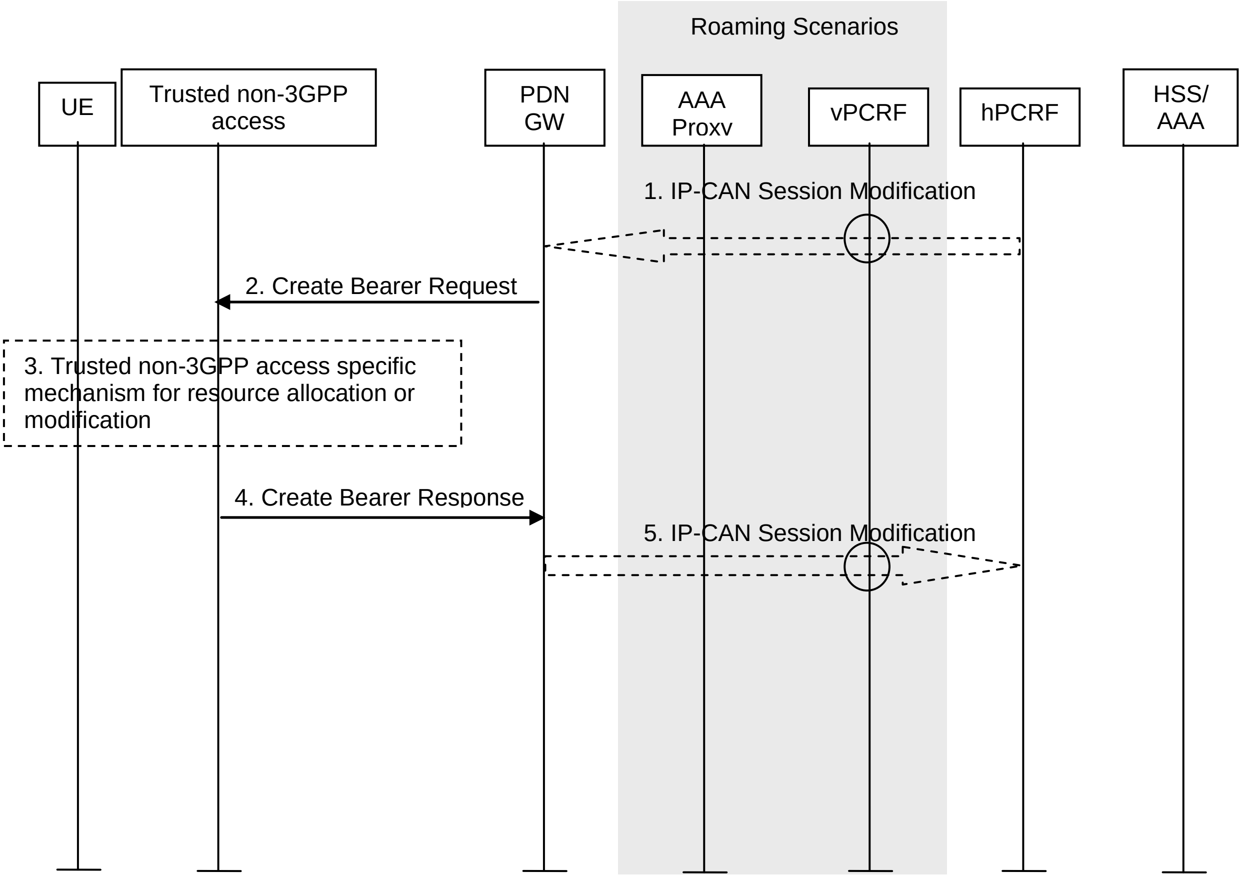

Roaming Scenarios
UE
Trusted non-3GPP access
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. IP-CAN Session Modification
2. Create Bearer Request
3. Trusted non-3GPP access specific mechanism for resource allocation or modification
4. Create Bearer Response
5. IP-CAN Session Modification

Figure 6.1.3.4-1: Dedicated S2a Bearer Activation Procedure with GTP on S2a

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], up to the point that the PDN GW requests IP CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

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 trusted non-3GPP access. The Linked EPS bearer Identity (LBI) is the EPS bearer Identity of the default S2a bearer.

3. If supported by the trusted non-3GPP access, a trusted non-3GPP access 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 trusted non-3GPP access selects an EPS bearer Identity, which has not yet been assigned to the UE. The trusted non-3GPP access then stores the EPS bearer Identity and links the dedicated S2a bearer to the default S2a bearer indicated by the Linked Bearer Identity (LBI). The trusted non-3GPP access uses the uplink packet filter (UL TFT) to determine the mapping of uplink traffic flows to the S2a bearer. The trusted non-3GPP access then

acknowledges the S2a bearer activation to the PGW by sending a Create Bearer Response (EPS bearer Identity, trusted non-3GPP access Address for the user plane, trusted non-3GPP access TEID of the user plane) message.

5. If the dedicated bearer activation procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not, allowing the completion of the PCRF-Initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], after the completion of IP CAN bearer signalling.

NOTE 1: The exact signalling of step 1 and 5 (e.g. for local break-out) is outside the scope of this TR. This signalling and its interaction with the dedicated bearer activation procedure are to be specified in TS 23.203 [4]. Steps 1 and 5 are included here only for completeness.

6.1.3.5 Network-initiated S2a bearer modification with GTP on S2a

6.1.3.5.1 PDN GW Initiated Bearer Modification

The PDN GW initiated bearer modification procedure for a GTP based S2a is depicted in figure 6.1.3.5.1-1. 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 6.1.3.5.2).

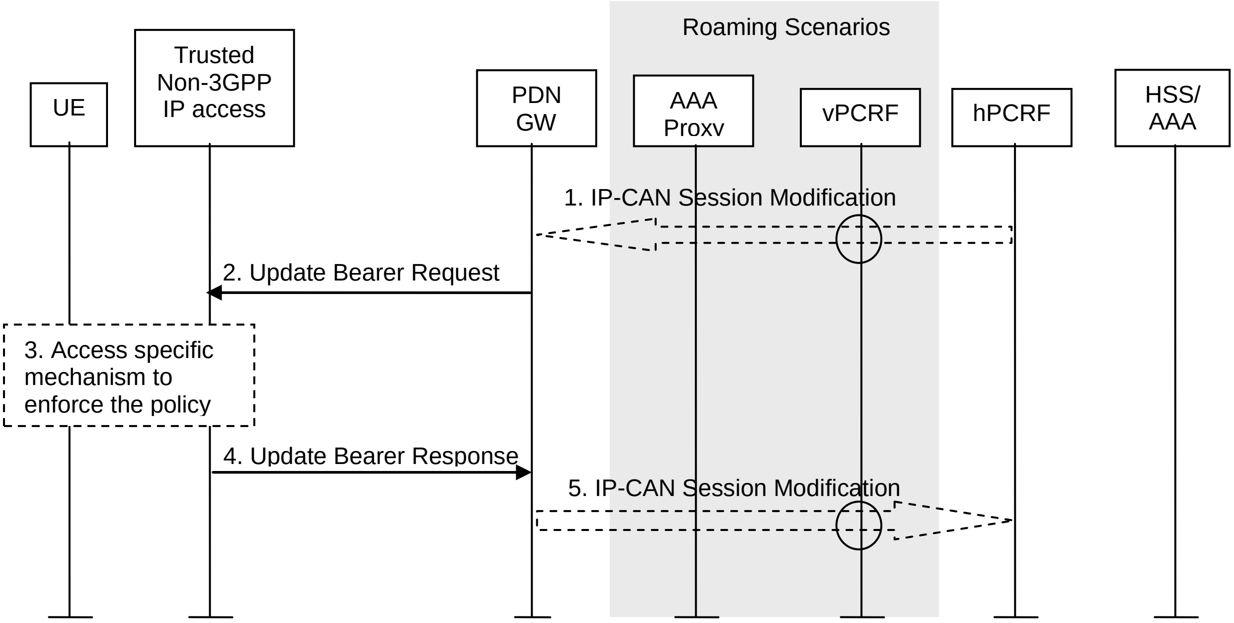

Roaming Scenarios
UE
Trusted Non-3GPP IP access
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. IP-CAN Session Modification
2. Update Bearer Request
3. Access specific mechanism to enforce the policy
4. Update Bearer Response
5. IP-CAN Session Modification

Figure 6.1.3.5.1-1: PDN GW-initiated S2a Bearer Modification Procedure with GTP on S2a

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], up to the point that the PDN GW requests IP-CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

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 trusted non-3GPP IP access.

3. If supported by the trusted non-3GPP access, an IP-CAN specific resource allocation or resource release procedure may be triggered by the enforcement of the received policy rules. The details of this step are out of the scope of 3GPP.

4. The trusted non-3GPP IP access 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. If the Bearer modification procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not by sending a Provision Ack message allowing the completion of the PCRF-Initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], after the completion of IP CAN bearer signalling.

NOTE: The exact signalling of step 1 and 5 (e.g. for local break-out) is outside the scope of this TR. This signalling and its interaction with the bearer activation procedure are to be specified in TS 23.203 [4]. Step 1 and 5 are included here only for completeness.

6.1.3.5.2 HSS Initiated Subscribed QoS Modification

The HSS Initiated Subscribed QoS Modification for a GTP-based S2a is depicted in figure 6.1.3.5.2-1.

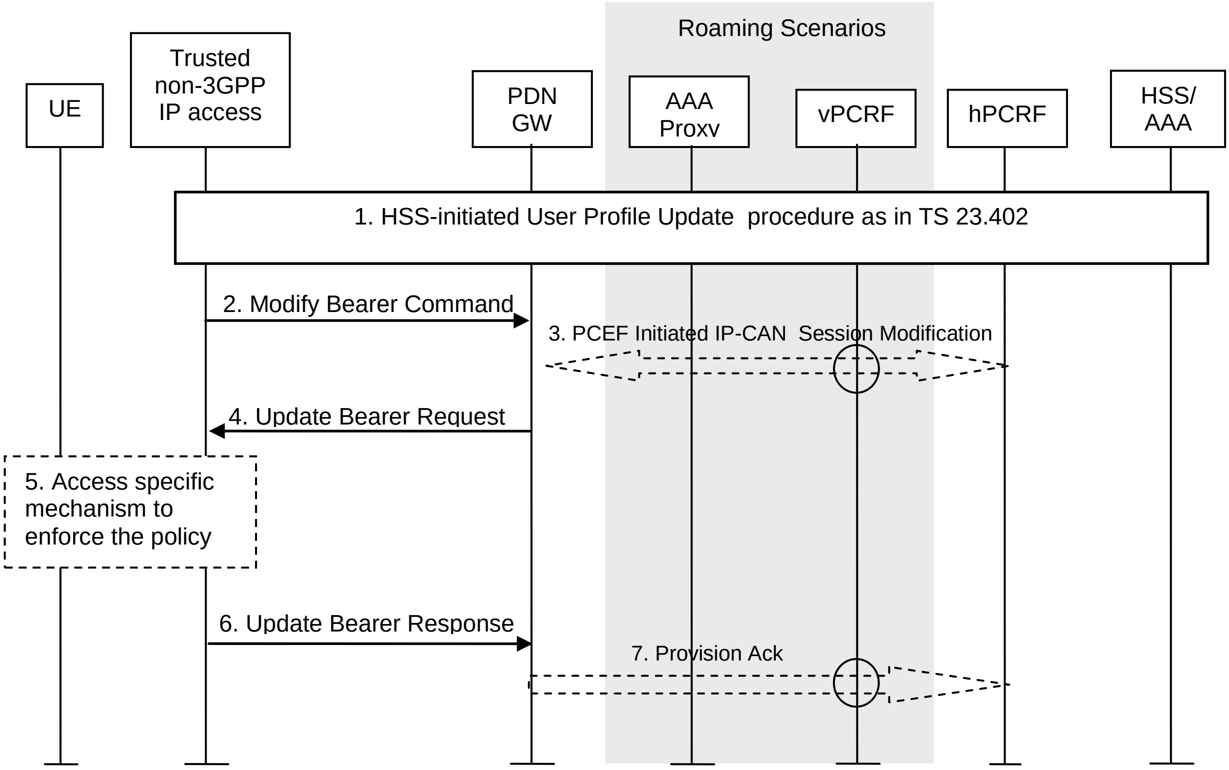

Roaming Scenarios
UE
Trusted non-3GPP IP access
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. HSS-initiated User Profile Update procedure as in TS 23.402
2. Modify Bearer Command
3. PCEF Initiated IP-CAN Session Modification
4. Update Bearer Request
5. Access specific mechanism to enforce the policy
6. Update Bearer Response
7. Provision Ack

Figure 6.1.3.5.2-1: HSS Initiated Subscribed QoS Modification

1. The HSS updates the User Profile as specified in clause 12.2.1 of TS 23.402 [3].

2. 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 trusted non-3GPP IP access 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.

3. If PCC infrastructure is deployed, the PDN GW informs the PCRF about the updated EPS bearer QoS. The PCRF sends the new updated PCC decision to the PDN GW. This corresponds to the PCEF-initiated IP CAN Session Modification procedure as defined in TS 23.203 [4].

   The PCRF may modify the APN-AMBR and the QoS parameters (QCI and ARP) associated with the default bearer in the response to the PDN GW as defined in TS 23.203 [4].

4. 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 trusted non-3GPP IP access.

5. If supported by the trusted non-3GPP access, an IP-CAN specific procedure may be triggered by the enforcement of the received policy rules. The details of this step are out of the scope of 3GPP.
6. The trusted non-3GPP IP access 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.
7. The PDN GW indicates to the PCRF whether the requested PCC decision was enforced or not by sending a Provision Ack message.

6.1.3.6 PDN GW initiated Resource Allocation Deactivation with GTP on S2a

This procedure depicted in figure 6.1.3.6-1 can be used to deactivate a dedicated bearer or deactivate all bearers belonging to a PDN address, for e.g., 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 a handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

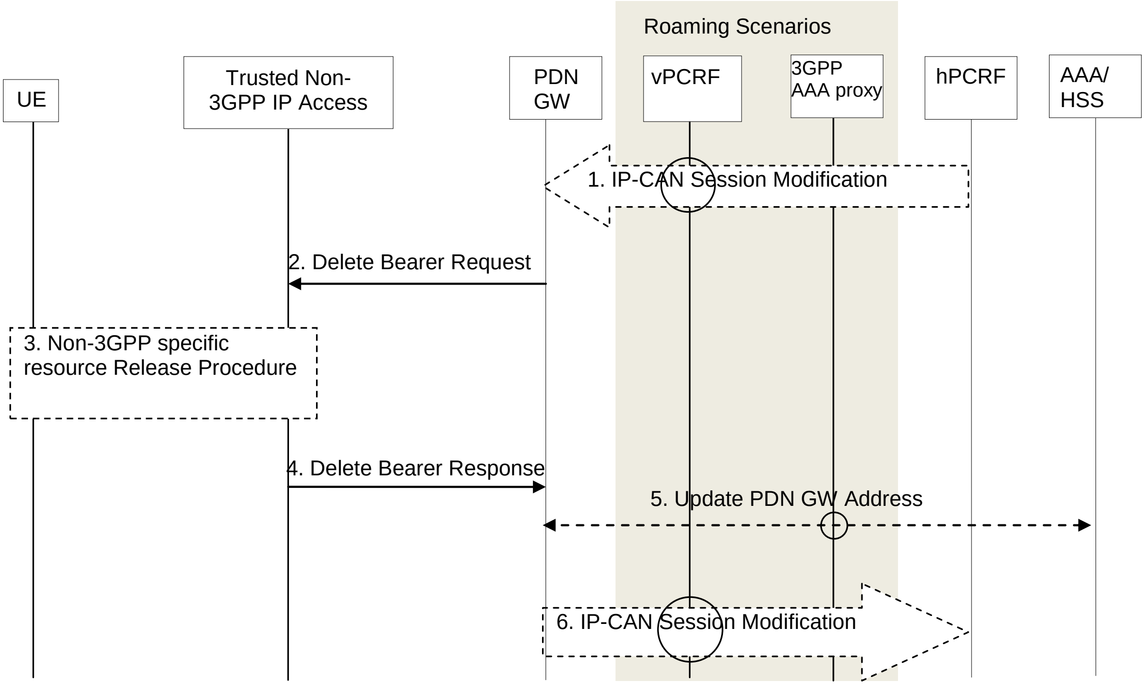

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
PDN GW
vPCRF
3GPP AAA proxy
hPCRF
AAA/ HSS
1. IP-CAN Session Modification
2. Delete Bearer Request
3. Non-3GPP specific resource Release Procedure
4. Delete Bearer Response
5. Update PDN GW Address
6. IP-CAN Session Modification

Figure 6.1.3.6-1: 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 6.1.3.6-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured within the PDN GW.

1. If dynamic PCC is deployed, the PDN GW initiated Bearer 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 Delete Bearer Request message (EPS Bearer Identity, Cause) to the trusted non-3GPP IP access.
3. If supported by the trusted non-3GPP access, the Non 3GPP specific resources may be released in the non-3GPP IP access. The details of this step are out of the scope of 3GPP.
4. The trusted non-3GPP IP access 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. If this is the last PDN connection for the given APN, the PDN GW identity information and APN corresponding to the UE's PDN Connection is removed from the AAA Server/HSS. This information is de-registered from the HSS as described in TS 23.402 [3].
6. The PDN GW deletes the bearer context related to the deactivated EPS 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.

6.1.3.7 Handovers without Optimizations Between 3GPP Accesses and Non-3GPP IP Accesses with S2a GTP

6.1.3.7.1 Handover from a trusted non-3GPP IP access with S2a GTP to 3GPP Access

The handover procedure from a trusted non-3GPP IP access using GTP S2a to E-UTRAN access using GTP S5/S8 connected to EPC is similar to the procedure specified in TS 23.402 [3], clause 8.2.1.1, except that:

- at step 1, the tunnel between trusted non-3GPP access and the PGW is a GTP tunnel;
- at step 7, the PDN GW may create dedicated bearers during this procedure.
- at step 18, the PDN GW shall initiate resource allocation deactivation procedure in the trusted non-3GPP IP access as defined in clause 6.1.3.6 PDN GW initiated Resource Allocation Deactivation with GTP on S2a.

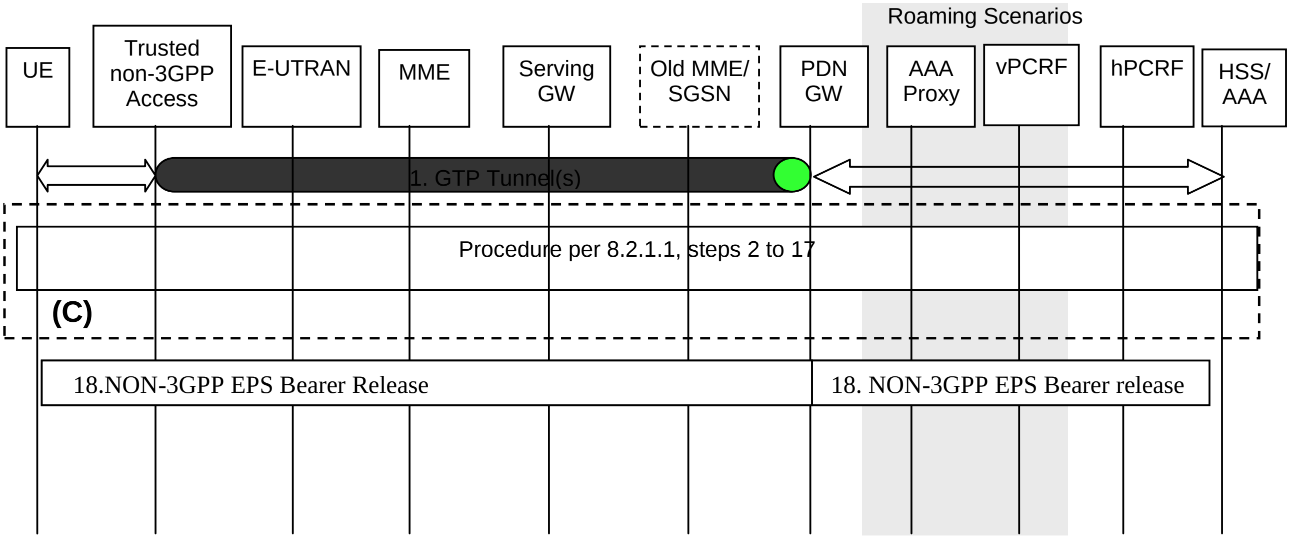


Figure 6.1.3.7.1-1: Handover from Trusted Non-3GPP IP Access with GTP on S2a to E-UTRAN

The handover procedure from a trusted non-3GPP IP access using GTP S2a to UTRAN/GERAN access using GTP S5/S8 connected to EPC is similar to the procedure specified in TS 23.402 [3], clause 8.2.1.3, except that:

- at step 1, the tunnel between trusted non-3GPP access and the PGW is a GTP tunnel;
- at step 10, the PDN GW may create dedicated bearers during this procedure.

- at step 17, the PDN GW shall initiate resource allocation deactivation procedure in the trusted non-3GPP IP access as defined in clause 6.1.3.6 PDN GW initiated Resource Allocation Deactivation with GTP on S2a.

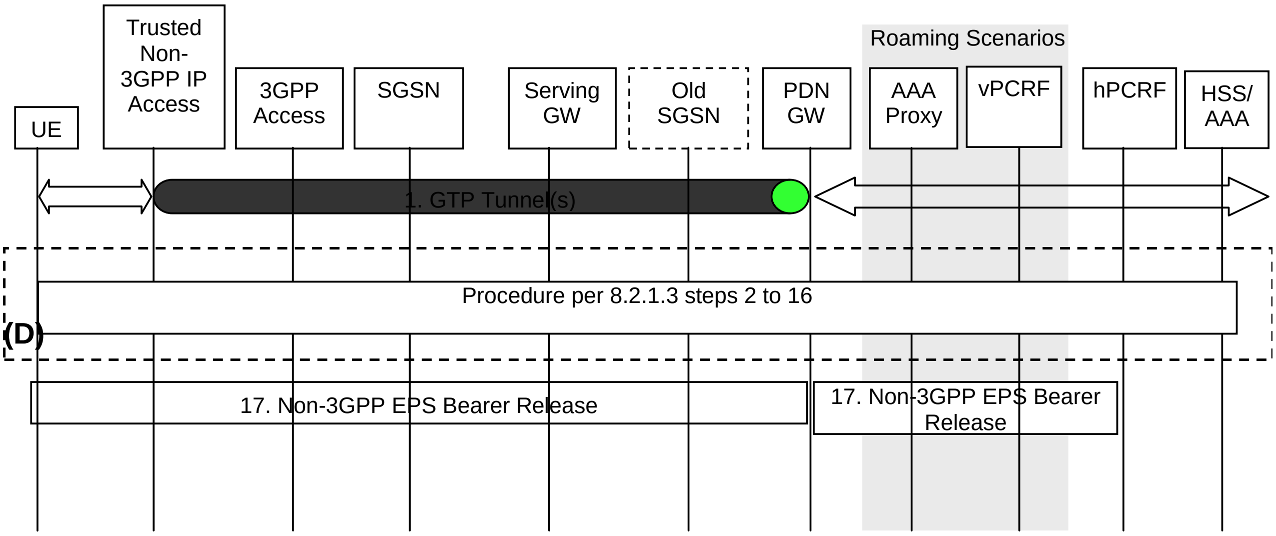

Trusted Non-3GPP IP Access
Roaming Scenarios
3GPP Access
SGSN
Serving GW
Old SGSN
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
UE
1. GTP Tunnel(s)
Procedure per 8.2.1.3 steps 2 to 16
(D)
17. Non-3GPP EPS Bearer Release
17. Non-3GPP EPS Bearer Release

Figure 6.1.3.7.1-2: Handover from Trusted Non-3GPP IP Access with GTP on S2a to UTRAN/GERAN

6.1.3.7.2 Handover from 3GPP Access to a trusted non-3GPP IP access with S2a GTP

NOTE 1: This procedure is based on TS 23.402 [3], clause 8.2.2. Only the differences are described below.

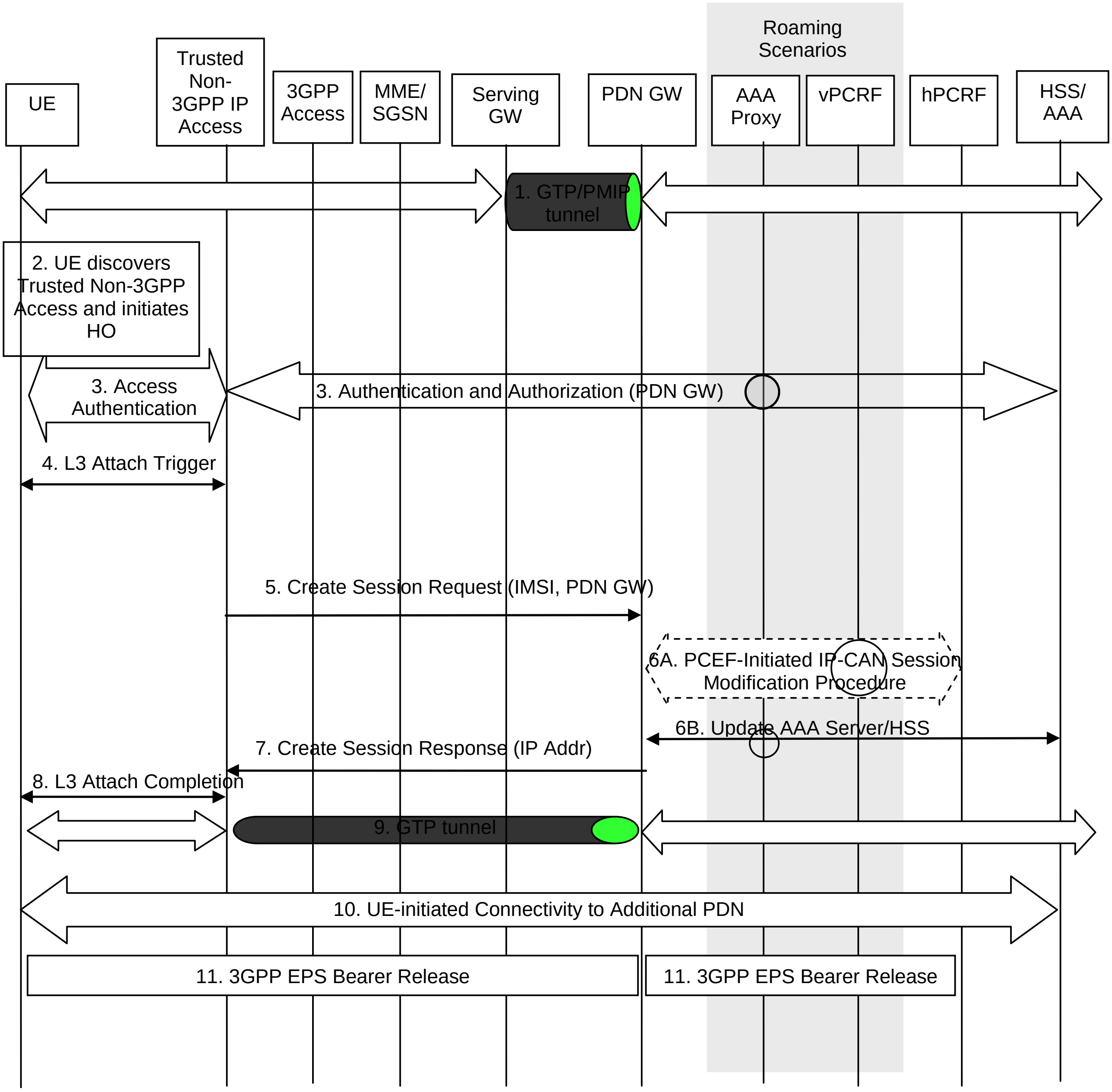

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
3GPP Access
MME/ SGSN
Serving GW
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. GTP/PMIP tunnel
2. UE discovers Trusted Non-3GPP Access and initiates HO
3. Access Authentication
3. Authentication and Authorization (PDN GW)
4. L3 Attach Trigger
5. Create Session Request (IMSI, PDN GW)
6A. PCEF-Initiated IP-CAN Session Modification Procedure
6B. Update AAA Server/HSS
7. Create Session Response (IP Addr)
8. L3 Attach Completion
9. GTP tunnel
10. UE-initiated Connectivity to Additional PDN
11. 3GPP EPS Bearer Release
11. 3GPP EPS Bearer Release

Figure 6.1.3.7.2-1: Handover from 3GPP Access to Trusted Non-3GPP IP Access with GTP on S2a

1-4) Same as step 1-4 in TS 23.402 [3] clause 8.2.2 except that at step 1, the tunnel between Serving GW and the PGW may be both a GTP or a PMIP tunnel.

5) The entity in the Trusted non-3GPP IP Access sends Create Session Request (IMSI, APN, Handover Indication, RAT type, Trusted non-3GPP IP Access TEID of the control plane, Trusted non-3GPP IP Access Address for the user plane, Trusted non-3GPP IP Access TEID of the user plane, EPS Bearer Identity) message to the PDN GW. The RAT type indicates the non-3GPP IP access technology type. If the UE supports IP address preservation and included the address in early steps, the Trusted non-3GPP IP Access sets the 'Handover Indication' in the Creation Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF.

NOTE 2: With GTP on S2a, APN, IMSI and EPS Bearer ID identifies a PDN connection over GTP based S2a.

NOTE 3: With GTP on S2a, there is no relation between the values of the EPS bearer identities used within 3GPP networks and non-3GPP networks.

NOTE 4: In a non-3GPP to 3GPP access handover, the 'Handover Indication' leads the PDN GW to delay switching the DL user plane traffic from non-3GPP to 3GPP until a subsequent Modify Bearer Request is received. In a 3GPP to non-3GPP handover scenario with GTP based S2a, the 'Handover Indication' should not delay the switching of DL user plane traffic from 3GPP to non-3GPP access.

6A-6B) Same as steps 7A and 7B in TS 23.402 [3] clause 8.2.2 with following additions:

- at step 8, the PDN GW may create dedicated bearers during this procedure.

7) The PDN GW responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Charging ID, Cause) message to the Trusted non-3GPP IP Access. The Create Session Response contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access.

8-11) Same as step 9-12 in TS 23.402 [3] clause 8.2.2, except that at step 12, the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

7 Additional considerations for WLAN access to EPC through S2a for Phase 1

7.1 Solutions without UE Impact

7.1.0 General

1) Multiple PDN connections in the WLAN access

Since the support of multiple PDN connections in the WLAN access would require the UE to signal the APN, a solution without UE impact only considers a single PDN connection in WLAN. This does not preclude multiple PDN connections through 3GPP and WLAN as long as there is only one PDN connection using WLAN access.

2) Mobility aspects

A solution without any impact to the UE only considers mobility without IP address preservation: the preservation on WLAN of the IP address the UE used on the 3GPP access would require changes in existing UEs as it is not specified in current 3GPP specifications.

NOTE: The security considerations of the internal WLAN-based trusted non-3GPP access network architecture are outside the scope of this study item.

7.1.1 Solution 1

7.1.1.1 Reference model

When the WLAN is considered as trusted by the operator, the WLAN AN is interfaced as any trusted non-3GPP access i.e. via STa to the 3GPP AAA Server and via S2a to a PDN-GW. EPC access via Trusted WLAN is supported through S2a interface. A single SSID offering simultaneous access for a UE to EPC through S2a and non-seamless offload is not supported. Non-seamless offload may however be supported in some deployments (e.g. with separate SSIDs for non-seamless offload and access to EPC through S2a via Wireless LAN, see clause 7.1.1.4).

The reference model is depicted in the following figure.

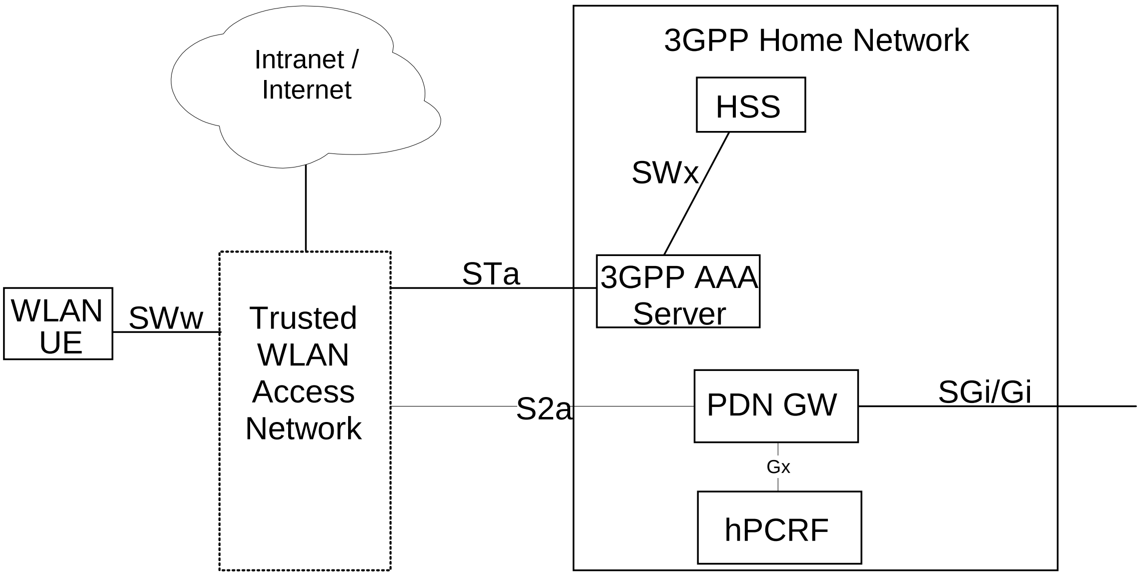


Figure 7.1.1.1-1: Non-roaming Trusted WLAN Inter-working reference model

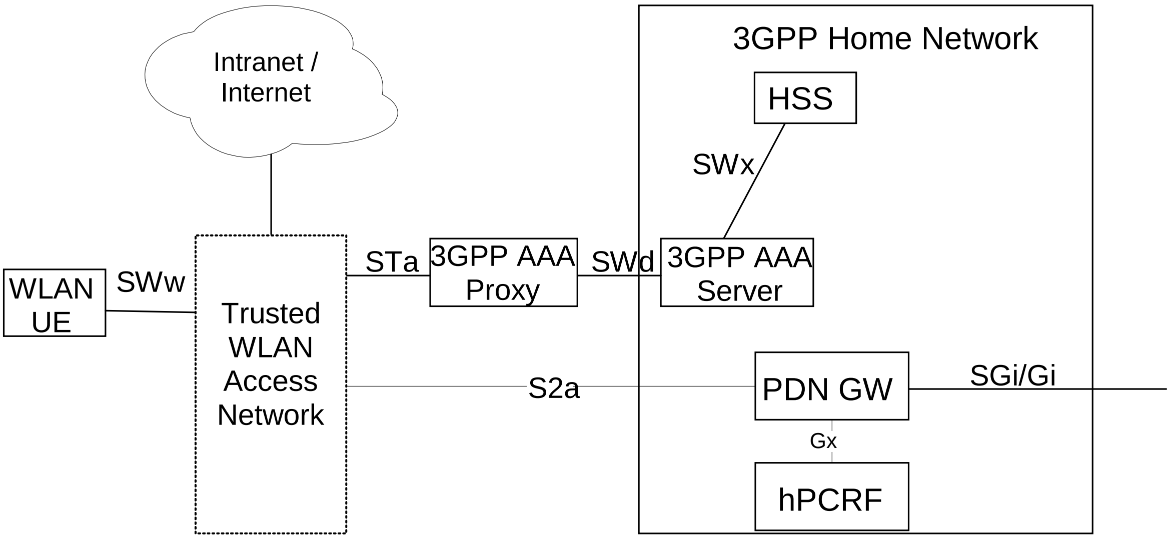


Figure 7.1.1.1-2: Home Routed Roaming Trusted WLAN Inter-working reference model

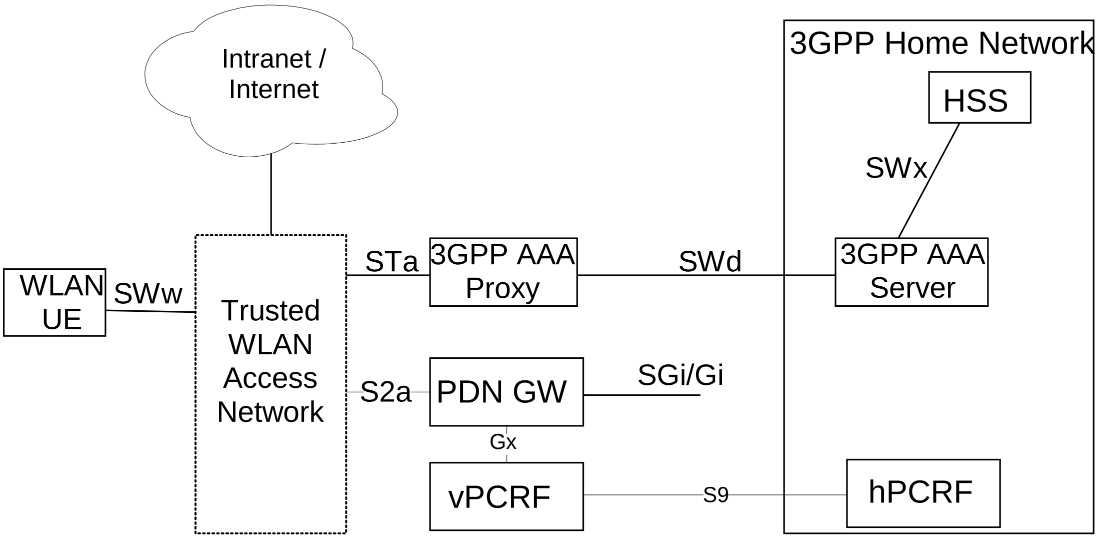


Figure 7.1.1.1-3: Local Breakout Roaming Trusted WLAN Inter-working reference model

Within the trusted non-3GPP IP access network (TNAN) we distinguish three functions:

- A WLAN Access Network (WLAN AN). This function terminates the UE's WiFi air link defined in IEEE 802.11 [5].
- A Trusted non-3GPP access's S2a peer (TNSP). This function terminates S2a.
- A Trusted non-3GPP access's STa peer (TNAP). This function terminates STa.

NOTE 1: Policy and QoS aspects are studied as part of BBAI.

NOTE 2: Whether multiple TNAN functions are mapped to a single non-3GPP access entity, or a single TNAN function is distributed among multiple non-3GPP access entities is out-of-scope of 3GPP.

STa reference point

The STa reference point is defined in TS 23.402 [3] and specified in TS 29.273 [7]. It connects the Trusted non-3GPP IP Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.

STa might need to be enhanced to support:

- A way for the Trusted WLAN Access Network to provide the AAA server with following information:
  - An indication on whether the Trusted WLAN AN supports S2a, non-seamless offload or both;

NOTE 3: Stage 3 discussions will determine whether existing "Mobility Capabilities" over STa may be reused for that purpose.

  - The SSID selected by the UE to access the Trusted WLAN AN.

- A way for the AAA server to provide the Trusted WLAN Access Network with following information:
  - The APN the user is to be associated with for EPC access; this is required for the Trusted WLAN Access Network to establish the PDN connection with the PDN GW. Based on the HPLMN operator configuration the HSS may provide the 3GPP AAA server with a default APN for Trusted WLAN Access Network.

NOTE 4: Stage 3 discussions will determine whether existing "Default APN" over STa may be reused for that purpose.

  - Whether access to EPC is allowed for the UE.

NOTE 5: Stage 3 discussions will determine whether existing "Mobility Capabilities" over STa may be reused for that purpose.

  - The UE IMSI; this is required for the Trusted WLAN Access Network to build the S2a messages towards the PDN-GW.

NOTE 6: Stage 3 discussions will determine whether existing "Permanent User Identity" over STa may be reused for that purpose.

SWw reference point

The SWw reference point connects the WLAN UE to the WLAN Access Network according to IEEE 802.11 [5]. This includes the support of:

- the security that was defined as part of 802.11-2007 [5] and thus the transport of EAP signalling messages for authentication signalling between the 3GPP AAA Server and the WLAN UE;
- parameters for identification of the operator networks for roaming purposes (i.e. PLMN list).

SWx reference point

The SWx reference point is defined for EPC in TS 23.402 [3]. It is specified at stage 3 level respectively in TS 29.273 [7].

7.1.1.2 Initial Attach Procedure with GTP on S2a and Anchoring in PDN GW

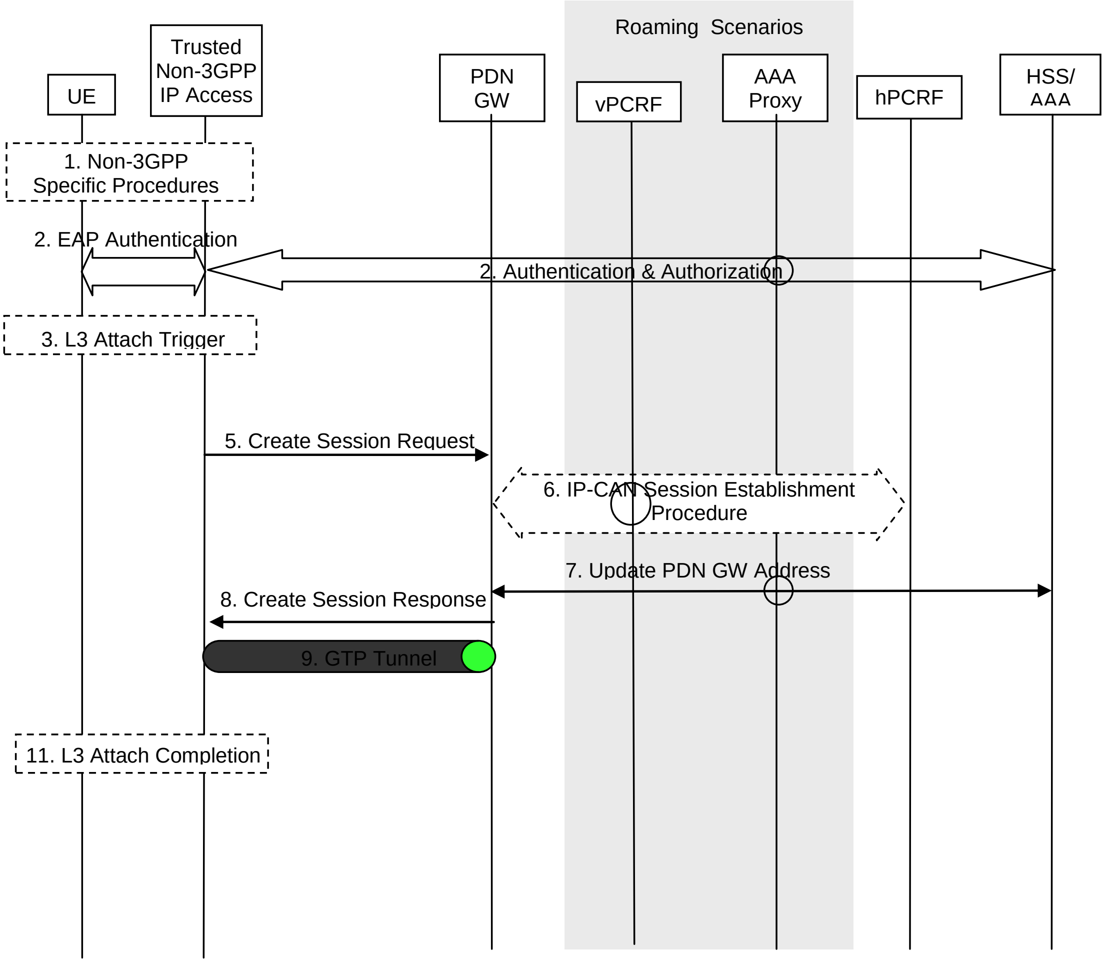

Roaming Scenarios
UE
Trusted Non-3GPP IP Access
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. L3 Attach Trigger
5. Create Session Request
6. IP-CAN Session Establishment Procedure
7. Update PDN GW Address
8. Create Session Response
9. GTP Tunnel
11. L3 Attach Completion

Figure 7.1.1.2-1: Initial attachment with Network-based MM mechanism over S2a for roaming, LBO and non-roaming scenarios

A per-UE point-to-point link between UE and TNSP is assumed. In particular, it is assumed that the trusted non-3GPP access does not do any routing of UE traffic between WLAN AN and TNSP. It is assumed that the WLAN AN applies upstream and downstream forced-forwarding between the UE's WiFi air link and the WLAN AN -TNSP link. The aspects of point-to-point link described in IETF RFC 5213 [17] and IETF RFC 5844 [18] also applies to the point-to-point link between UE and TNSP. The implementation of the point-to-point link is out-of-scope for 3GPP.

In this specific solution, it is assumed that TNSP is the first hop router and the DHCP server.

NOTE 1: The link model is different from GTP based S5/S8 and GTP based S2b.

No specific mechanisms are defined to support AP-to-AP handover.

Refer to clause 6.1.3.1. Based on assumptions for solutions with no impact to UE, UE cannot provide APN and PCO to TNSP. So, there are following differences than clause 6.1.3.1:

- At step 2, the following additions apply:
  - The HSS provide APN information to the Trusted Non-3GPP IP Access in the subscription data. HSS provides a default APN for WLAN. PDN type is indicated from HSS in this step. Based on the HPLMN operator configuration the HSS may provide the 3GPP AAA server with a default APN for Trusted WLAN Access Network.

NOTE 2: If the APN used in 3GPP side is the same as the default APN for Trusted WLAN the network may select the same or different PDN GWs for the PDN connections when PDN connections to this APN are activated via 3GPP access network and Trusted WLAN in the same time. If the same PDN GW is selected then the APN-AMBR is enforced for the PDN connections. If different PDN GWs are selected then the APN-AMBR is enforced separately in the PDN GWs for the PDN connections, i.e. the UE will receive double amount of bandwidth for the APN. Therefore it is recommended that the default APN for Trusted WLAN access be different from any APN that the UE may use on the 3GPP side.

  - The UE and the EPC are mutually authenticated through the WLAN Access as defined in TS 23.402 [3] clause 4.9.1.
  - IEEE 802.1X as defined by IEEE 802.11 [5] is used over the WLAN air link to carry EAP.
  - After EAP authentication, UE traffic over the WLAN air link may be confidentiality and integrity protected as defined by IEEE 802.11 [5].
  - The TNAN may indicate to the AAA server via STa whether it supports S2a, non-seamless offload or both. The HSS/AAA may indicate via STa whether access to EPC via S2a is or is not allowed for this subscriber. The HSS/AAA decision to allow EPC access or not could be based on information elements such as subscriber profile, access network, SSID selected.

- At step3, For IPv4 address configuration, the use of DHCPv4 as in IETF RFC 5844 [18] is the L3 attach trigger.
- At step 3, For IPv6 address configuration, the use of RS as in IETF RFC 5213 [17] or LL-DAD NS is the L3 attach trigger. The TNSP does not send RAs until an L3 attach trigger is received.

NOTE 3: It is assumed that, to identify the UE, the L3 triggers are transported in an L2 frame that contains the UE L2 address (MAC address).

- The TNAN determines based on HSS/AAA indication or pre-configured information whether or not to establish S2a.
- If the TNAN determined that S2a shall not be used steps 5-9 are skipped. Instead, the TNAN assigns an IPv4 address and/or IPv6 prefix to the UE (depending on the trigger received in step 3) and offloads the traffic.
- At step 5, when TNSP receives L3 attach trigger message, the TNSP selects default APN according the subscription data received in step 2. If the L3 attach trigger is of an IP version not supported by the subscription PDN Type, the TNSP does not send Create Session Request. Otherwise, the TNSP sends a Create Session Request with the PDN Type of the subscription data:
  - If the L3 attach trigger is IPv4 and step 2 indicates that PDN type IPv4v6 is supported for the default APN, then PDN type in the Create Session Request is set to IPv4v6. If the UE also performs an IPv6 L3 attach trigger, then the TNSP will correlate both requests to the same PDN connection.
  - If the L3 attach trigger is IPv6, and step 2 indicates that PDN type IPv4v6 is supported for the default APN, then PDN type in the Create Session Request is set to IPv4v6. If the UE also performs an IPv4 L3 attach trigger, then the TNSP will correlate both requests to the same PDN connection.
  - If the L3 attach trigger is IPv4, and step 2 indicates that PDN type is IPv4-only, then PDN type in the Create Session Request is set to IPv4.
  - If the L3 attach trigger is IPv6, and step 2 indicates that PDN type is IPv6-only, then PDN type in the Create Session Request is set to IPv6.
- At step 8, PDN GW sends Create Session Response to the TNSP.
- At step 11, for IPv4, a DHCPv4 message with allocated IPv4 address is sent. For IPv6, the TNSP starts sending RAs with the allocated prefix and sets "autonomous address configuration" flag and "O" flag (IETF RFC 4861 [11]).

NOTE 4: A UE might request to get some IP configuration parameters (e.g. DNS server) by means of DHCP. These parameters sent by TNSP(acting as a DHCP server) to the UE in a DHCP reply. These parameters are retrieved by the TNSP(acting as a DHCP client) from the PGW by means of DHCP.

7.1.1.3 Without-UE-impact procedures except Initial Attach

Based on the GTP-S2a procedures in clause 6, for the solution without UE impact the following procedures are considered:

- Detach and PDN Disconnection with GTP on S2a:
  - Trusted WLAN AN and HSS/AAA may disconnect the PDN Connection and detach the UE, and the PDN GW may initiate Resource Allocation Deactivation for the default bearer as the PDN disconnection. If there is no traffic received from the UE for a configurable duration and the WLAN AN detects the UE has left based on unanswered probes (e.g. ARP Request, Neighbour Solicitation message), it disconnects the PDN Connection. In these cases the UE IP address(es) are released in the network. When disconnecting the PDN Connection, the TNAN needs to locally remove the UE context and de-authenticate and disconnect the UE at Layer 2 according to IEEE Std. 802.11-2007 [5]. When UE connects to the network next time, the L2 disconnection serves as an indication to the UE that the previous IPv4 address/IPv6 prefix might no longer be valid. The UE can then proceed with re-validation or re-acquisition of its IPv4 address / IPv6 prefix.
  - The UE can send an explicit DHCPv4 message to release the IPv4 address, then the PDN connection is disconnected when the PDN type is IPv4.
- PDN GW Initiated Bearer Modification and HSS Initiated Subscribed QoS Modification procedures may be used to modify the default and dedicated bearer but correspond to no signalling over Trusted WLAN's airlink.
- The dedicated bearer activation procedure may be used to activate the dedicate bearer in S2a but correspond to no signalling over Trusted WLAN's airlink.

In addition, the following procedures in clause 6 are not supported:

- UE-initiated Connectivity to Additional PDN connection.
- The handover between Trusted WLAN and 3GPP Access with IP address preservation.

7.1.1.4 SaMOG deployment

WLAN networks may be deployed such that separate SSIDs are used for EPC-routed and non-seamless WLAN offload, e.g. SSID_EPC and SSID_NSO.

WLAN networks may also be deployed such that the same SSID in a WLAN Access Point provides different type of network access to different users attached to this Access Point. For example, SSIDx may provide EPC-routed access for subscriber A, but non-seamless WLAN offload for subscriber B. In such a deployment it would be up to the operator to provide network configuration that supports different user access preferences, subscriptions and UE configurations.

It is recommended that the UE can be configured to apply different behaviour when connected to different SSIDs, e.g. allow or prevent the usage of certain applications on specific SSIDs. For example, for the SSIDs used for SaMOG the UE can be configured to disable applications that require local connectivity (e.g. DLNA applications) and enable applications that require EPC connectivity to the default APN used for SaMOG. Such kind of special behaviour for SSIDs used for SaMOG can improve the user experience and prolong the UE battery life.

NOTE: An unmodified UE can be configured to apply different behaviour when connected to different SSIDs by means which are outside the scope of this document. For example, the UE can be configured over-the-air, by means of a downloadable application, or by means of manual configuration.

7.1.1.5 PMIP based S2a considerations

The solution described above can also work when PMIP is used over S2a with the following considerations:

- To support PMIP, the TNSP shall implement the MAG function as it is specified in TS 23.402 [3], clause 6 for S2a. Instead of GTP messages the relevant PMIP messages are used as it is specified in TS 23.402 [3], clause 6 for S2a.
- The considerations described on APN and PDN type selection in clause 7.1.1.2 are also valid when PMIP based S2a is used.

- The link model, IPv4 address and IPv6 prefix allocation considerations of the clauses describing the solution with GTP S2a (e.g. TNSP is the first hop router and DHCPv4 server shall be located in the TNSP) are also valid when PMIP based S2a is used.

7.1.2 Solution 2

7.1.2.0 General

This solution is based on the S2a bearer creation and deletion between a Trusted Non-3GPP WLAN Access and the 3GPP Home Network be driven by the AAA signalling between these two. A key difference to the solution described in clause 7.1.1 is that this solution uses EAP and AAA signalling to trigger establishment of the S2a session, while the solution in clause 7.1.1 uses L3 messages to trigger the S2a session. The interfaces towards EPC (STa and S2a) do not differ between the solutions.

NOTE: Although the solution is described for a GTP-based S2a, it would equally apply to a PMIP-based system were the GTP signalling be replaced by the corresponding PMIP signalling (i.e. Create Session Request replaced by Proxy Binding Update, and Create Session Reply replaced by Proxy Binding Acknowledgement, as well as the corresponding BBERF procedures between Trusted WLAN Access Gateway and PCRF).

7.1.2.1 Reference Model

NOTE: The shaded area in Figures 7.1.2.1-1, 7.1.2.1-2, and 7.1.2.1-3 refers to Trusted Non-3GPP WLAN Access functionality.

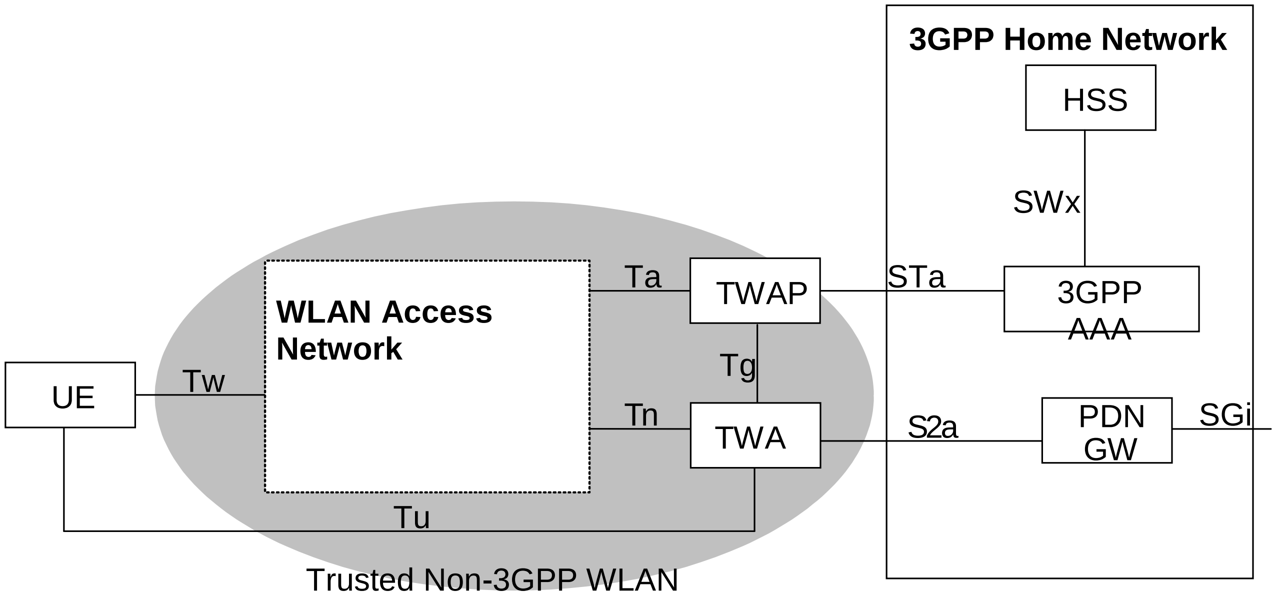


Figure 7.1.2.1-1: Non-roaming reference model

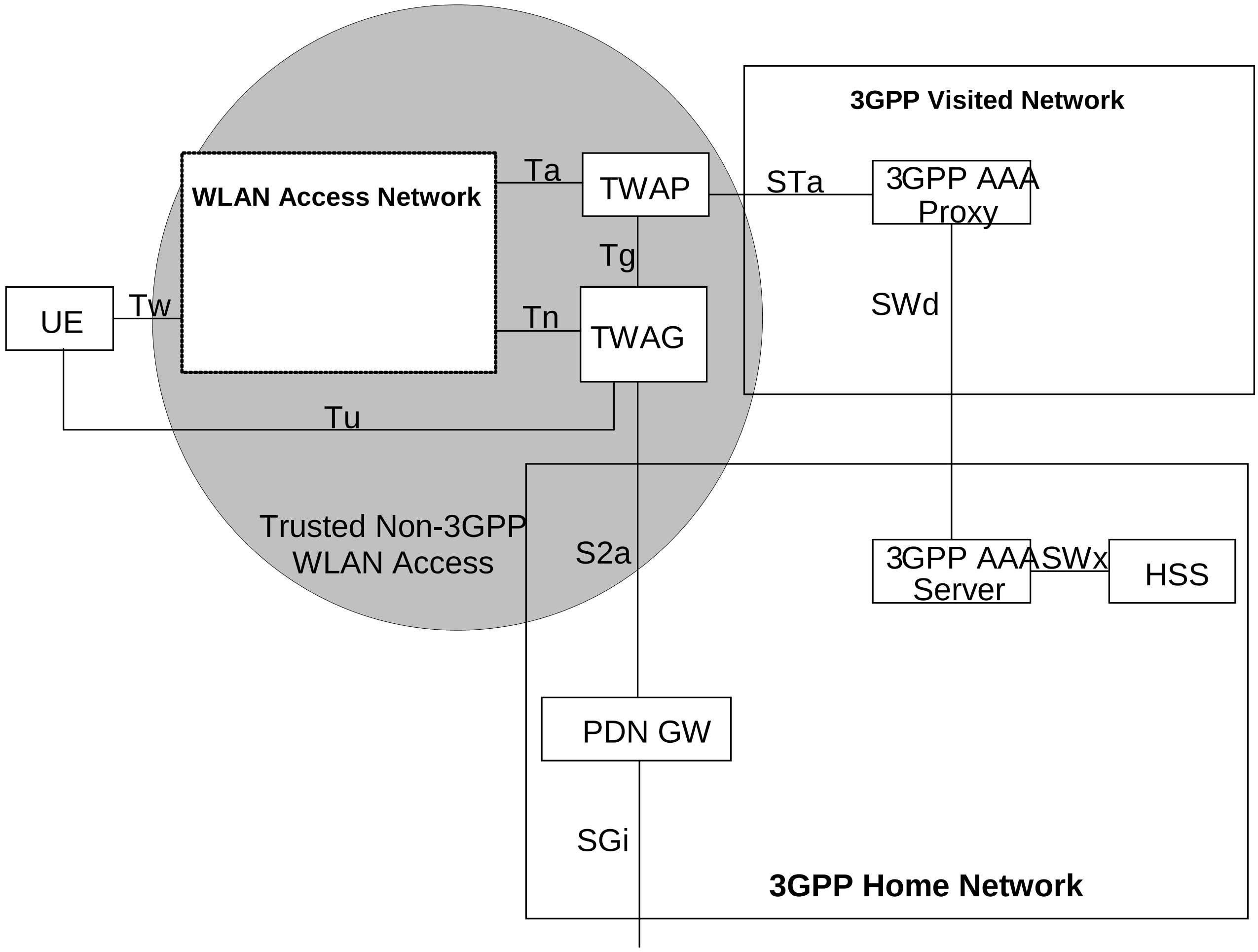


Figure 7.1.2.1-2: Roaming reference model Trusted Non-3GPP WLAN Access - Home Routed

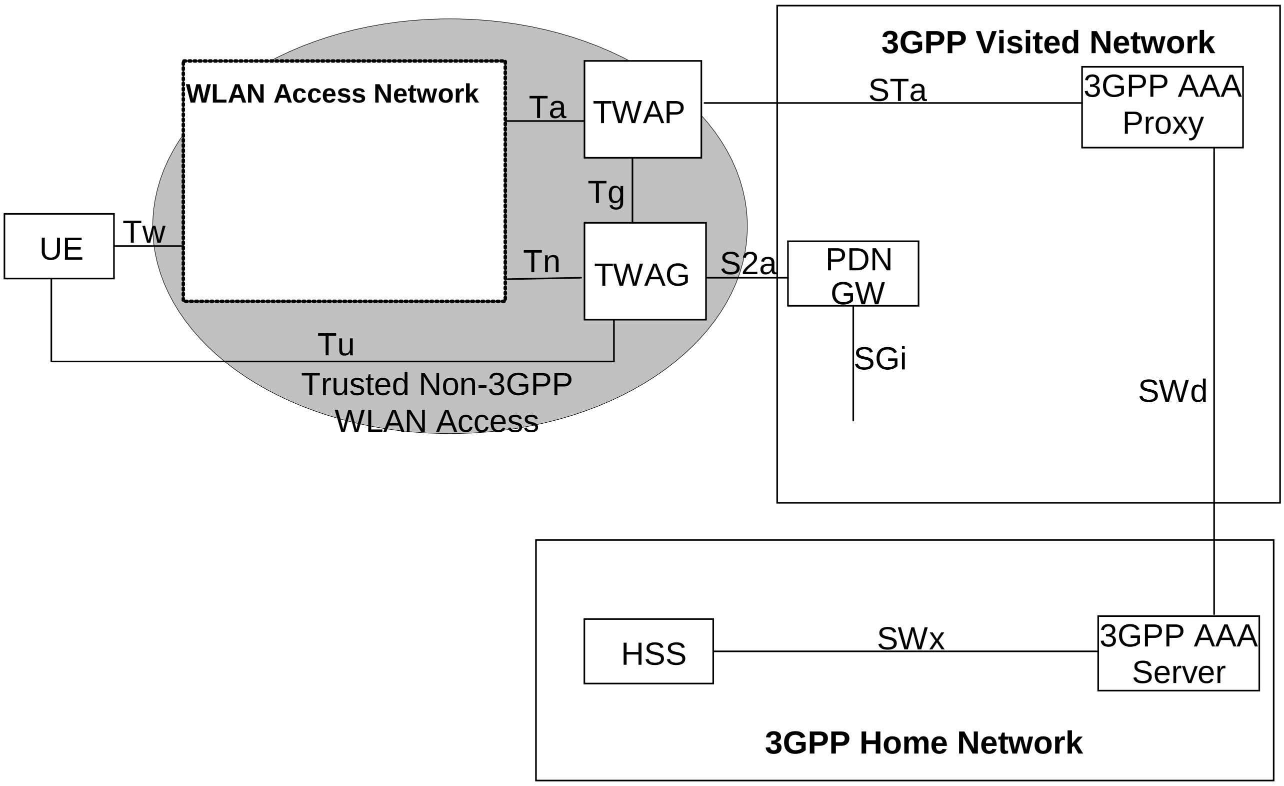


Figure 7.1.2.1-3: Roaming reference model Trusted Non-3GPP WLAN Access - Local Break-Out

7.1.2.2 Network elements

7.1.2.2.1 UE

For the purpose of accessing a Trusted Non-3GPP WLAN Access the UE is assumed to be unmodified and has the following standard functions:

- WLAN Access Network authentication based on EAP methods.
- Configure an IP address on the WLAN using the relevant IETF standards, depending on the specific WLAN deployment:
  - For IP version 4: DHCP as per IETF RFC 2131. Optionally, Detecting Network Attachment in IPv4 (DNAv4) according to IETF RFC 4436.
  - For IP version 6: Stateless Address Autoconfiguration (SLAAC) as per IETF RFC 4861 [11], and optionally stateless DHCPv6 as per IETF RFC 3736 [19]. Optionally, Detecting Network Attachment in IPv6 (DNAv6) according to IETF RFC 6059 [14].

7.1.2.2.2 Trusted WLAN AAA Proxy

The Trusted WLAN AAA Proxy (TWAP) function includes:

- Relaying the AAA information between the WLAN Access Network and the 3GPP AAA Server or Proxy in case of roaming.
- Establishing Binding of UE IMSI with UE MAC address on the WLAN Access Network into (IMSI, MAC) tuple via snooping on the AAA protocol carrying EAP-AKA exchange.
- Detecting L2 Attach of UE to the WLAN Access Network via snooping on the AAA protocol for EAP-Success message.
- Detecting L2 Detach of UE from the WLAN Access Network via snooping on the AAA protocol for Accounting-Request STOP message.
- Informing the Trusted WLAN Access Gateway of WLAN Attach and Detach events for UE with (MAC, IMSI) tuple.
- Protocol conversion when the Ta and STa reference points do not use the same protocol (e.g. Ta based on RADIUS).
- Transfer necessary information for suitable per-UE L2 encapsulation (e.g. 802.1Q VLAN tag or MPLS label) between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway.

The Trusted WLAN AAA Proxy functionality can reside in a separate physical network node, it may reside in the Trusted WLAN Access Gateway or any other physical network node.

7.1.2.2.3 Trusted WLAN Access Gateway

The Trusted WLAN Access Gateway function includes:

- For IP version 4:
  - Default IPv4 Router.
  - DHCP server according to IETF RFC 2131 [9]. The TWAG allocates to the UE the IPv4 address that is allocated to the UE by the PDN GW.
- For IP version 6:
  - Default IPv6 Router according to IETF RFC 4861 [11].
- Enforces routing of packets between the UE MAC address and the GTP tunnel for that UE.

- Enforce per-UE L2 encapsulation of traffic to/from the UE. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

NOTE 1: There is a per-UE subnet point-to-point link and subnet between the UE and the Trusted WLAN Access Gateway that acts as the default router. This link model is the same as the one used for PMIP-based S5/S8 and differs from that of GTP-based S5/S8.

NOTE 2: Whether multiple TNAN functions are mapped to a single non-3GPP access entity, or a single TNAN function is distributed among multiple non-3GPP access entities is out-of-scope of 3GPP.

7.1.2.3 Reference Points

7.1.2.3.1 Ta reference point

The Ta reference point applies to Trusted Non-3GPP WLAN Access.

The Ta reference point connects the WLAN Access Network to the Trusted WLAN AAA Proxy. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and accounting related information. The reference point has to accommodate also legacy WLAN Access Networks.

EAP authentication shall be transported over the Ta reference point.

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between UE and 3GPP Network; As a side effect, allowing the Trusted WLAN AAA Proxy to detect L2 attach of the UE.

- Carrying data for authorization (including the authorization information update) signalling between WLAN Access Network and 3GPP Network.

- Carrying accounting signalling per WLAN user, e.g. for charging purposes; As a side effect, allowing the Trusted WLAN AAA Proxy to detect L2 detach of the UE.

- Carrying keying data for the purpose of radio interface integrity protection and encryption;

- Informs WLAN Access Network of per-UE L2 encapsulation information to be used with the Trusted WLAN Access Gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

- Purging a user from the WLAN Access Network for immediate service termination.

7.1.2.3.2 Tg reference point

The Tg reference point applies to Trusted Non-3GPP WLAN Access.

The Tg reference point connects the Trusted WLAN AAA Proxy to the Trusted WLAN Access Gateway. This is a AAA interface used to:

- Trusted WLAN AAA Proxy notify Trusted WLAN Access Gateway of WLAN attach and detach events.

- Trusted WLAN Access Gateway Informs Trusted WLAN AAA Proxy of per-UE L2 encapsulation information to be used between the WLAN Access Network and the Trusted WLAN Access Gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

7.1.2.3.3 Tn reference point

The Tn reference point applies to Trusted Non-3GPP WLAN Access.

The Tn reference point connects the WLAN Access Network and the Trusted WLAN Access Gateway and provides the following functionality:

- Per-UE encapsulation between the WLAN Access Network and the Trusted WLAN Access Gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

7.1.2.3.4 Tw reference point

The Tw reference point applies to Trusted Non-3GPP WLAN Access.

The Tw reference point connects the UE to the WLAN Access Network per IEEE 802.11 [5] specifications. The definition of IEEE Physical and Medium Access Control layers protocols (e.g. Layer 1 and Layer 2 defined by IEEE 802.11 [5] standards) is out of the scope of 3GPP.

The functionality of the reference point is based on IEEE 802.11 [5] specifications and it is intended to transport signalling messages including:

- Attach and Detach request from the UE to the WLAN Access Network.

- Detach signal from the WLAN Access Network to the UE.

- Parameters for authentication signalling between the 3GPP AAA Server and the UE;

- Per-UE encapsulation of data frames between the UE and the WLAN Access Network as per IEEE 802.11 [5] specifications.

7.1.2.3.5 Tu reference point

The Tu reference point applies to Trusted Non-3GPP WLAN Access.

The Tu reference point represents the point-to-point link and per-UE subnet between the UE and the Trusted WLAN Access Gateway. Transport for the Tu reference point is provided by a combination of:

- The Tw reference point provides an IEEE 802.11 association between the UE and a BSSID/ESSID in the WLAN Access Network, as per IEEE 802.11 specifications.

- The WLAN Access Network internally provides per-UE encapsulation between the BSSID/ESSID and the Tn endpoint. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

- The Tn reference point provides per-UE encapsulation between the WLAN Access Network and the Trusted WLAN Access Gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [16], 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway via the Trusted WLAN AAA Proxy are dependent on the specifics of the WLAN Access Network Deployment and out-of-scope for 3GPP.

7.1.2.4 Procedures

For the steps that already exist in the generic Trusted Non-3GPP Access procedure and are re-used in the Trusted Non-3GPP WLAN Access procedure, identical numbering is used, and the differences are outlined, if any. For the steps that are specific to the Trusted Non-3GPP WLAN Access procedure and do not exist in the generic Trusted Non-3GPP WLAN Access procedure, the steps are indexed with the number of the generic preceding step and a letter, and a description of the step is provided.

7.1.2.4.1 Initial Attach to Trusted Non-3GPP WLAN Access procedure

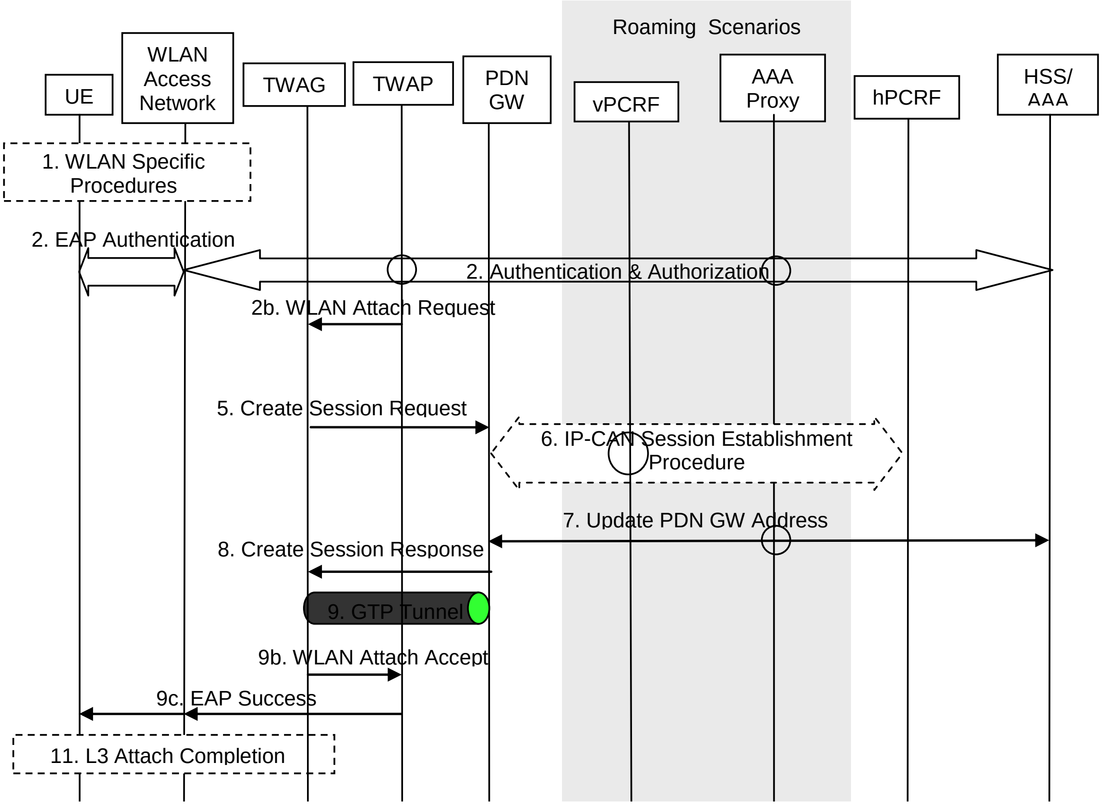


Figure 7.1.2.4.1-1: Initial attach to Trusted Non-3GPP WLAN Access

The procedure for Initial Attach to Trusted Non-3GPP WLAN Access is represented in Figure 7.1.2.4.1-1 and described below. It is based on the generic Initial Attach to Trusted Non-3GPP Access procedure described in clause 6.1.3.1. with the following differences:

- At step 2, the following additions apply:
  - The HSS/AAA provides to the Trusted Non-3GPP WLAN Access the APN to which the UE will be attached. in the subscription data. PDN type is indicated from HSS in this step.
  - The mutual authentication between the UE and the EPC as defined in TS 23.402 [3], clause 4.9.1 is carried according to IEEE 802.11 [5] specifications through the Trusted Non-3GPP WLAN Access.
  - At reception of the EAP Success, the Trusted WLAN AAA Proxy buffers it and notifies the Trusted WLAN Access Gateway of the layer 2 attach of the UE and provides MAC address and IMSI of the UE as depicted in step 2b.
- At step 5, after the Trusted WLAN AAA Proxy informs of layer 2 attach of the UE, the Trusted WLAN Access Gateway selects the APN as per the subscription data received in step 2 and send Create Session Request to the PDN GW with the PDN type.
- At step 8, After allocating an IPv6 prefix and/or an IPv4 address to the UE, the PDN GW sends Create Session Response to the Trusted WLAN Access Gateway. Deferred IPv4 address allocation may be used.
- At step 9b, the Trusted WLAN Access Gateway notifies the Trusted Non-3GPP Access AAA Proxy of successful GTP tunnel establishment, and provides the necessary parameters for establishment of a point-to-point link towards the UE through the WLAN Access Network.
- At step 9c, the Trusted WLAN AAA Proxy delivers the buffered EAP success to the WLAN Access Network together with the necessary parameters for establishment of a point-to-point link between the UE and the Trusted WLAN Access Gateway. On receiving this, the WLAN Access Network configures the point-to-point link adequately and informs the UE of EAP success.

- At step 11, after the UE is associated and authenticated with the WLAN Access Network, the UE performs IP layer configuration with the Trusted WLAN Access Gateway acting as the default router according to standard IETF procedures [9] [12] [13] [14] [19].

NOTE: The WLAN Access Gateway can send unsolicited IP layer configuration signalling, e.g. DHCPv4 or RA, over the point-to-point link towards the UE.

7.1.2.4.2 UE/Trusted Non-3GPP WLAN Access Network Initiated Detach procedure

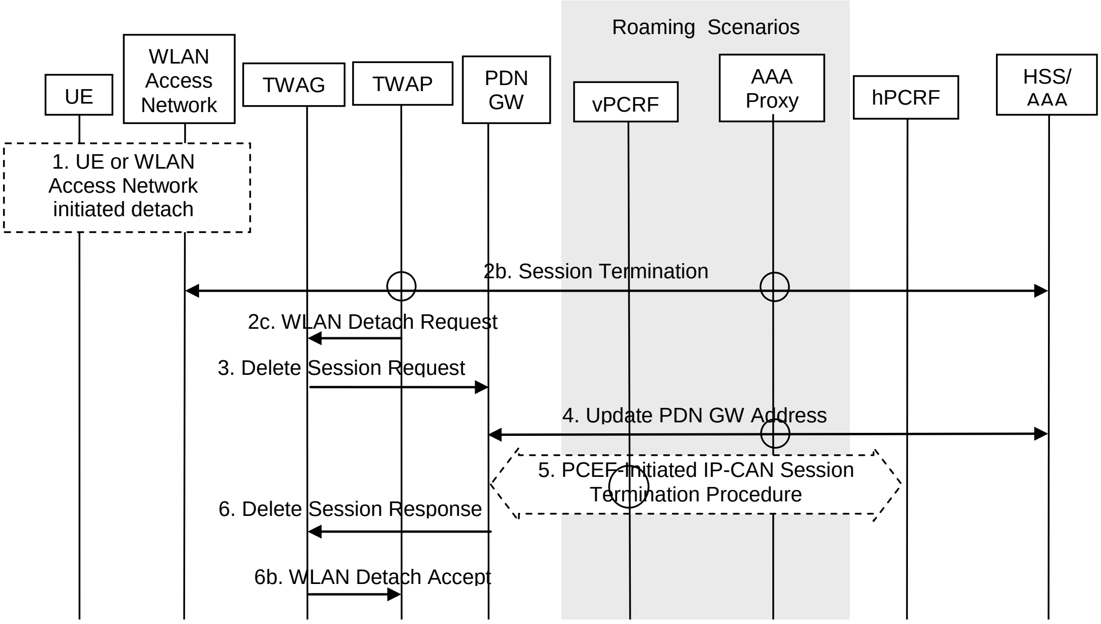


Figure 7.1.2.4.2-1: UE/Trusted Non-3GPP WLAN Access Network Initiated Detach

The procedure for UE/Trusted Non-3GPP WLAN Access Network Initiated Detach is represented in Figure 7.1.2.4.2-1 and described below. It is based on the generic UE/Trusted Non-3GPP IP Access Network Initiated Detach procedure described in clause 6.1.3.2.1. with the following differences:

- At step 2, the following additions apply:
  - In step 2b, the UE/Trusted Non-3GPP WLAN Access Network Initiated Detach triggers AAA signalling between the WLAN Access Network and the home HSS/AAA server to terminate the session.
  - Based on the AAA signalling for session termination, the Trusted WLAN AAA Proxy sends a WLAN Detach Request to the Trusted WLAN Access Gateway.
- Step 3 is initiated by the Trusted WLAN Access Gateway based on the WLAN Detach Request received from the Trusted WLAN AAA Proxy.
- At step 6, the following addition applies:
  - In step 6b, the Trusted WLAN Access Gateway confirms session deletion by sending to the Trusted WLAN AAA Proxy a WLAN detach accept.

7.1.2.4.3 HSS/AAA Initiated Detach procedure

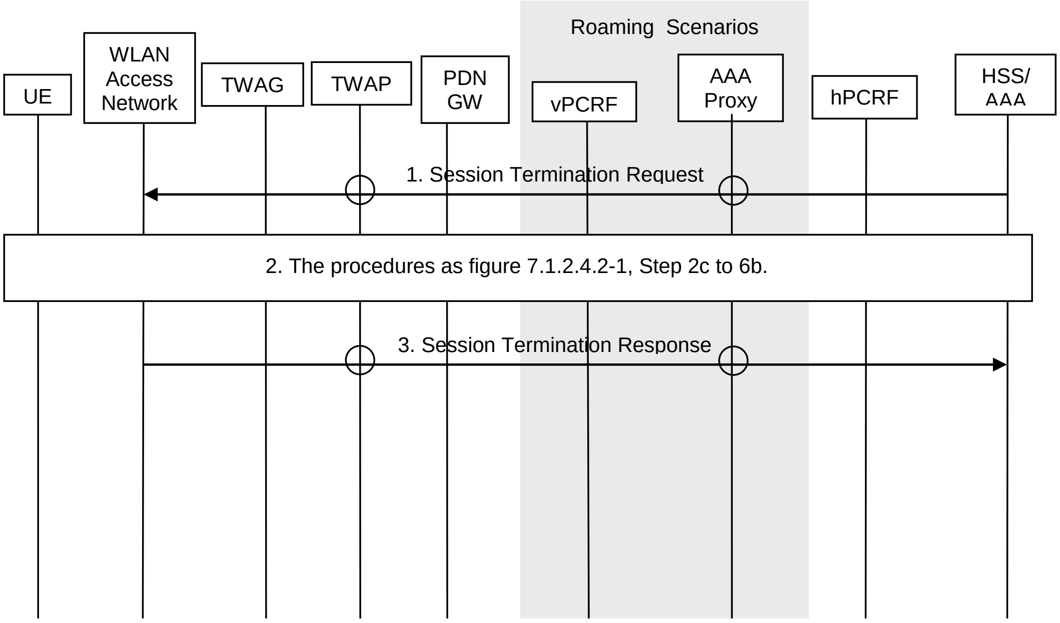

Roaming Scenarios
UE
WLAN Access Network
TWAG
TWAP
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as figure 7.1.2.4.2-1, Step 2c to 6b.
3. Session Termination Response

Figure 7.1.2.4.3-1: HSS/AAA Initiated Detach

The procedure for HSS/AAA Initiated Detach from Trusted Non-3GPP WLAN Access Network is represented in Figure 7.1.2.4.3-1 and described below. As for the UE/Trusted Non-3GPP WLAN Access Network Initiated Detach, it is based on the generic HSS/AAA Initiated Detach procedure described in clause 6.1.3.2.2 with the following differences:

- At step 2, the step 2c to 6b of the UE/Trusted Non-3GPP WLAN Access Network Initiated Detach procedure described in clause 7.1.2.4.2 are followed.

7.1.2.4.4 Other procedures

Other procedures defined for the generic Trusted Non-3GPP IP Access refer to clause 7.1.1.3 descriptions.

7.1.3 Handovers with or without TNSP/TWAG relocation with unmodified UEs

No specific mechanisms are defined to support AP-to-AP handover with and without TNSP/TWAG relocation. However, this does not preclude the support of IP address preservation in handovers without TNSP/TWAG relocation when supported by procedures out of 3GPP scope.

8 Additional considerations for WLAN access to EPC through S2a for Phase 2

Editor's note: Phase 2 of the study is aiming at studying enhancements to the Rel-11 solution to avoid those limitations (except emergency attach). In this phase it is expected that there will be some impacts to the UE.

8.1 Requirements

Editor's note: This clause will contain the requirement(s) related to SaMOG Phase 2 study.

The solutions shall comply with the following Requirements:

- The SaMOG phase 2 solution (e.g. possibly with impact to the UE) shall be able to co-exist with the SaMOG Release 11 solution.

The solutions shall comply with one or more of the following requirements:

- For a UE, multiple simultaneous PDN connections over Trusted WLAN are supported, including the support for establishment of concurrent PDN Connections via 3GPP access and over WLAN.
- For a UE, PDN Connectivity to EPC over Trusted WLAN concurrent with non-seamless WLAN offload is supported.
- The UE is capable of IP address preservation in case of mobility between a 3GPP access and a Trusted WLAN. The UE is capable to request IP address preservation per PDN connection in case of mobility between a 3GPP access and a Trusted WLAN.
- The UE is capable of signalling the requested APN over Trusted WLAN, and the UE is capable of receiving the selected APN over Trusted WLAN (e.g. in case the UE did not indicate an APN).
- The UE is capable of indicating whether it requests a PDN connection or a NSWO connectivity service over Trusted WLAN, and the UE is capable of receiving an indication of whether the granted service is a PDN connection or NSWO connectivity (e.g. in case the UE did not indicate the kind of service it was requesting). A solution may also enable NSWO connectivity establishment only as the first connection. It is not required to release the NSWO connection without releasing the other connections.
- The solution should minimize the UE functional changes.

8.1A Key issues

- Regarding the feature of handover with IP address preservation. S2a already supports the hand-over indication that can be used by the TWAG to tell the PGW that the IP address is to be preserved. A solution is needed to enable the UE to provide to the TWAN an indication of whether the access to the TWAN corresponds to a "handover" (with IP address preservation) or "initial attach".
- Regarding the feature of connecting to a non-default APN. Also here, S2a already supports this. The TWAN will also get all relevant APN profile information for this UE from the 3GPP AAA/HSS as part of the STa authentication and authorization process. A solution is needed to enable the UE to explicitly indicate which APN to connect to, and for the UE to be informed about the APN that the TWAN connected the UE to.
- Regarding the feature of the UE choosing between access to EPC and NSWO. Also here, the TWAN will also get all relevant APN profile information for this UE from the 3GPP AAA/HSS as part of the STa authentication and authorization process. A solution is needed for enabling the UE to indicate to the network whether an IP session is requested for EPC access or for non-seamless WLAN offload, and the network to respond whether the access request has been granted.
- Regarding the feature of the UE requesting a connection to an additional PDN. Also here, a solution is needed for the UE to request an additional PDN connection. Besides this, additional logic may be needed to correlate an individual user plane IP packet to an individual PDN connection. The solution shall take into account all situations and in particular when:

  1) Two or more PDN connections from one UE might have the same IP address. This is in particular possible if these PDN connections are towards different PDN(s) using IPv4 private addressing.

  2) Downlink (link layer) broadcasts do not include a specific UE target IP address (associated with a PDN connection).

  3) Downlink IP multicast does not include a specific UE target IP address, and the sources of multicast services would have also the same IPv4 private address.

  The UE, the TWAG and/or the link between them, may need to implement means to cope with these situations.

- Regarding the support for the same UE of simultaneous access to EPC through S2a and of non-seamless offload, similar considerations than for the support of simultaneous PDN connections apply.

8.2 Solutions

Editor's Note: This clause will describe the solution(s) for SaMOG Phase 2 study.

8.2.1 Solution 1: Tunnelled approach with dedicated UE-TWAG control protocol

8.2.1.1 Functional Description

Editor's Note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.1.1.1 Overview

This solution uses a two-scenario approach to support handover, non-default APN and multiple PDN connections:

1. Single-connection scenario: In this scenario, the network or the UE only supports a single IP connection over WLAN. An IP connection is either a PDN connection or a NSWO connection. EAP signalling between UE and network is enhanced to carry attach parameters (e.g. handover indicator or APN or a request for NSWO).

2. Multi-connection scenario: In this scenario, the network and the UE both support multiple connections over WLAN. In the multi-connection scenario, a signalling protocol to manage PDN connections is needed. Also, a user-plane separation mechanism is needed to separate user-plane traffic between the different active PDN connections. A NSWO IP address or prefix is obtained through standard IETF procedures (i.e. DHCP or IPv6 Stateless Address Auto-configuration).

Negotiation of which scenario to choose is done once as part of the attachment EAP signalling between UE and network.

8.2.1.1.2 User plane

In the single-connection scenario, the PDN connection over WLAN uses the per-UE point-to-point link as defined in TS 23.402 [3] clause 16. Such point-to-point link carries MAC frames. The MAC frame would typically carry an IP packet. IP is indicated by means of the "EtherType" field in the MAC header as defined in IEEE 802.1 (e.g. IPv4 is indicated by the Ethertype 0x0800).

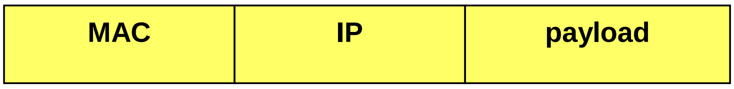


Figure 8.2.1.1.2-1: Frame format for the single-connection scenario

For the multi-connection scenario, there is at most one NSWO connection. For all PDN connections over WLAN, an additional layer between MAC and IP is used when carrying IP packets belonging to these connections. The MAC "Ethertype" field would in this case instead indicate "XYZ", where "XYZ" is an identifier for the protocol that is used to include: 1) A key to differentiate the PDN connections from each other; 2) A next header indicator, which will be typically IP. The key is unique within the scope of a single UE. The key combined with the MAC address of the UE provides a globally unique identification for a PDN connection. The TWAG and the UE can use this identification to correlate a packet to the correct PDN connection. In the following two clauses, two alternatives are proposed for "XYZ".

Editor's Notes: One of these two alternatives needs to be chosen. Which one is still FFS.

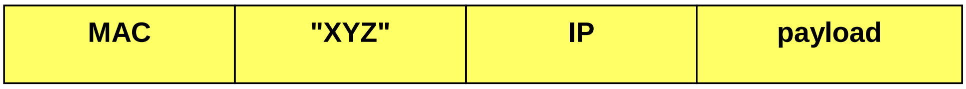


Figure 8.2.1.1.2-2: Frame format for PDN connections in the multi-connection scenario

8.2.1.1.2.1 Alternative 1: XYZ = GRE

In this alternative, XYZ is the GRE header as defined in IETF RFC 2890. The GRE key is used to differentiate the PDN connections from each other. This requires that GRE is defined by IEEE as new EtherType.

As the access point is functioning like a layer-2 bridge, it forwards frames between its WiFi interface and its wired interface without checking the EtherType value. If the access point implements a mapping between IEEE 802.11e priorities and DSCP, then the DSCP will be found on a different offset for frames with EtherType GRE compared to frames with EtherType IPv4 or IPv6.

8.2.1.1.1.2.2 Alternative 2: XYZ = VLAN

In this alternative, XYZ is an extension of the MAC header, forming a VLAN-tagged MAC header. The VLAN ID is used as key to differentiate the PDN connections from each other.

The AP performs translation between the IEEE Std 802.11 air link and the IEEE 802 AP-TWAG segment e.g. using IEEE 802.11 integration service per IEEE 802.11-2007 appendix M. The solution relies on the VLAN ID to be carried un-modified to the TWAG.

The VLAN ID used to distinguish PDN connections is encapsulated over the air in LLC SNAP and thus cannot be used for any other (non-3GPP) service differentiation over the air.

As described in TS 23.402 [3] clause 16, the WLAN AN enforces upstream and downstream forced-forwarding between the UE's WLAN IEEE 802.11 association and the TWAG. The way this forced-forwarding is enforced ensures that the VLAN ID used to multiplex TWAN connectivity services is in a different protocol stack layer than VLAN ID potentially used on the transport interface between the UE and the TWAG.

The VLAN ID used to multiplex TWAN connectivity services is not used to route traffic on the path between the AP and the TWAG.

If the access point implements a mapping between IEEE 802.11e priorities and DSCP, then the DSCP will be found on a different offset for VLAN-tagged frames compared to frames without VLAN tagging.

An example of protocol stacks showing how UE MAC address and VLAN-ID can be transported between UE and TWAG are depicted in figure 8.2.1.1.1.2-1.

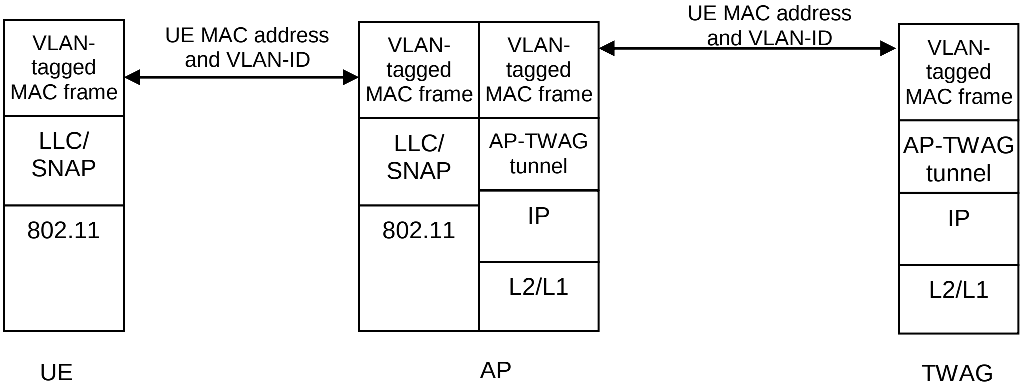


Figure 8.2.1.1.1.2.2-1: Example of UE-TWAG protocol stacks

This UE-TWAG protocol stacks example has following characteristics:

- **AP -TWAG tunnelling**

  The AP -TWAG tunnelling, as used by SAMOG phase 1 / Rel11 deployments, is assumed to be on top of IP layer in order to allow the AP to reach a TWAG that may be located beyond the access line IP Edge (BNG). This allows layer 2 headers exchanged between UE and TWAG above that tunnel (e.g. VLAN Id used on the UE-TWAG interface) to be independent from layer 2 headers (e.g. VLAN Id) which may already exist on the path between AP and IP Edge / TWAG, thus avoiding interferences with VLAN-ID used in current deployments between UE and IP Edge.

NOTE 1: Definition of the tunnel between AP and TWAG is out of 3GPP scope. There may be e.g. one AP-TWAG tunnel per AP, or an AP-TWAG tunnel per PDN connection (in which case it should be dynamic i.e. established by signalling).

- **VLAN-ID as used between UE and TWAG for SAMOG phase 2 multiplexing**

  VLAN-ID as used between the UE and the TWAG for SAMOG phase 2 multiplexing is carried on the radio path in the VLAN tagged MAC frame on top of 802.11/LLC/SNAP. This VLAN-ID can be transported via the user plane in the (VLAN tagged) frame carried by (above) the AP -TWAG tunnel as shown in the figure (e.g. in case of a AP -TWAG tunnel defined per AP).

NOTE 2: In the case of an AP -TWAG tunnel per PDN connection, this VLAN-ID could also be carried via the control plane used to establish that tunnel.

- **UE MAC Address**

  UE MAC address is carried on the radio path in the relevant 802.11 address field. The UE MAC address can be transported via the user plane in the frame carried by (above) the AP -TWAG tunnel as shown in the figure (e.g. in case of a AP -TWAG tunnel defined per AP).

NOTE 3: In the case of an AP -TWAG tunnel per PDN connection, the UE MAC address could also be carried via the control plane used to establish that tunnel.

8.2.1.1.3 Control plane

8.2.1.1.3.1 EAP

EAP authentication signalling is extended in the UE to network direction in order to indicate:

- The support of single or multiple PDN connections capability.
- In case of single PDN connection scenario:
  - the requested connectivity (NSWO or PDN connection).
  - in case of PDN connection:
    - the connectivity type (v4, v6, or v4v6).
    - an optional hand-over indicator.
    - optionally the requested APN (mandatory if the handover indication is provided).
    - optionally, a PCO.
- In case of multiple PDN connection scenario:
  - Whether NSWO is requested or not.

EAP authentication signalling is extended in the network to UE direction in order to indicate:

- the selection of single or multiple PDN connections capability.
- In case of single PDN connection scenario:
  - Whether the requested connectivity (NSWO or a PDN connection) has been granted.
  - For PDN connection:
    - The Selected APN.
    - A PCO.
- In case of multiple PDN connection scenario:
  - Whether NSWO is allowed or not.

8.2.1.1.3.2 WLCP

A UE-TWAG protocol is needed to control (i.e. setup and teardown) the per-PDN point-to-point link. This protocol is denoted as WLCP (WLAN Control Protocol). WLCP is a protocol defined by 3GPP and is transported above the layer 2. WLCP is not an IP protocol and sits below the IP layer.

WLCP provides any foreseeable session management functionality required for PDN connections (based on the PDN connection management defined over the cellular link):

- Establishment of PDN connections
- Handover of PDN connections
- Request the release of a PDN connections by the UE or notify the UE of the release of a PDN connection
- IP address assignment (both IPv4 and IPv6 address assignment mechanisms defined for NAS can be applied, e.g. the delivery of the IPV4 address through WLCP, DHCPv4, and the use of SLAAC for IPv6)
- PDN parameters management
    - APN, PDN/PDP type, address, PCO, request type. Etc.
    - As described in clause 8.2.1.1.1, a User Plane Connection ID (GRE key or VLAN ID) value is needed to differentiate PDN connections. When establishing a new per-UE-and-PDN point-to-point link using WLCP, the network decides upon this User Plane Connection ID value and returns it to the UE using WLCP.

The WLCP may need to support functionality to verify the availability of the UE (i.e. if the UE is still connected to a WLAN AP) if existing mechanisms as described for Trusted WLAN Access in rel-11 would not to be sufficient.

WLCP applies to the support of multiple PDN connections and enables a UE behaviour similar to behaviour over cellular link. WLCP is a protocol running between the UE and the TWAG, thus the intermediate nodes (e.g. AP) between the UE and the TWAG do not need to support / understand WLCP.

The NAS SM defined in TS 24.008 is the starting point for the WLCP protocol design, and a subset of the SM functionality is used. Specifically:

- Only basic PDP Context Activation/Deactivation procedures are needed. No secondary PDP context procedure is considered. Activate PDP Context Request/Accept/Reject and Deactivate PDP Context Request/Accept are used.
- Some parameters not needed (e.g. QoS, etc.) others possibly updated (e.g. protocol options), with stage 3 defining such details
- No eMBMS is considered
- No support of emergency PDN connection is considered in release 12
- LIPA functionality not required

Basing WLCP on TS 24.008 enables the separation of the attach procedure from the connectivity procedures, i.e. it allows the device to be attached without having an active PDN connection and does not require the device to initiate a detach after the device has disconnected all PDN connections.

NAS SM assumes the presence of a GMM state machine. For WLCP, no GMM is needed, and it is assumed that a successful EAP authentication and AP association brings the device in a state where WLCP can be used.

Any functionality, procedure (including network-initiated ones) and parameters defined for existing NAS in 24.008 or 24.301 can be re-used if determined needed later (e.g. low priority indication, QoS support, etc.).

NOTE 1: It is up to stage 3 to define aspects such as segmentation, retransmission, etc. since these have already been solved for existing NAS and CT1 has the expertise to address these aspects.

NOTE 2: Security considerations for WLCP are for SA3 to discuss, e.g. need for integrity protection, whether the underlying security resulting from a successful EAP authentication suffice, etc.

8.2.1.1.3.2.1 WLCP Transport

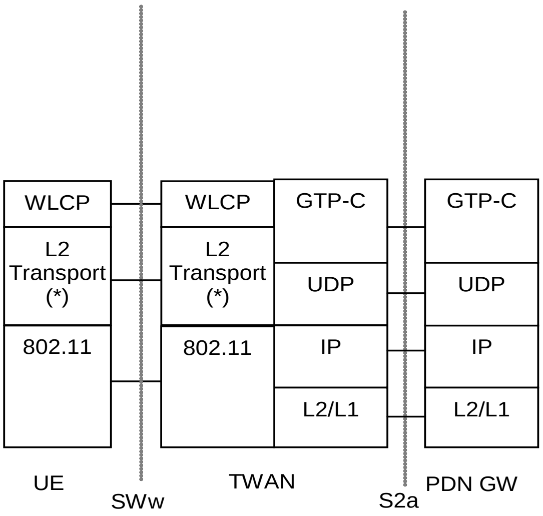
WLCP is transported above layer 2. A new EtherType indicating the control protocol needs to be defined by IEEE. The payload of such frame contains the control protocol message. Various solutions are possible for structuring the control protocol frame. As an example, the control signalling can use the same frame format as user plane signalling, i.e. with an intermediate GRE/VLAN header also for control signalling. Alternatively, this intermediate layer is omitted for control signalling. The detailed frame format can be left to stage 3 to decide.

When the UE does not yet know the TWAG MAC address, the UE uses MAC broadcast to reach the TWAG.

8.2.1.1.4 Protocol Stacks

Editor's note: Impact on link model due to handover support is FFS.

The figure below illustrates the control plane for WLCP.



Legend:
802.11: This refers to Layer 1 and Layer 2 defined by IEEE Std 802.11-2007 [5].
L2 Transport: This refers to the transport defined in 8.2.1.1.3.2.1.
WLCP: This refers to the protocol defined in 8.2.1.1.3.2.1
GTP-C: The GPRS Tunnelling Protocol control plane consists of signalling messages between the Trusted WLAN Access Gateway and the PDN- GW over the S2a interface. It is defined in TS 29.274 [25].
UDP: This is the transport layer protocol onto which both GTP-C and GTP-U are layered.

Figure 8.2.1.1.4-1: Protocol Stack for WLCP.

8.2.1.2 Procedures

8.2.1.2.1 Initial Attach in WLAN on S2a

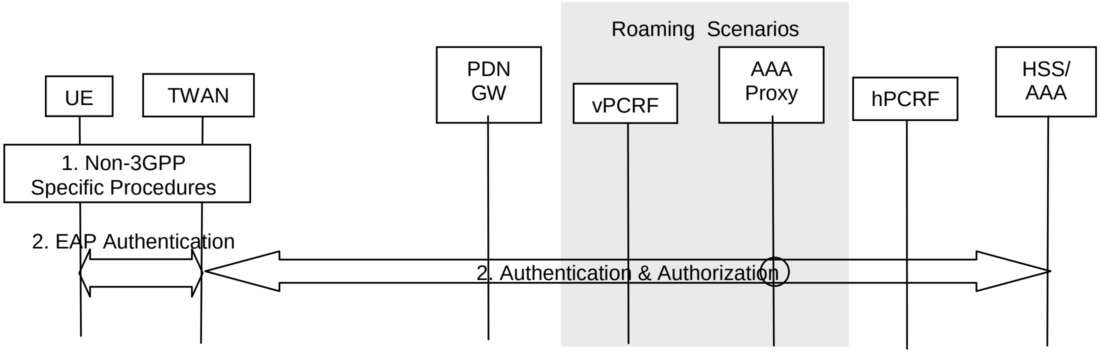


Figure 8.2.1.2.1.1-1: Initial attachment in WLAN on GTP S2a for roaming and non-roaming scenarios

The procedure is as TS 23.402 [3] clause 16.2.1 with the following additions:

- Step 2. As part of this step, the UE shall send an indication to the network whether it supports single-connection or multi-connection or both. If the UE supports the single-connection scenario, the UE also indicates whether it requests EPC access or non-seamless WLAN offload. If the UE requests EPC access, it may indicate APN.

  These indicators are sent in EAP-AKA to the 3GPP AAA. The 3GPP AAA sends these indicators to the TWAN. Depending on the capabilities of the network and the request of the UE, the network informs the UE as part of step 2 whether the single-connection scenario or the multi-connection scenario is selected. If UEs support both single-connection and multi-connection and the network supports the multiple-connection, then the network selects the multi-connection scenario.

  In case the single-connection scenario is selected, the procedure continues as described in clause 8.2.1.2.2. In case the multi-connection scenario is selected, the procedure continues as described in clause 8.2.1.2.3.

8.2.1.2.2 Initial Attach in single-connection scenario in WLAN on S2a (continuation)

8.2.1.2.2.1 Initial Attach in single-connection scenario in WLAN on GTP S2a (continuation)

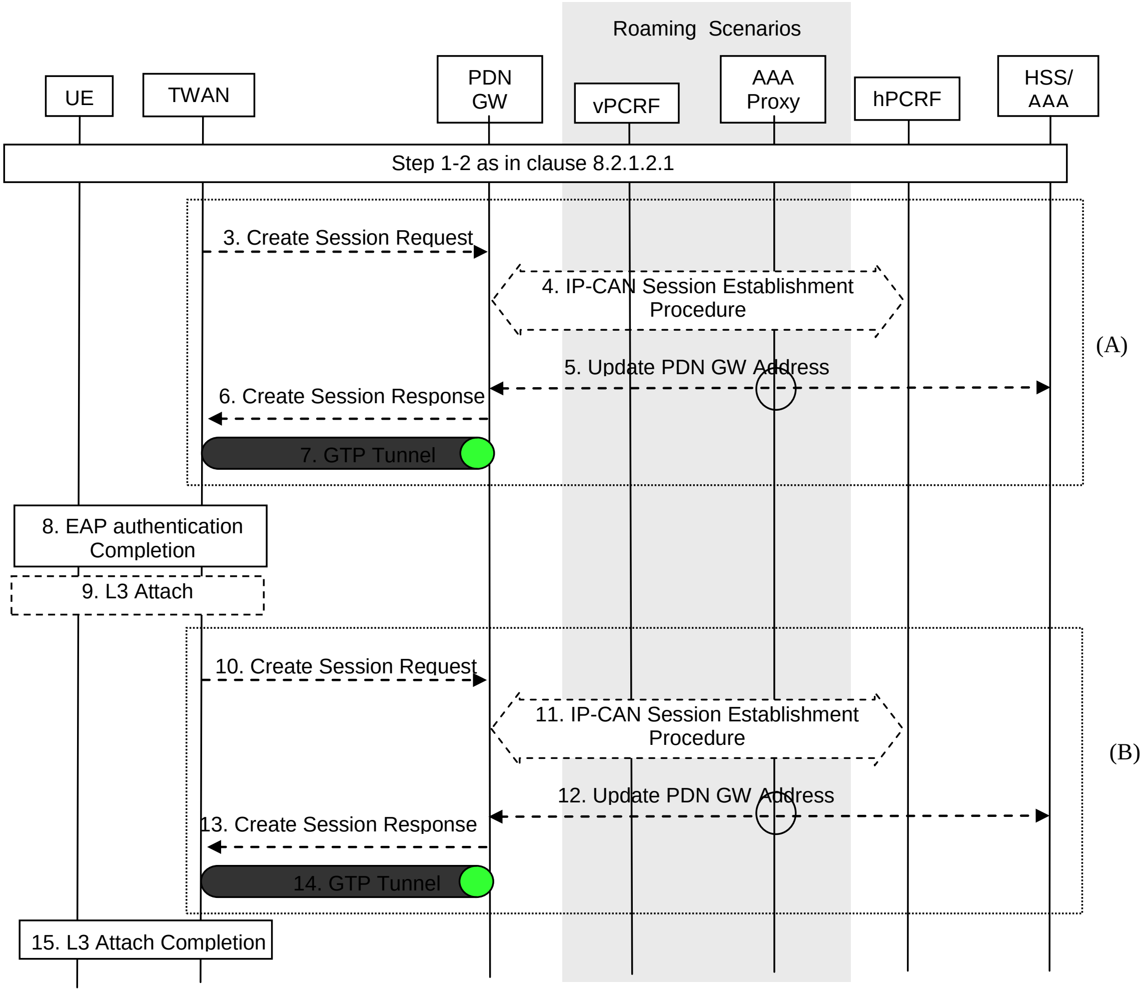

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Step 1-2 as in clause 8.2.1.2.1
3. Create Session Request
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Create Session Response
7. GTP Tunnel
(A)
8. EAP authentication Completion
9. L3 Attach
10. Create Session Request
11. IP-CAN Session Establishment Procedure
12. Update PDN GW Address
13. Create Session Response
14. GTP Tunnel
(B)
15. L3 Attach Completion

Figure 8.2.1.2.2.1-1: Initial attachment in single-connection scenario in WLAN on GTP S2a for roaming and non-roaming scenarios

The procedure continues from step 2 in clause 8.2.1.2.1:

- Step 2. As part of this step, the UE is made aware of the network support of SAMOG phase 2 features and if the requested connectivity feature (attach to non-default APN, non-seamless WLAN offload, EPC-routed traffic) is accepted by the network. Also, if the UE requested EPC access without indicating APN, then the network indicates the selected (default) APN. If the UE requested EPC access and indicated an APN, then the network verifies that it is allowed by subscription. If the UE requested NSWO and it was accepted by the network, steps

3-7 and 10-14 are skipped. If the requested connectivity feature is not possible, the request is rejected with a relevant authorization failure.

- Step 3 and step 10. The TWAN selects the PDN GW for the APN, and includes the APN in the Create Session Request. The APN is determined by the TWAN based on the UE request and on the subscription data received from the AAA server.

NOTE: In the single-connection scenario, if a UE using NSWO wants to establish a PDN Connection, or if the UE has a PDN Connection but wants to use NSWO, the UE needs to detach from TWAN and make a new Initial Attach.

8.2.1.2.2.2 Initial Attach in single-connection scenario in WLAN on PMIP S2a (continuation)

Editor's notes: This procedure is still to be added.

8.2.1.2.3 Initial Attach in multi-connection scenario in WLAN on S2a (continuation)

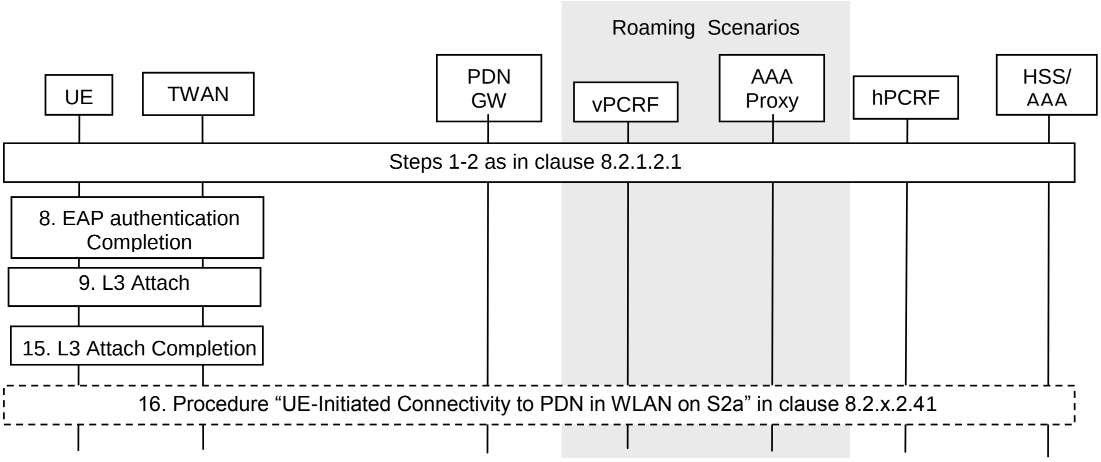

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Steps 1-2 as in clause 8.2.1.2.1
8. EAP authentication Completion
9. L3 Attach
15. L3 Attach Completion
16. Procedure “UE-Initiated Connectivity to PDN in WLAN on S2a” in clause 8.2.x.2.41

Figure 8.2.1.2.3-1: Initial attachment in multi-connection scenario in WLAN on GTP S2a for roaming, and non-roaming scenarios

The procedure continues from step 2 in clause 8.2.1.2.1:

- Step 2. As part of this step, the UE is made aware of the network support of SAMOG phase 2 features. Non-seamless WLAN offload is possible if the network supports this and the UE is entitled to use this. As part of step 2, the UE is made aware whether or not non-seamless WLAN offload is possible. If non-seamless WLAN offload is possible, then the UE receives the address or prefix of the non-seamless WLAN offload connection as part of steps 9 and 15. If non-seamless WLAN offload is not possible, then step 9 and 15 are not performed.

- Step 16. The procedure "UE-Initiated Connectivity to PDN in WLAN on S2a" in clause 8.2.1.2.4 may be performed to establish a PDN connection.

8.2.1.2.4 UE-Initiated Connectivity to PDN in WLAN on S2a

8.2.1.2.4.1 UE-Initiated Connectivity to PDN in WLAN on GTP S2a

This procedure can only be performed if the multi-connection scenario was selected during authentication.

This procedure is used when the UE has previously attached to WLAN and the UE wishes to establish one or more PDN connections over WLAN. This procedure is also used when the UE already has one or more PDN connections over WLAN and wishes to establish one or more additional PDN connections over WLAN. This procedure is also used to request for connectivity to an additional PDN connection over WLAN when the UE is simultaneously connected to WLAN and a 3GPP access, and the UE already has active PDN connections over both the accesses. The UE establishes a separate point-to-point link to the TWAG for each PDN connection.

There can be more than one PDN connection per APN when GTP is used between the TWAN and the PDN GW. During the establishment of a new PDN connection, the TWAN allocates and sends a default S2a bearer ID to the PDN

GW. The default S2a bearer ID is unique in the scope of the UE within a TWAG, i.e. the IMSI and the default S2a bearer ID together identify a PDN connection within a TWAG. In order to be able to identify a specific established PDN connection, both the TWAG and the PDN GW shall store the default S2a bearer ID.

NOTE: The establishment of a connection to a PDN connection does not impact the NSWO connection if that was previously setup. As a separate point-to-point link is used for each PDN connection, traffic separation can be achieved between all connections including the NWSO connection.

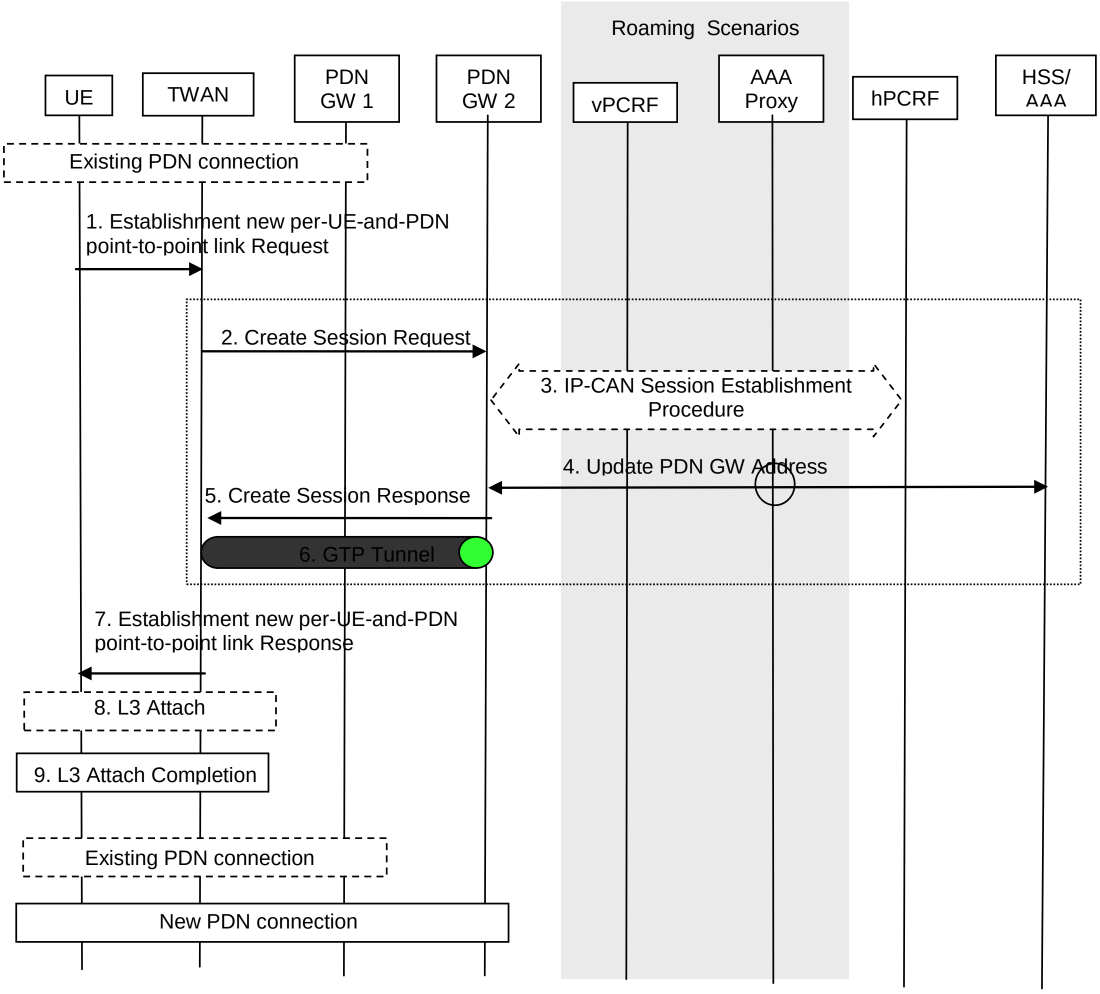

Roaming Scenarios
UE
TWAN
PDN GW 1
PDN GW 2
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Existing PDN connection
1. Establishment new per-UE-and-PDN point-to-point link Request
2. Create Session Request
3. IP-CAN Session Establishment Procedure
4. Update PDN GW Address
5. Create Session Response
6. GTP Tunnel
7. Establishment new per-UE-and-PDN point-to-point link Response
8. L3 Attach
9. L3 Attach Completion
Existing PDN connection
New PDN connection

Figure 8.2.1.4.2.1-1: UE-Initiated Connectivity to PDN in WLAN on GTP S2a

- Step 1. The UE triggers the establishment of a new per-UE-and-PDN point-to-point link by means of WLCP. This step establishes the setup of a new per-UE-and-PDN-connection point-to-point link to the TWAG. The UE may indicate the requested APN. The UE triggers the re-establishment of an existing PDN connectivity by providing a handover indicator. In that case, it shall provide an APN.

- Step 2-6. Same as step 3-7 in clause 8.2.1.2.2.1. As part of these steps, the TWAN verifies that the APN requested by the UE is allowed by subscription. Upon handover, the TWAN selects the PDN GW handling this PDN connection; otherwise, the TWAN performs PDN GW selection as described in TS 23.402 [3]. Steps 2-6 are executed with the selected PDN GW.

- Step 7. By means of WLCP, the TWAN returns a response to the establishment of a new per-UE-and-PDN point-to-point link. This response contains a User Plane Connection ID. If the UE did not indicate the APN in the request, then the response indicates the selected default APN. If the UE does not receive an IPv4 address in this step, it may negotiate the IPv4 address with DHCPv4 in step 8,

- Step 8. As step 9 in clause 8.2.1.2.2.1.

- Step 9. As step 15 in clause 8.2.1.2.2.1.

8.2.1.2.4.2 UE-Initiated Connectivity to PDN in WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.1.2.5 Handover procedure in single-connection scenario from 3GPP access to WLAN on S2a

8.2.1.2.5.1 Handover in single-connection scenario from 3GPP access to WLAN on GTP S2a

This procedure is used in the single-connection scenario to hand over a single PDN Connection from 3GPP access to WLAN. The decision to use the single-connection scenario is made during authentication as described in clause 8.2.1.2.1.

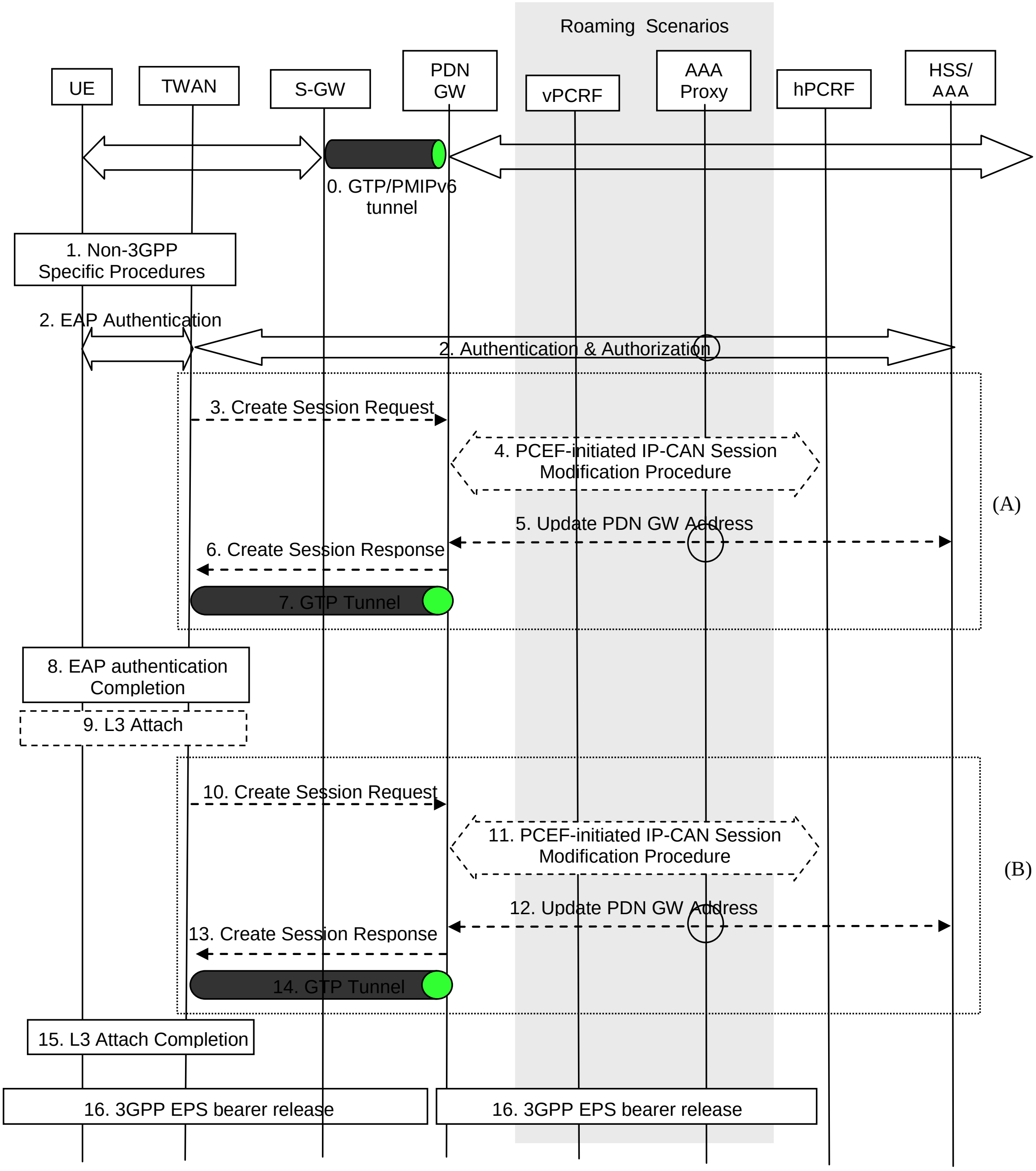

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0. GTP/PMIPv6 tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request
4. PCEF-initiated IP-CAN Session Modification Procedure
5. Update PDN GW Address
6. Create Session Response
7. GTP Tunnel
(A)
8. EAP authentication Completion
9. L3 Attach
10. Create Session Request
11. PCEF-initiated IP-CAN Session Modification Procedure
12. Update PDN GW Address
13. Create Session Response
14. GTP Tunnel
(B)
15. L3 Attach Completion
16. 3GPP EPS bearer release
16. 3GPP EPS bearer release

Figure 8.2.1.2.5.1-1: Handover in single-connection scenario from 3GPP access to Trusted WLAN on GTP S2a for roaming and non-roaming scenarios

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 8.2.1.2.5.1-1:

- 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 home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy are not involved, except for the authentication and authorization in step 2.

The steps in figure 8.2.1.2.5.1-1 are based on figure 8.2.1.2.2.1-1, with the following changes:

- Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.
- Step 2. As step 2 in 8.2.1.2.1.1with the following addition: If the UE supports single-connection, then the UE indicates handover via EAP-AKA to 3GPP AAA.
- Step 3 and 10. As step 3 and 10 in 8.2.1.2.2.1 with the following addition: The handover indication is set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP access and to initiate a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF.
- Step 4 and 11. The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [4]. The Event Report indicates the change in Access Type.

  If the PDN GW decides to allocate a new IP address/prefix instead of preserving the old IP address/prefix, as described in TS 23.402 [3] clause 4.1.3.2.3, the PDN GW executes an IP-CAN session Establishment Procedure with the PCRF instead of a PCEF-Initiated IP-CAN Session Modification Procedure.
- Step 6 and 13. The PDN GW responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Charging ID, Cause). The Create Session Response contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access. The Charging Id provided by the PGW is the Charging Id previously assigned to the default bearer of the PDN connection in the 3GPP access.
- Step 16. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.1.2.5.2 Handover in single-connection scenario from 3GPP access to WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.1.2.6 Handover procedure in multi-connection scenario from 3GPP access to WLAN on S2a

8.2.1.2.6.1 Handover in multi-connection scenario from 3GPP access to WLAN on GTP S2a

This procedure is used in the multi-connection scenario to hand over a one or more PDN Connection from 3GPP access to WLAN. The decision to use the multi-connection scenario is made during authentication as described in clause 8.2.1.2.1.

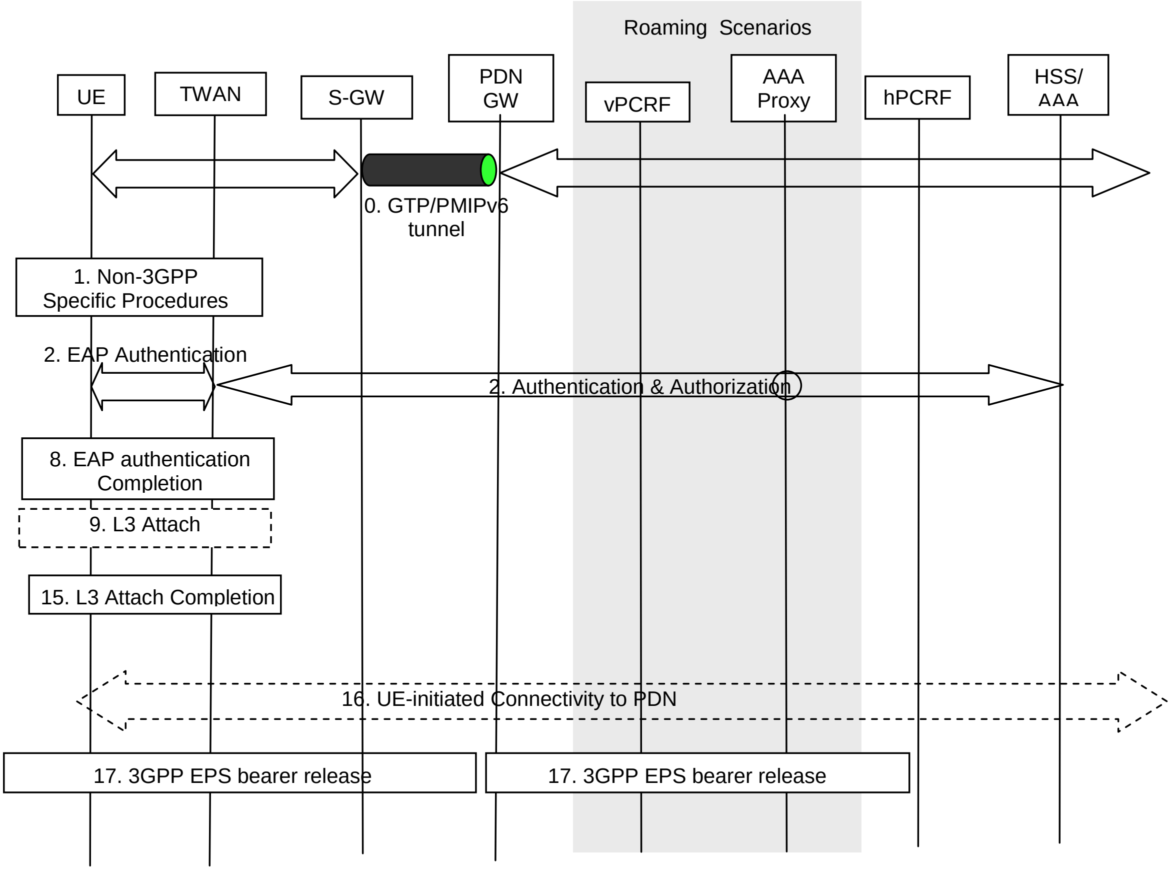

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0. GTP/PMIPv6 tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
8. EAP authentication Completion
9. L3 Attach
15. L3 Attach Completion
16. UE-initiated Connectivity to PDN
17. 3GPP EPS bearer release
17. 3GPP EPS bearer release

Figure 8.2.1.2.6.1-1: Handover from 3GPP access to Trusted WLAN on GTP S2a for roaming and non-roaming scenarios

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 8.2.1.2.6.1-1:

- 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 home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy are not involved, except for the authentication and authorization in step 2.

If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 1 to 15 shall be skipped and the UE shall only perform step 16 for each PDN connection that is being transferred from 3GPP access.

If the UE is connected only to 3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 15 shall be performed. As described in clause 8.2.1.2.3, these steps result in the UE receiving the address or prefix of the non-seamless WLAN offload connection, if supported by the network for this UE. The UE shall then perform step 16 for each PDN connection that is being transferred from 3GPP access.

Step 17 shall be repeated for each PDN connection that is being transferred from 3GPP access. Step 16 can occur in parallel for each PDN. Other aspects related to the handover for multiple PDNs are described in TS 23.402 [3] clause 8.1.

The steps in figure 8.2.1.2.6.1-1 are based on figure 8.2.1.2.3-1, with the following changes:

- Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.

- Step 2. As step 2 in 8.2.1.2.1 with the following addition: The UE indicates handover via EAP to 3GPP AAA.

- Step 16. For connectivity to multiple PDN connections, the UE establishes connectivity to each PDN that is being transferred from 3GPP access, by executing the UE-initiated Connectivity to PDN procedure specified in clause 8.2.1.2.4.

- Step 17. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.1.2.6.2 Handover from 3GPP access to WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.1.2.7 Handover procedure from WLAN on S2a to 3GPP access

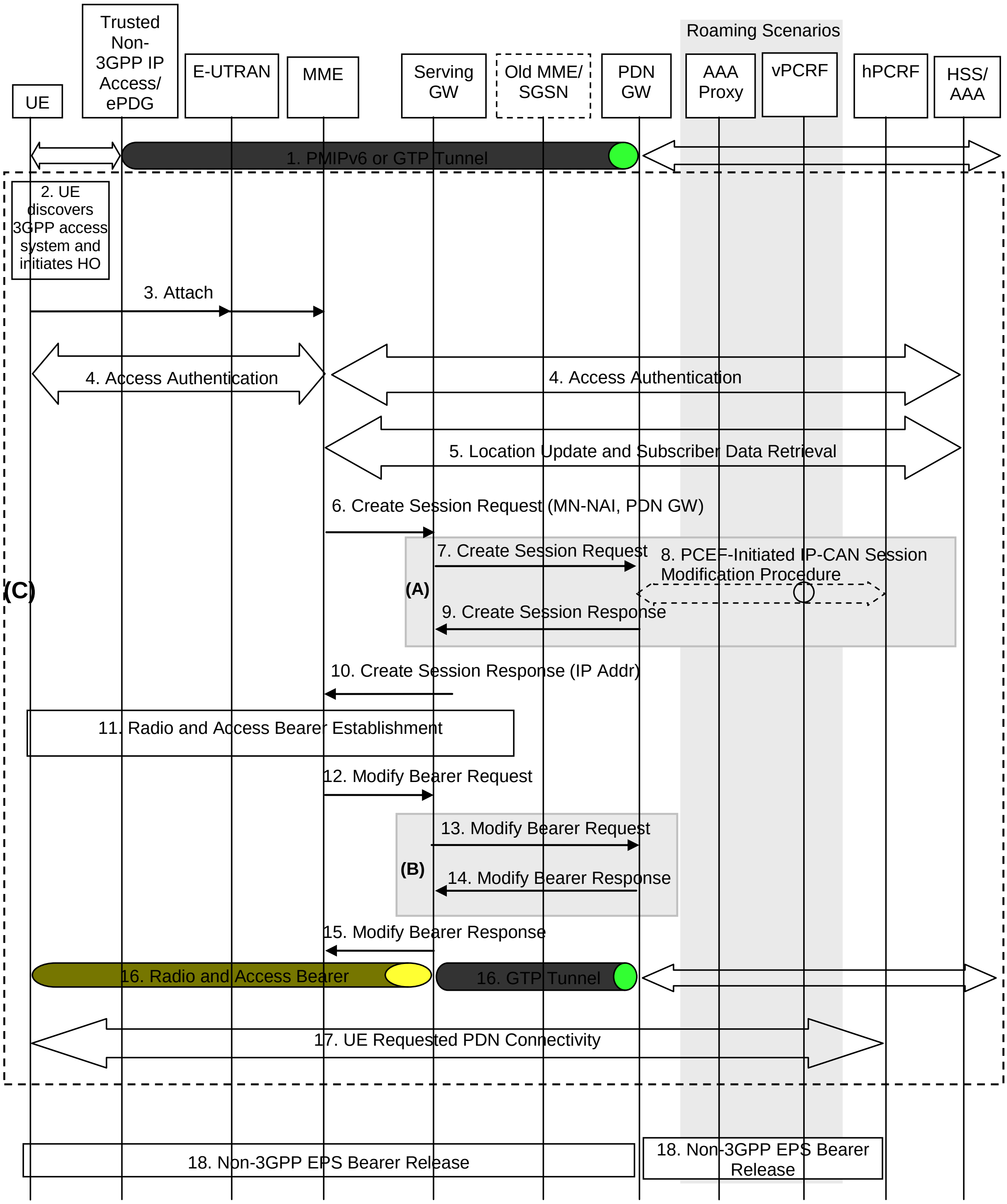

UE
Trusted Non-3GPP IP Access/ ePDG
E-UTRAN
MME
Serving GW
Old MME/ SGSN
PDN GW
Roaming Scenarios
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. PMIPv6 or GTP Tunnel
2. UE discovers 3GPP access system and initiates HO
3. Attach
4. Access Authentication
4. Access Authentication
5. Location Update and Subscriber Data Retrieval
6. Create Session Request (MN-NAI, PDN GW)
7. Create Session Request
8. PCEF-Initiated IP-CAN Session Modification Procedure
(A)
(C)
9. Create Session Response
10. Create Session Response (IP Addr)
11. Radio and Access Bearer Establishment
12. Modify Bearer Request
13. Modify Bearer Request
(B)
14. Modify Bearer Response
15. Modify Bearer Response
16. Radio and Access Bearer
16. GTP Tunnel
17. UE Requested PDN Connectivity
18. Non-3GPP EPS Bearer Release
18. Non-3GPP EPS Bearer Release

Figure 8.2.1.2.7-1: Handover from Trusted WLAN on GTP S2a to 3GPP access for roaming and non-roaming scenarios

This procedure is as in TS 23.402 [3] clause 8.2.1.1/8.2.1.2 with the following differences:

- Step 1. There is a GTP or PMIP tunnel between TWAN and PGW
- Step 18. The PDN GW shall initiate resource allocation deactivation procedure in the TWAN as defined in clause 8.2.1.2.9.

8.2.1.2.8 Detach and PDN disconnection in WLAN on S2a

8.2.1.2.8.1 Detach and PDN disconnection in WLAN on GTP S2a

8.2.1.2.8.1.1 UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection Procedure in WLAN on GTP S2a

For UE/TWAN initiated detach, this procedure is the same as TS 23.402 [3] clause 16.3.1.1.

If the single-connection scenario was selected during authentication, then the UE/TWAN requested PDN disconnection procedure is the same as TS 23.402 [3] clause 16.3.1.1.

If the multi-connection scenario was selected during authentication, then this clause applies to UE/TWAN-requested PDN disconnection procedure. For multiple PDN connections, this disconnection procedure shall be repeated for each PDN connection that needs to be released.

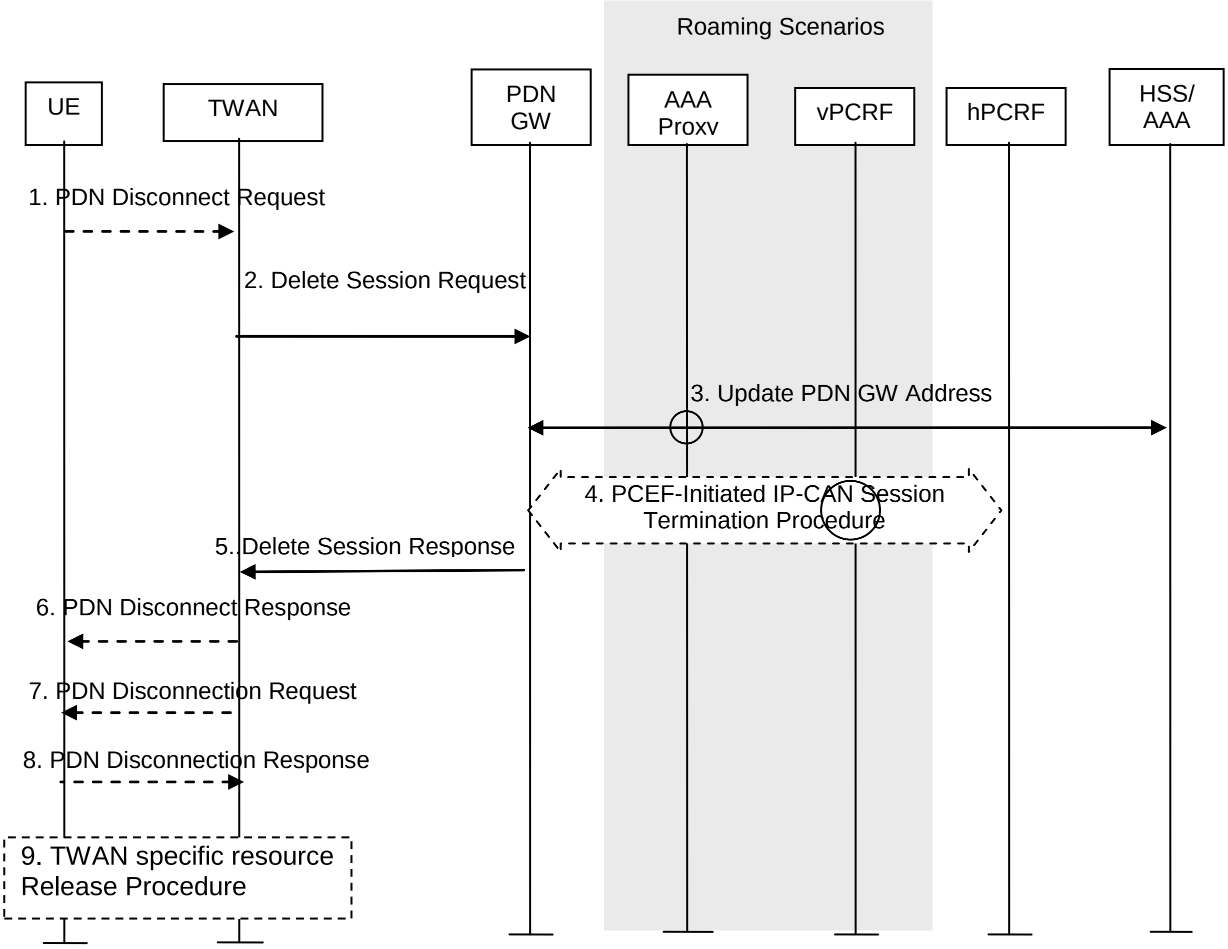

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. PDN Disconnect Request
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. PDN Disconnect Response
7. PDN Disconnection Request
8. PDN Disconnection Response
9. TWAN specific resource Release Procedure

Figure 8.2.1.2.8.1.1-1: UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF do not occur. Instead, the PDN GW may employ static configured policies.

- Step 1. If the PDN disconnection is initiated by the UE, the UE sends a PDN Disconnection Request (User Plane Connection ID) to the TWAG by means of WLCP.
- Step 2. The TWAN releases the PDN connection and sends a Delete Session Request (Linked EPS Bearer ID) message for this PDN connection to the PDN GW.

- Step 3. The PDN GW informs the 3GPP AAA Server of the PDN disconnection.

- Step 4. The PDN GW deletes the IP-CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [4].

- Step 5. The PDN GW acknowledges with a Delete Session Response (Cause) message.

- Step 6. If the PDN disconnection was initiated by the UE in step 1, then the UE is informed of the disconnection by means of a WLCP PDN Disconnection Response.

- Step 7. If the PDN disconnection was initiated by the TWAG, then the UE is informed of the disconnection by means of a WLCP PDN Disconnection Request (User Plane Connection ID).

- Step 8. The UE acknowledges the disconnection request received in step 7.

NOTE: Either step 1 and 6, or step 7 and 8, are performed

8.2.1.2.8.1.2 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a

This procedure is the same as TS 23.402 [3] clause 16.3.1.2.

8.2.1.2.8.2 Detach and PDN disconnection in WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.1.2.9 PDN GW initiated Resource Allocation Deactivation

8.2.1.2.9.1 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

If the single-connection scenario was selected during authentication, then this procedure is the same as TS 23.402 [3] clause 16.4.1.

If the network selected the multi-connection scenario during authentication, then this procedure is as in TS 23.402 [3] clause 16.4.1 with the following difference: If all TWAN resources related to a PDN connection are released, then in step 3 the UE is informed of the PDN connection release using WLCP.

8.2.1.2.9.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.1.3 Impacts on existing nodes or functionality

Editor's note: Impact on existing nodes or functionality is still to be added.

Refer to clause 8.2.1.4.

8.2.1.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 should be evaluated.

This is a "2 scenarios" solution that supports *single-connection* UEs and *multi-connection* UEs.

i) Impacts to existing network deployment

   a) New requirements on WLAN APs compared to Rel-11

      None

   b) Additional assumptions on AP-TWAG link

      None beyond those of SAMOG Rel11

ii) Impacts to UE

Support of the tunnelling mechanism when the UE supports the Multi-connection scenario as in all solutions that support simultaneous multiple PDN connections)

Support of the WLCP (when the UE supports the Multi-connection scenario)

Support of the new EtherType (when the UE supports the Multi-connection scenario)

Support of EAP-AKA' modifications to support PDN connection set-up (when the UE supports the single-connection scenario)

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA')

EAP-AKA' extension for the capability negotiation and for the support of the single-connection scenario

iv) Impacts to protocols defined by other SDOs (e.g. DHCP)

Depending on the user plane and control plane variant, one or two new IEEE EtherType values are needed.

v) Control plane

a) Latency/load of first/additional PDN connections setup and handover procedures

Compared to SaMOG Rel-11, only one extra exchange (request-reply) of WLCP messages for each PDN connection setup and handover procedures

When established, NSWO connectivity is created during EAP-AKA' exchange i.e. does not delay the establishment of further PDN connections

b) Network element impacts (e.g. AAA signalling etc.)

AAA to relay some information of EAP-AKA' signalling at initial attach. No new message exchange to support at AAA level

The TWAG must support WLCP

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements

a) Co-existence with Rel-11 SaMOG

b) Support for IP address preservation during handover

c) Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDN connections (in case of multiple connection scenario)

Compliant with all requirements

As a new control protocol is to be defined, this protocol can be made extendable with new information elements and messages for future uses and can be based on functionality already existing in 3GPP specifications for the cellular link

vii) Others functional limitations

None

On top of the points above, the solution shares some common points with all other solutions such as the need for the UE and the AAA server to support EAP-AKA' modifications.

The small overhead due to tunnelling (VLAN, GRE key) may slightly reduce the path MTU. This point is shared with all other solutions that share the same user plane tunnelling

8.2.2 Solution 2: Layer 2 solution based on Stateful Address Configuration of Per-PDN Connection/NSWO Point-to-Point Link Multiplexed at Layer 2

8.2.2.1 Functional Description

8.2.2.1.1 User Plane Multiplexing for Per-PDN Connection / NSWO Point-to-Point Link

8.2.2.1.1.0 General

The solution relies on the use of Stateful Address Configuration of Per-PDN Connection / NSWO Point-to-Point Link Multiplexed at Layer 2.

In addition to the two mechanisms described as part of this solution in clause 8.2.2.1.1.1 (Per PDN/NSWO VLAN Id), and clause 8.2.2.1.1.2 (Per PDN/NSWO TWAG MAC Address), any type of per-PDN/NSWO packet marking mechanism layered directly over L2 but below IPv4/IPv6 could be used with this solution, including, but not limited to, keyed GRE over Ethernet as described as part of Solution 1 in clause 8.2.1, or a new 3GPP specific LLC/SNAP header as described as part of Solution 8 in clause 8.2.8.

Multiple PDN Connections to the same APN are supported via allocation of multiple identifiers (e.g. VLAN Ids) for multiple point-to-point links.

8.2.2.1.1.1 Per-PDN Connection/NSWO Virtual Point-to-Point Link Model based on distinct VLAN ID

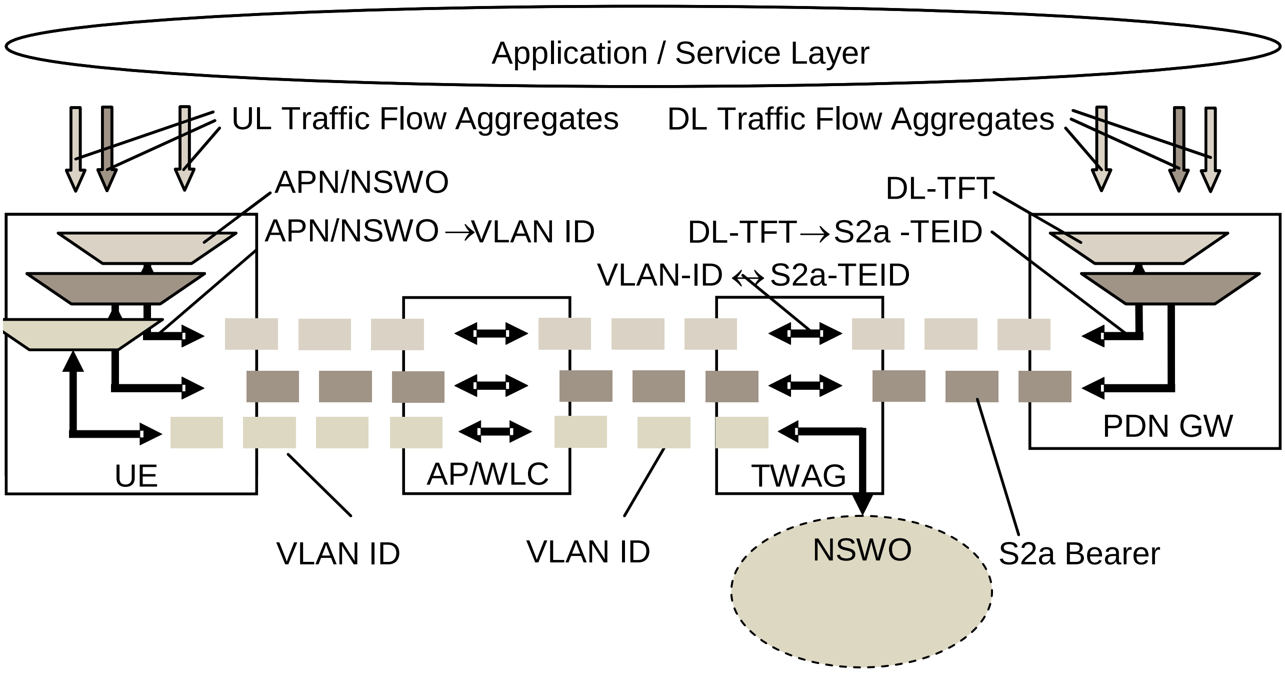


Figure 8.2.2.1.1.1-1: Point-to-point link model for PDN connection and NSWO access based on distinct VLAN ID

In this link model the virtual point-to-point link required to transport traffic for a given PDN connection, of for Non-Seamless WLAN Offload (NSWO) is realized via the TWAG reserving a distinct VLAN ID that uniquely (on a per-UE basis) corresponds to an APN or NSWO. These distinct VLAN ID are configured on the TWAG interface, i.e. the TWAG can receive and send layer 2 frames from and to each of these VLAN ID.

As depicted in Figure 8.2.2.1.1.1-1, the virtual point-to-point link is realized via enforcing forwarding of uplink and downlink IP packets between distinct PDN connections and NSWO access into their corresponding VLANs via marking layer 2 frame contacting these IP packets with the appropriate VLAN ID. VLAN marking over the IEEE Std 802.11 air link is performed as per Annex P of IEEE 802.11 [5].

On the UE, each of the virtual point-to-point link is modelled as a virtual interface that is exposed to the IP layer with a fixed IPv4 and/or IPv6 address(es). Applications can bind sockets to a specific virtual interface thus in effect binding the socket to a specific PDN connection or to NSWO access. Packet transmission occurs as follow:

- In the uplink direction, all IP packets transmitted via the virtual interface, including IP multicast packets, are encapsulated in layer 2 frames marked with the VLAN ID that corresponds to the PDN connection or NSWO access the socket/interface is bound to. On the receiving side, the TWAG is able to de-multiplex incoming packets towards the appropriate PDN connection or NSWO access via looking up the VLAN ID of the layer 2 data frame.
- In the downlink direction, the TWAG transmits all IP packets, including IP multicast packets, encapsulated in layer 2 frames marked with the VLAN ID that corresponds to the PDN connection or NSWO access the packet originated from. On the receiving side, the UE is able to de-multiplex incoming packets towards the appropriate PDN connection or NSWO access via looking up the VLAN ID of the layer 2 data frame, and passes the IP packets contained in these frames to the IP layer via the corresponding virtual interface.

8.2.2.1.1.2 Per-PDN Connection/NSWO Virtual Point-to-Point Link Model based on distinct layer 2 TWAG MAC addresses

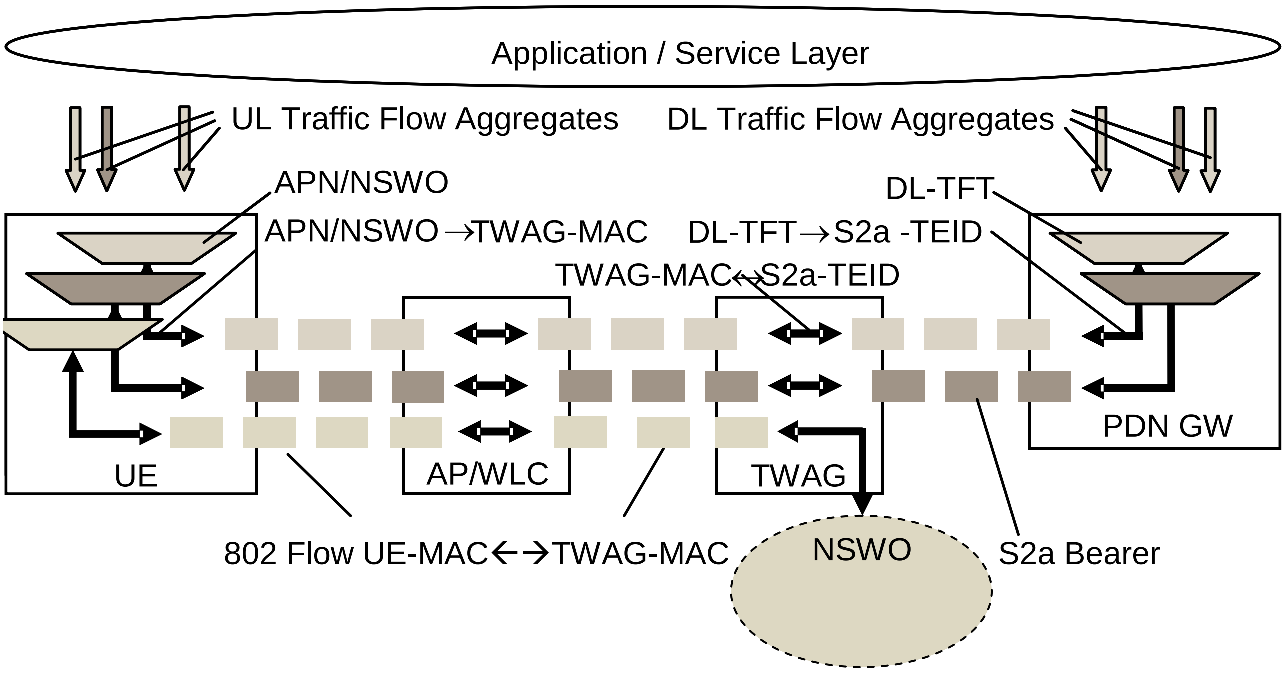

Application / Service Layer
UL Traffic Flow Aggregates
DL Traffic Flow Aggregates
APN/NSWO
DL-TFT
APN/NSWO→TWAG-MAC
DL-TFT→S2a -TEID
TWAG-MAC↔S2a-TEID
UE
AP/WLC
TWAG
PDN GW
802 Flow UE-MAC←→TWAG-MAC
NSWO
S2a Bearer

Figure 8.2.2.1.1.2-1: Point-to-point link model for PDN connection and NSWO access based on distinct layer 2 TWAG MAC addresses

In this link model the virtual point-to-point link required to transport traffic for a given PDN connection, of for Non-Seamless WLAN Offload (NSWO) is realized via the TWAG reserving a distinct MAC address that uniquely (on a per-UE basis) corresponds to an APN or NSWO. These distinct layer 2 MAC addresses are configured on the TWAG interface, i.e., the TWAG can receive and send layer 2 frames from each of these MAC addresses.

As depicted in Figure 8.2.2.1.1.2-1, the virtual point-to-point link is realized via enforcing a forced forwarding of uplink and downlink IP packets respectively to and from the corresponding layer 2 TWAG MAC address located in the layer 2 header of the frame containing the IP packets.

On the UE, each of the virtual point-to-point link is modelled as a virtual interface that is exposed to the IP layer with a fixed IPv4 and/or IPv6 address(es). Applications can bind sockets to a specific virtual interface thus in effect binding the socket to a specific PDN connection or to NSWO access. Packet transmission occurs as follow:

- In the uplink direction, all IP packets transmitted via the virtual interface, including IP multicast packets, are encapsulated in layer 2 frames with destination layer 2 address set to the layer 2 unicast MAC address of the TWAG that corresponds to the PDN connection or NSWO access the socket/interface is bound to. On the receiving side, after identifying the associated UE using the source MAC address of the data frame, the TWAG is able to de-multiplex incoming packets towards the appropriate PDN connection or NSWO access via looking up the layer 2 destination address TWAG-MAC of the data frame.

- In the downlink direction, the TWAG transmits all IP packets, including IP multicast packets, encapsulated in layer 2 frames with source layer 2 address set to the layer 2 unicast MAC address of the TWAG that corresponds to the PDN connection or NSWO access the packet originated from. On the receiving side, the UE is able to de-multiplex incoming packets towards the appropriate PDN connection or NSWO access via looking up the layer 2 source unicast MAC address of the data frame, and passes the IP packets contained in these frames to the IP layer via the corresponding virtual interface.

8.2.2.1.2 Initial Attach in WLAN

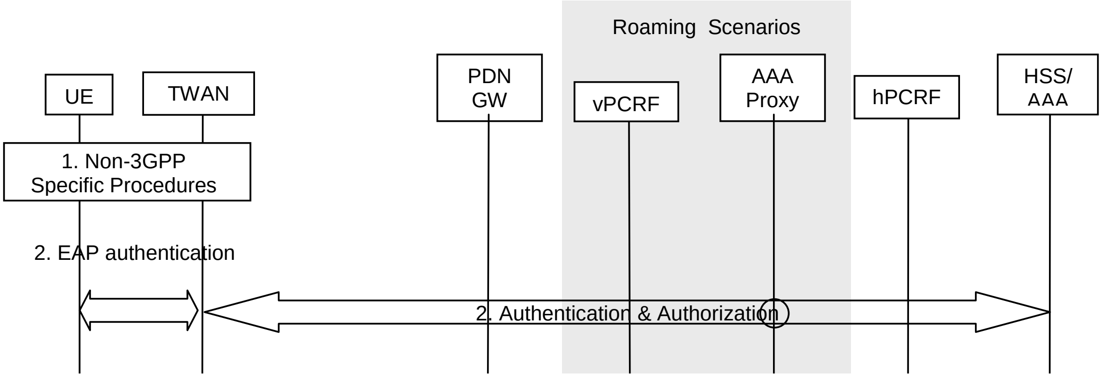


Figure 8.2.2.1.2-1: Initial Attach in WLAN on GTP or PMIP S2a for roaming, LBO and non-roaming scenarios

As depicted in Figure 8.2.2.1.2-1, the initial attach procedure occurs with the following steps:

The first step of the proposal is for both the UE, the Trusted WLAN Access, and the 3GPP AAA Server in the HPLMN to discover whether all of them do support fully fledged Trusted WLAN Access to the EPC (i.e., as per the requirements, concurrent multiple PDN connections, IP address preservation, and concurrent NSWO and EPC access). This is done in the following way:

1. The UE discovers the TWAN and associates with it.

2. The TWAN begins the EAP exchange by sending an EAP Request message as part of the IEEE 802.1X authentication procedure [5]. As part of the EAP exchange, the UE, the Trusted WLAN Access, and the 3GPP AAA Server in the HPLMN to discover whether all of them do support fully fledged Trusted WLAN Access to the EPC (i.e. as per the requirements, concurrent multiple PDN connections, IP address preservation, and concurrent NSWO and EPC access):

   a) The UE indicates support to the 3GPP AAA server in the HPLMN via including an indication EAP-AKA attribute in the EAP-AKA Response messages it sends.

   b) The Trusted WLAN Access indicates support to the 3GPP AAA server in the HPLMN via including an indication AAA attribute in the Diameter EAP-Request message it sends.

   c) The 3GPP AAA server in the HPLMN indicates to the Trusted WLAN Access that both itself and the UE have support via inclusion of the same indication AAA attribute in the Diameter EAP-Answer message it sends.

   d) The 3GPP AAA server in the HPLMN indicates to UE that both itself and the Trusted WLAN Access have support via inclusion of a similar indication attribute within the EAP-AKA Request message.

   e) If either of the UE, the Trusted WLAN Access Network, or the 3GPP AAA Server in the HPLMN support fully fledged Trusted WLAN Access to the EPC, failback to single PDN connection to a default per-subscription APN ensues (phase 1 SaMOG) according to steps 3-15 of clause 16.2.1of TS 23.402 [3] in case of GTP S2a or clause 16.2.2 of TS 23.402 [3] in case of PMIP S2a. If on the other hand all of the UE, the Trusted WLAN Access Network, and the HPMLN support fully fledged Trusted WLAN Access to the EPC, neither PDN connections nor Non-Seamless WLAN Offload (NSWO) is offered automatically by the Trusted WLAN Access without explicit request from the UE as described in clause 8.2.2.1.3.

8.2.2.1.3 UE Requested PDN or NSWO connectivity

The UE explicitly requests establishment of PDN connections and/or NSWO in two steps: preparation and execution.

In a first preparation step, the UE queries from the network the values of the VLAN or TWAG MAC address to use to reach a list of APNs it might want to establish a PDN connection to in the future, including the unspecified 'default' APN that will be selected by the network (similar to the default APN that exists in phase 1 of SaMOG), as well as NSWO. The UE also indicates to the network the PDN Type of the PDN connection it will desire to establish. The signalling to carry on with this query from the UE to the network based on the use of EAP-AKA [22] extensions attributes during the authentication phase. As a result of this query, the network indicates to the UE a list of VLAN identifiers (first variant of the virtual point-to-point link model), TWAG MAC addresses (second variant of the virtual point-to-point link model), or any other point-to-point link multiplexing identifier (e.g., for keyed GRE or new 3GPP SNAP protocol) that corresponds to each of the APN in which it has expressed interest in connecting to (as well as the value that was selected by the network as the 'default' APN) on one hand, and to NSWO on the other hand. Again, the signalling to carry on with this indication from the network to the UE is based on the use of EAP-AKA extension attributes that are populated by the 3GPP AAA Server based on information received from the Trusted WLAN Access. A list of L2 identifiers for multiplexing of the point-to-point links is chosen locally by the TWAN based on configuration, and sent to the AAA server over STa. The AAA server extracts from this list as many L2 identifiers as there are PDN connections requested by the UE in the EAP Response/Identity, and includes it together with the authorized PDN types for those APN as per the subscription in the EAP Request/AKA-Challenge or AKA-Reauthentication message sent back to the UE, while the list of APNs for the PDN connections requested by UE is sent to the TWAN over STa.

In case of a selected PDN GW only allowing single IP version PDN Type IPv4 for an APN, if the UE requests dual IP version PDN Type IPv4v6, the PDN GW that only supports IPv4 only completes the DHCPv4 address configuration exchange and never sends an IPv6 Router Advertisement. Based on not receiving IPv6 configuration parameters but receiving IPv4 configuration parameters, the UE concludes that the selected PDN GW only allows single IP version PDN Type IPv4. In case of a selected PDN GW only allowing single IP version PDN Type IPv6 for an APN, if the UE requests dual IP version PDN Type IPv4v6, the PDN GW that only supports IPv6 only completes the IPv6 Stateless Address Auto-configuration exchange and never replies to DHCP messages sent by the UE. Based on not receiving IPv4 configuration parameters but receiving IPv6 configuration parameters, the UE concludes that the selected PDN GW only allows single IP version PDN Type IPv6.

IF a UE expects to need multiple PDN connections to a single APN, it needs to requests multiple point-to-point link multiplexing identifiers for that same APN. The network may decide to respond fully to the request, or with a lesser number of point-to-point link multiplexing identifiers.

NOTE 1: Because the values of the point-to-point link identifiers for the various APNs the UE wishes to connect to are negotiated during the EAP-AKA exchange, APNs need to be known prior to authentication with the Trusted WLAN Access. In the unlikely event that the UE needs to connect to an unforeseen APN, the UE would be required to disconnect, then reconnect, to the Trusted WLAN Access.

NOTE 2: Because the values of the point-to-point link identifiers for the various APNs the UE wishes to connect to are negotiated during the EAP-AKA exchange, all this information needs to fit in a single EAP-AKA message. This places a limit on the number of the point-to-point links and APNs that can be negotiated. However given that on a 3GPP access a UE is also limited to a maximum of 12 simultaneous bearers, and hence PDN connections, it is deemed reasonable that for Trusted WLAN Access a limitation also exists.

NOTE 3: In case where the subscription profile list the wildcard APN, the TWAN would need to send all APNs supported by an HPLMN (with corresponding VLAN IDs or TWAG MAC addresses) to the UE via EAP-AKA' or ANQP.

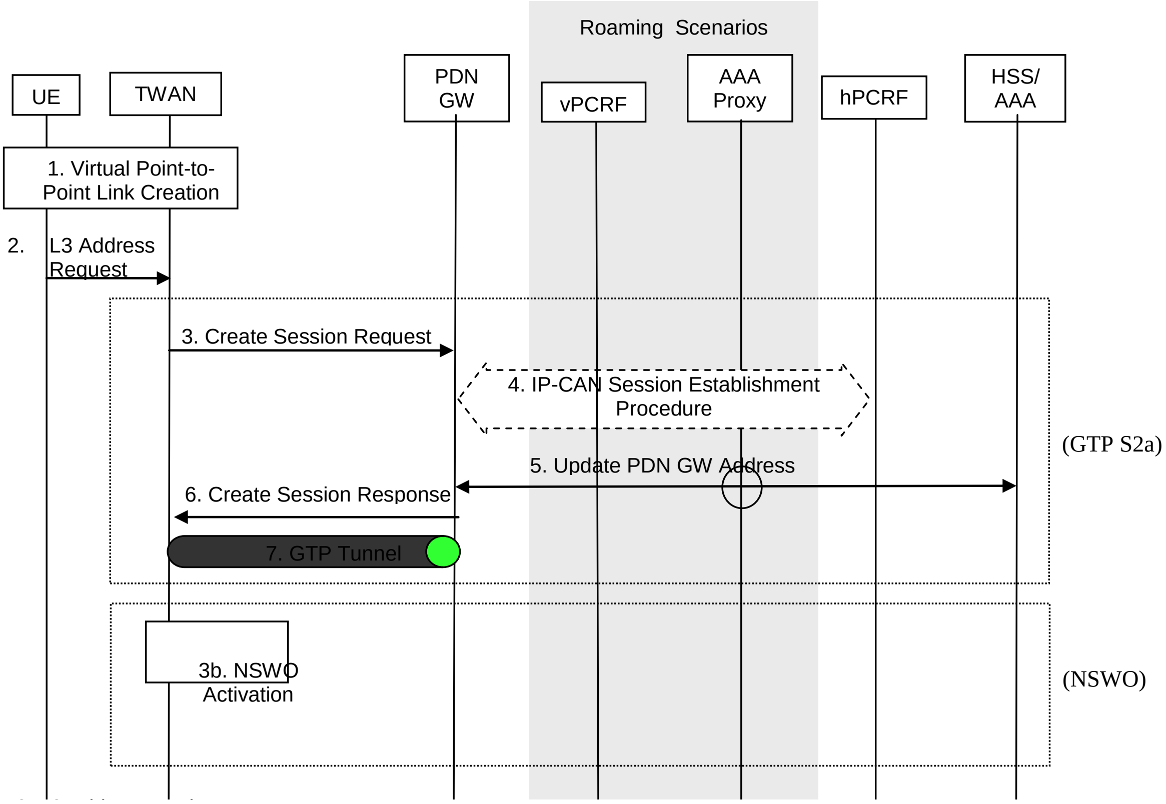


Figure 8.2.2.1.3-1: UE requested PDN or NSWO connectivity for GTP-based S2a

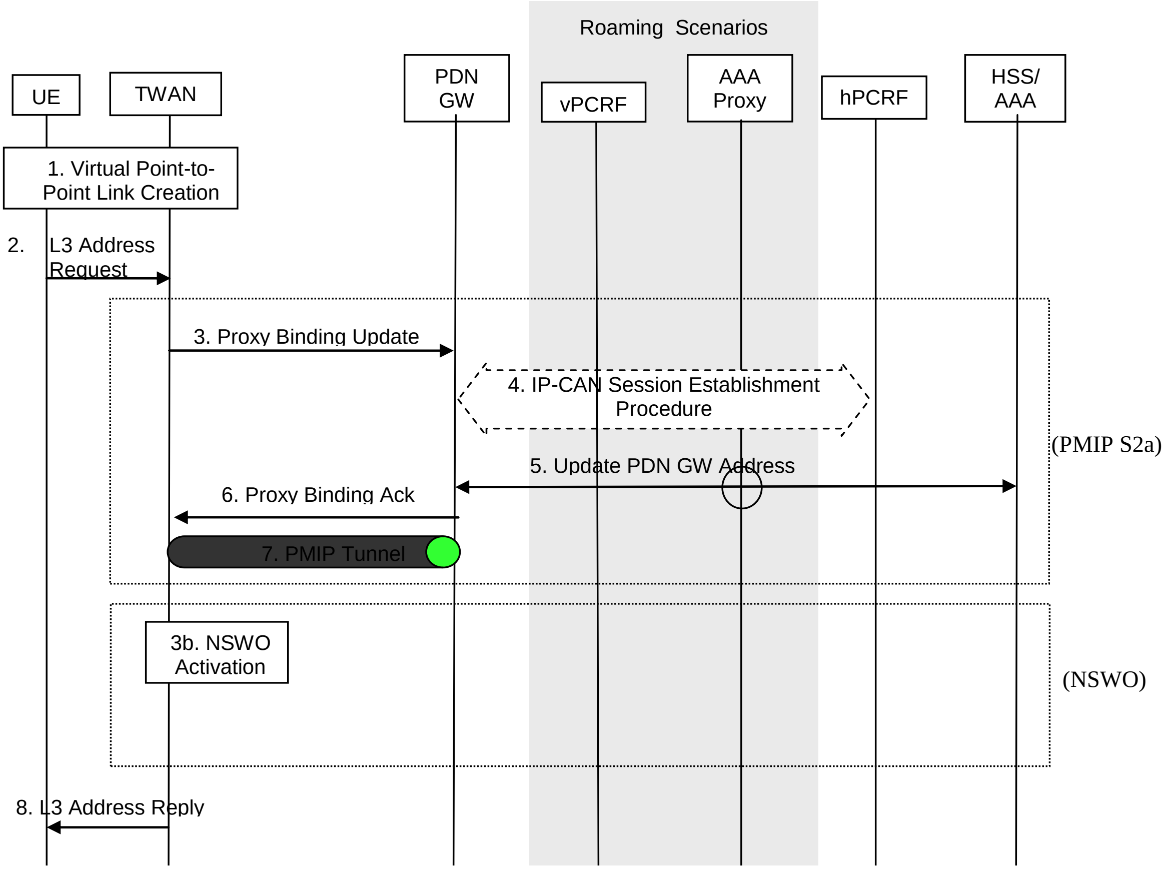


Figure 8.2.2.1.3-2: UE requested PDN or NSWO connectivity for PMIP-based S2a

In a second execution step, the UE explicitly requests establishment of a PDN connection to a specific APN or activation and deactivation of NSWO as per the following steps depicted in Figure 8.2.2.1.3-1 for GTP-based S2a and Figure 8.2.2.1.3-2 for PMIP-based S2a:

1. The UE creates a virtual IP interface corresponding to the APN towards which it desires to establish a PDN connection, or to NSWO.

2. The UE requests allocation of an IPV4 and/or IPv6 address for this virtual interface by sending a DHCP or DHCPv6 request message from this virtual interface. In the first variant of the virtual point-to-point link model, the layer 2 frame carrying the DHCP is marked with the corresponding VLAN Id. In the second variant of the virtual point-to-point link model, the layer 2 frame carrying the DHCP message will be unicasted to the corresponding TWAG MAC address.

NOTE 4: The UE may requests allocation of an IPv4 address via DHCP but still perform IPv6 Stateless Address Auto-Configuration (SLAAC) for configuration of its IPv6 address. In this case, the UE or the network signal the will to tear down a PDN connection and/or NSWO access based solely on DHCP signalling for the IPv4 address.

3-7. When the TWAG receives the DHCP IPv4 and/or IPv6 address allocation request over the virtual interface corresponding to a specific VLAN (first variant of the virtual point-to-point link model) or TWAG MAC address (second variant of the virtual point-to-point link model), that corresponds to an APN it requests to the PDN GW creation of a GTP or PMIP tunnel for the APN as per steps 3-7 of respectively clause 16.2.1 or 16.2.2 of TS 23.402 [3] in case of GTP-based S2a or PMIP-based S2a, otherwise it activates NSWO if the virtual interface corresponds to NSWO access (step 3b).

8. The TWAG then sends a DHCP reply to the UE with an IPv4 address and/or IPv6 address as allocated by the PDN GW or by the NSWO access. The UE can then use the PDN connection via the virtual interface. Within the Trusted WLAN Access, the different virtual point-to-point links ensure separation of user plane traffic belonging to separate APNs and NSWO. The TWAG enforces forwarding between specific virtual point-to-point links and the GTP or PMIP tunnels towards the specific APNs, or NSWO access.

8.2.2.1.4 UE Requested PDN or NSWO disconnection

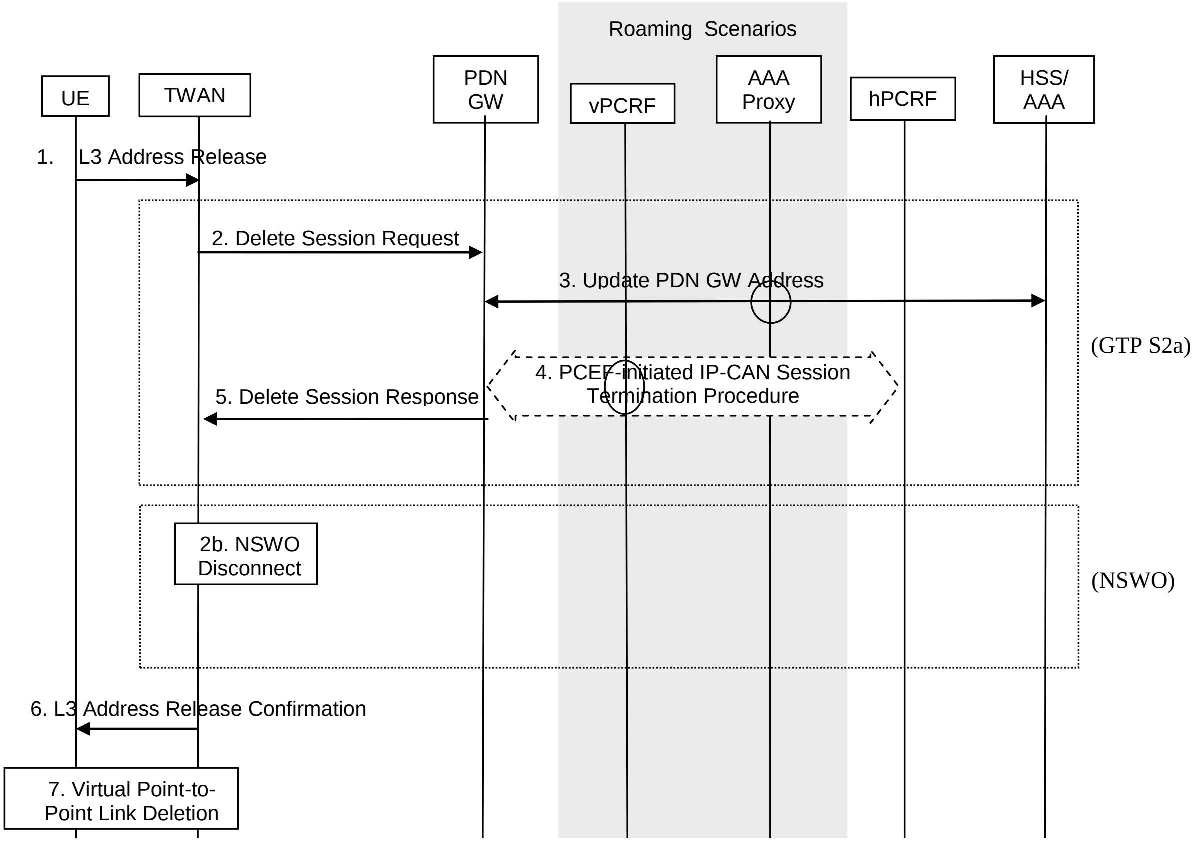

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. L3 Address Release
2. Delete Session Request
3. Update PDN GW Address
(GTP S2a)
4. PCEF-initiated IP-CAN Session Termination Procedure
5. Delete Session Response
2b. NSWO Disconnect
(NSWO)
6. L3 Address Release Confirmation
7. Virtual Point-to-Point Link Deletion

Figure 8.2.2.1.4-1: UE requested PDN or NSWO disconnection for GTP-based S2a

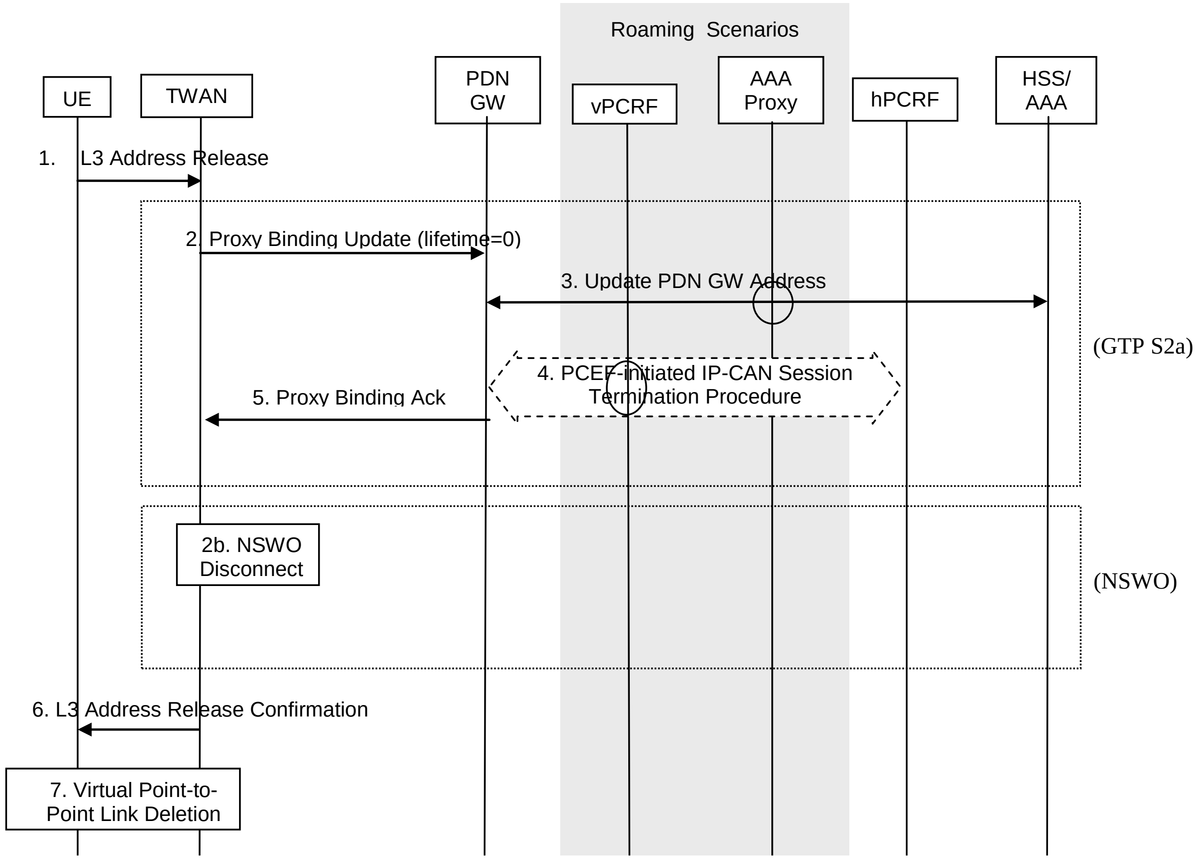

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. L3 Address Release
2. Proxy Binding Update (lifetime=0)
3. Update PDN GW Address
(GTP S2a)
4. PCEF-initiated IP-CAN Session Termination Procedure
5. Proxy Binding Ack
2b. NSWO Disconnect
(NSWO)
6. L3 Address Release Confirmation
7. Virtual Point-to-Point Link Deletion

Figure 8.2.2.1.4-2: UE requested PDN or NSWO disconnection for PMIP-based S2a

The UE explicitly requests disconnection of a PDN disconnection to a specific APN or deactivation of NSWO and deactivation of NSWO as per the following steps:

1. The UE releases the IPv4 and/or IPv6 address allocated for the virtual interface by sending a DHCP or DHCPv6 release from this virtual interface. In the first variant of the virtual point-to-point link model, the layer 2 frame carrying the DHCP message is marked with the corresponding VLAN Id. In the second variant of the virtual point-to-point link model, the layer 2 frame carrying the DHCP message will be unicasted to the corresponding TWAG MAC address.

2. When the TWAG receives the DHCP IPv4 and/or IPv6 address release message over the virtual interface corresponding that corresponds to an APN, it requests to the PDN GW deletion of the GTP tunnel, or the PMIP tunnel for this APN as per steps 2-5 of respectively clause 16.3.1.1 of TS 23.402 [3] in case of GTP-based S2a, or clause 16.3.2.1 of TS 23.402 [3] in case of PMIP-based S2a, or disconnects NSWO if the virtual interface corresponds to NSWO (step 2b).

6. The TWAG then sends a DHCP reply to the UE to confirm release of the IPv4 address and/or IPv6 address for the PDN connection or the NSWO access.

7. The UE then deletes the virtual IP interface for the virtual point-to-point link corresponding the PDN connection, or to NSWO.

8.2.2.1.5 HSS/AAA Initiated PDN or NSWO Disconnection procedure in WLAN

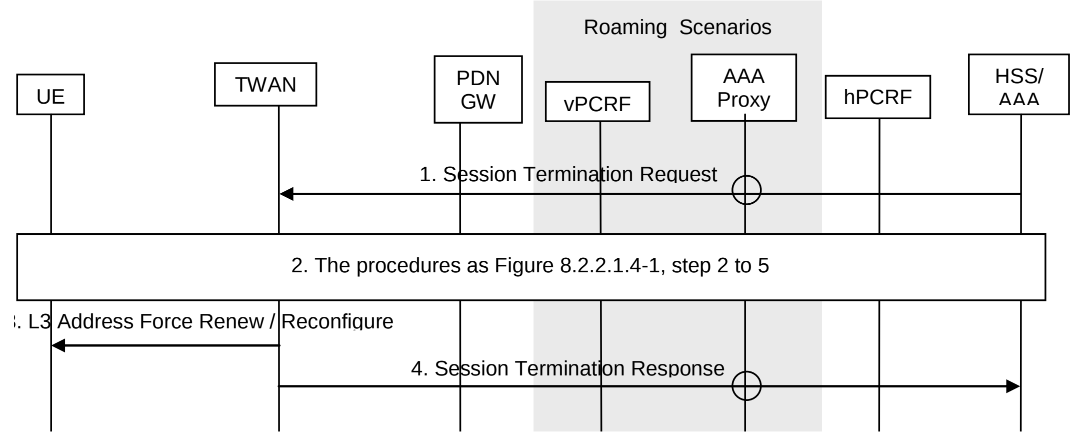

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as Figure 8.2.2.1.4-1, step 2 to 5
. L3 Address Force Renew / Reconfigure
4. Session Termination Response

Figure 8.2.2.1.5-1: HSS/AAA Initiated Detach on GTP S2a

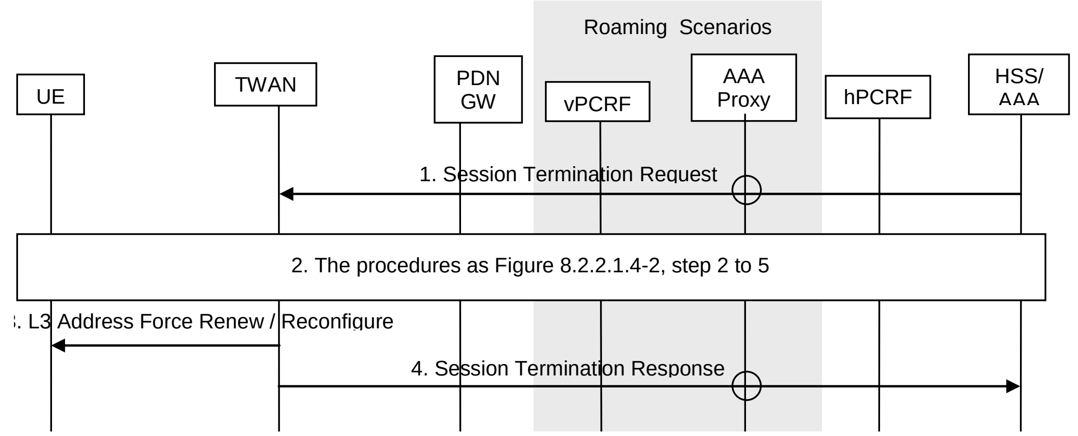

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as Figure 8.2.2.1.4-2, step 2 to 5
. L3 Address Force Renew / Reconfigure
4. Session Termination Response

Figure 8.2.2.1.5-2: HSS/AAA Initiated Detach on PMIP S2a

The procedure for HSS/AAA Initiated Detach from TWAN is represented in Figure 8.2.2.1.5-1 in case of GTP-based S2a and Figure 8.2.2.1.5-2 in case of PMIP-based S2a and described below:

1) The HSS/AAA sends a Session Termination Request message to the TWAN to detach a specific UE.

2) The step 2 to 5 of the UE/TWAN Initiated PDN or NSWO Disconnection procedure described in clause 8.2.2.1.4 are followed.

3) The TWAG force the UE to renew its IPv4 and/or IPv6 address(es) by sending a DHCP FORCERENEW message as per IETF RFC 3203 [24] or DHCPv6 Reconfigure message as per IETF RFC 3315 [23]. The DHCP FORCERENEW message is secured via Forcerenew Nonce Authentication as per RFC 6704 [29]. When the UE proceeds with renewing the address lease for the APN or NSWO, the TWAG can in turn refuse to do so, notifying to the UE that the PDN or NSWO has been disconnected.

4) TWAN sends a Session Termination Response message to 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates this to the HSS as described in clause 12.1.2 of TS 23.402 [3]. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3 of TS 23.402 [3].

8.2.2.1.6 HSS/AAA Initiated Detach procedure in WLAN

This procedure is similar to clause 16.3.2.2.2 of TS 23.402 [3].

8.2.2.1.7 Handover from 3GPP Access to Trusted WLAN Access

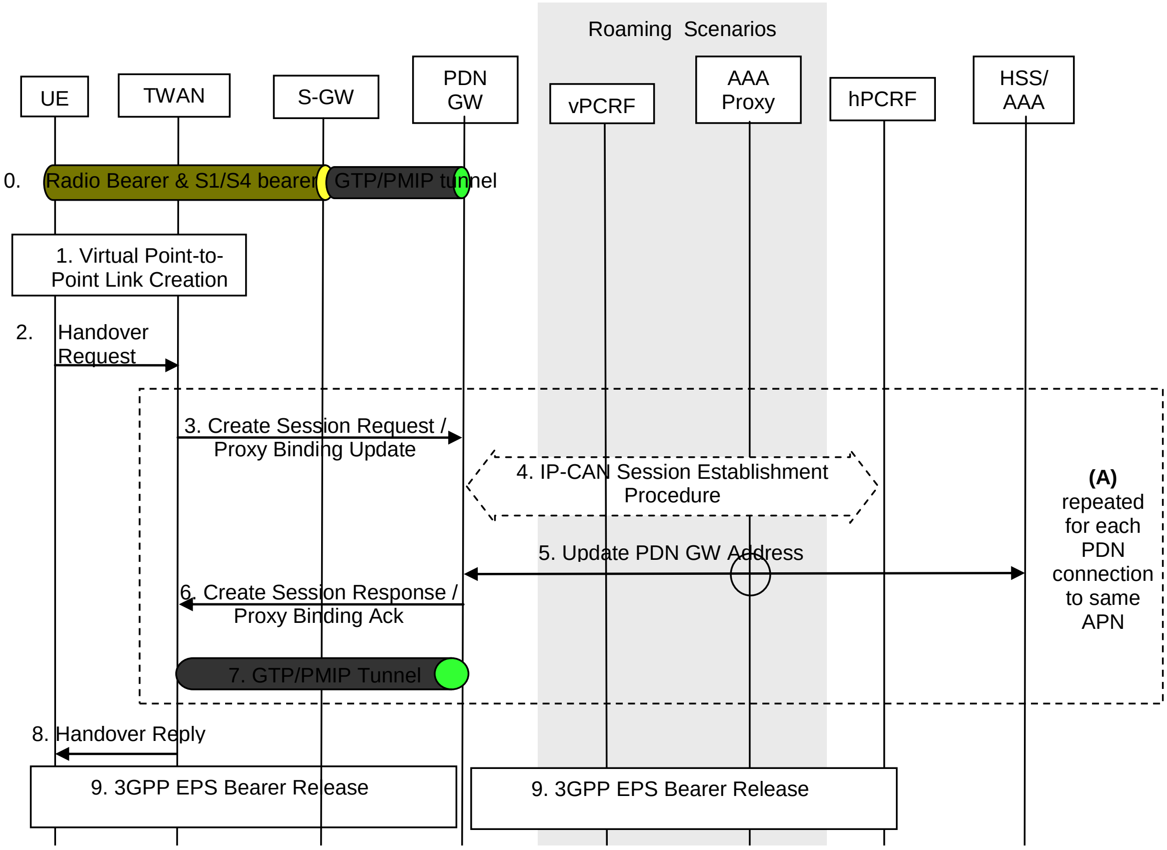

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0.
Radio Bearer & S1/S4 bearer
GTP/PMIP tunnel
1. Virtual Point-to-Point Link Creation
2. Handover Request
3. Create Session Request / Proxy Binding Update
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Create Session Response / Proxy Binding Ack
7. GTP/PMIP Tunnel
(A) repeated for each PDN connection to same APN
8. Handover Reply
9. 3GPP EPS Bearer Release
9. 3GPP EPS Bearer Release

Figure 8.2.2.1.7-1: Handover from 3GPP Access to Trusted WLAN Access

In a second execution step, the UE explicitly requests handover of a PDN connection to a specific APN as per the following steps depicted in Figure 8.2.2.1.7-1 for GTP-based S2a and Figure 8.2.2.1.7-2 for PMIP-based S2a:

0. The UE is connected in the 3GPP Access and has a GTP or PMIP tunnel on the S5/S8 interface.

1. The UE creates a WLAN virtual IP interface corresponding to the APN towards which it desires to handover a PDN connection.

2. The UE requests handover of the PDN connection from the 3GPP access to this WLAN virtual interface by sending a DHCP and/or DHCPv6 request message from this WLAN virtual interface that contains a handover indication for the PDN connection. The handover indication consists of requesting allocation of the same IPV4 address than previously allocated for the PDN connection over the 3GPP access, or of an IPv6 address within the same IPv6 prefix than previously allocated for the PDN connection over the 3GPP access. The DHCP requests are transmitted over the virtual point-to-point link negotiated during authentication phase, i.e., the layer 2 frame carrying the DHCP is marked with the corresponding VLAN Id, or unicasted to the corresponding TWAG MAC address, or encapsulated with the corresponding GRE key.

NOTE: The UE is not required to request re-allocation of all addresses it had previously been allocated over the 3GPP access; a single request for one of the addresses that were used over the 3GPP access is enough to signal a handover indication to the TWAG. The UE may however request allocation for as many addresses as it wishes. Hence for an IPv4v6 PDN connection the handover indication signalling may be based entirely on DHCPv4 with no use of DHCPv6. If that is the case the UE may configure with Stateless Address Autoconfiguration the same IPv6 address than previously allocated with Stateless Address Autoconfiguration for the PDN connection over the 3GPP access based on receiving from the TWAG the same IPv6 prefix in a router advertisement.

3. When the TWAG receives the first DHCP IPv4 and/or IPv6 address allocation request with a handover indication over the virtual point-to-point link corresponding to a specific APN, it request the PDN GW handover of the corresponding GTP or PMIP tunnel for the PDN connection to that APN. This is done by sending a Create Session Request or Proxy Binding Update with the handover indication for each of the PDN connections to the

same APN. In case of multiple PDN connections to a same APN, the steps 3-5 in (A) shall be repeated for each PDN connection to the same APN that is being transferred from 3GPP access to Trusted WLAN access. The steps in (A) can occur in parallel for each PDN connection..

4. The PDN GW initiates the IP-CAN Session Modification Procedure with the PCRF, as specified in TS 23.203 [4].

5. The selected PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12.

6. The PDN GW returns a Create Session Response or a Proxy Binding Update message to the TWAG, including the IPv4 and/or IPv6 address(es) allocated for the UE.

7. The GTP or PMIP tunnel is set up between the TWAN and the PDN GW.

8. The TWAG then sends a DHCP reply to the UE with the IPv4 address and/or IPv6 address as re-allocated by the PDN GW. The UE can then continue to use the PDN connection via the WLAN virtual interface.

8.2.2.1.8 Handover from Trusted WLAN Access to 3GPP Access

This procedure is as described in clause 8.2.1.3 of TS 23.402 [3] for GTP-based S5/S8, with the difference that there is a GTP tunnel instead of a PMIP tunnel in step 1 in case of GTP-based S2a, and that the resource allocation deactivation procedure initiated by the PDN GW in step 17 is as defined in clause 16.4 of TS 23.402 [3], followed by the additional step of the UE then deleting the virtual IP interface for the virtual point-to-point link corresponding the PDN connection.

8.2.2.2 Impacts on existing nodes or functionality

The UE shall support:

- Creation and deletion of per-PDN/NSWO WLAN virtual interfaces for the chosen user plane multiplexing scheme (VLAN, or unicast L2)

- For IPv4 PDN connections: stateful address configuration mechanisms DHCP, DHCP Forcerenew, DHCP Forcerenew Nonce Authentication.

- For IPv4v6 PDN connections: stateful address configuration mechanisms DHCP, DHCP Forcerenew, DHCP Forcerenew Nonce Authentication, and/or DHCPv6.

- For IPv6 PDN connections: stateful address configuration mechanism DHCPv6

- Enhanced EAP-AKA' method for negotiation of SaMOG phase 2 capabilities with the UE, and discovery of per-PDN user plane multiplexing identifier (VLAN Id, or TWAG MAC address)

The TWAN shall support:

- Creation and deletion of per-PDN/NSWO WLAN virtual interfaces for the chosen user plane multiplexing scheme (VLAN Id, or TWAG MAC address)

- For IPv4 PDN connections: stateful address configuration mechanisms DHCP, DHCP Forcerenew, DHCP Forcerenew Nonce Authentication.

- For IPv4v6 PDN connections: stateful address configuration mechanisms DHCP, DHCP Forcerenew, DHCP Forcerenew Nonce Authentication, and/or DHCPv6.

- For IPv6 PDN connections: stateful address configuration mechanism DHCPv6

- Additional AVP for negotiation of SaMOG phase 2 capabilities with the AAA server, and discovery of per-PDN user plane multiplexing identifier (VLAN Id, or TWAG MAC address)

The AAA server shall support:

- Additional AVP for negotiation of SaMOG phase 2 capabilities with the TWAN, and discovery of per-PDN user plane multiplexing identifier (VLAN Id, or TWAG MAC address)

- Enhanced EAP-AKA' method for negotiation of SaMOG phase 2 capabilities with the UE, and discovery of per-PDN user plane multiplexing identifier (VLAN Id, or TWAG MAC address)

8.2.2.3 Evaluation

The following aspects are considered and evaluated for the solution:

i) Impacts to existing network deployment:

a) There is no requirement for WLAN APs compared to Rel-11.

b) The TWAG shall support the point-to-point link multiplexing, the EAP-AKA enhancements, and the binding of an IPv4 and/or IPv6 session(s) for stateful address configuration with a PDN connection.

ii) Impacts to UE:

a) The UE shall support the point-to-point link multiplexing, the AAA enhancements, and the binding of an IPv4 and/or IPv6 session(s) for stateful address configuration with a PDN connection.

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA'):

The following protocols are extended:

a) EAP-AKA is extended with UE network capability negotiation and PDN point-to-point link management (APN, PDN type, point-to-point link identifiers)

b) STa protocol is extended with UE network capability negotiation and PDN point-to-point link management (APN, PDN type, point-to-point link identifiers).

iv) Impacts to protocols defined by other SDOs (e.g. DHCP):

No impact on other SDOs.

v) Control plane

a) The latency/load of first PDN connection is as for phase 1 SaMOG, i.e., EAP-AKA based authentication and IP layer address configuration. The latency/load of additional PDN connections is less as it only requires IP layer configuration.

b) There is impact on the AAA server as it needs to be enhanced with the EAP-AKA extensions and the STa extensions.

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements:

a) Co-existence with Rel-11 SaMOG

b) Support for IP address preservation during handover

c) Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDN connections

vii) Other functional limitations:

a) Limitation on the number of point-to-point links to specific APNs that can be negotiated - but no different from limit on number of bearers on 3GPP access.

b) Limitation that APNs the UE will connect to have to be known prior to WLAN authentication phase. Were it not the case, connection to an unforeseen APN when the UE is already authenticated to WLAN would require UE to disconnect and reconnect to the WLAN such that the new APN can be negotiated in EAP-AKA authentication. The UE disconnecting and reconnecting from WLAN may cause the UE to release existing PDN connections anchored over the TWAN.

8.2.3 Solution 3: Stateful DHCP-based Solution

8.2.3.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

NOTE: The solution does not support stateless auto-configuration DHCPv6.

8.2.3.1.1 Functional Overview and Overall System Impacts

8.2.3.1.1.1 Overview

The following table summarizes the proposed solution with respect to the Rel-12 SaMOG system requirements.

Table 8.2.3.1.1.1- 1: Solution overview

Requirements		Solution
Co-exist with the SaMOG Release 11 solution	- R12 UE interworks with Rel-11 TWAN and vice versa - R12 TWAN supports both R11 and R12 UEs attaching to the same TWAG - 3GPP AAA updates PDN GW identification to support HO operation for Rel-12 UE	Supports UE Rel-12 capability Indication obtained from EAP-AKA' Based on prior detection of the UE's release version during the capability negotiation, 3GPP AAA determines whether to update PDN GW identification to support HO operation for Rel-12 UE
Multiple simultaneous PDN connections over Trusted WLAN including the simultaneous support Non-seamless WLAN offload (NSWO)	Control Plane	Via DHCP request message to trigger additional PDN connection establishment.
	User Plane compatible with existing PDN connections	- User data for Multiple EPC-routed PDN connections can be separated by GRE tunnel. - Differentiate NSWO traffic from EPC-routed connection(s) without GRE tunnel Supporting NSWO, IPv4, IPv6 and dual-stack as specified in DHCP request and permitted by the 3GPP UE's subscription policy
IP address preservation	Signalling handover indication for IP address preservation to TWAN and the IP address	TWAN determines UE requirement of IP address preservation by special indication in DHCP request message
Signalling the requested APN over Trusted WLAN		UE signals APN using DHCP request message

8.2.3.1.1.2 UE Impacts

For the purpose of accessing a Trusted Non-3GPP WLAN Access, the UE will be modified with the following enhancements with respect to Rel-11 UE:

- Control Plane:
  - Incorporate the requested APN, uplink GRE key, and HO indication in DHCP request message to communicate with TWAN/EPC.
  - Support SAMOG phase 2 capabilities exchange and negotiation with TWAN during the EAP Authentication and Authorization operation.
  - Indicate the desired connectivity service (NSWO access/ PDN connection), and receive the indication via DHCP response message.

  - Support IPv4, IPv6 and dual-stack PDN connection corresponding to the UE's subscription policy with its operator
  - Support hand-over and release specific PDN connection or multiple PDN connections.
  - Set-up and release the NSWO access.
  - Support multiple simultaneous (TWAN) connectivity services i.e. both EPC-routed and NSWO simultaneously.
  - Decide on the unique downlink GRE key for the EPC-routed traffic across all the PDN connections and sent it to TWAN, and also track the uplink GRE key that is assigned by the TWAN
- User Plane:
  - Encapsulate and decapsulate GRE-over-IP tunnel for its EPC-routed PDN connection
  - Simultaneous support for EPC-routed and NSWO traffic

8.2.3.1.1.3 Trusted WLAN Access Gateway Impacts

The Trusted WLAN Access Gateway is enhanced with respect to Rel-11 TWAG with the following functions:

- Control Plane:
  - Support the TWAN side of the operations corresponding to UE's operation as described in clause 8.2.3.1.1.2 above.
  - Binding the PDN connection for S2a GTP/PMIP tunnel.
- User Plane:
  - Enforces routing of packets between the PDN connection and the GTP/PMIP tunnel for that UE.
  - Encapsulate and decapsulate GRE-over-IP tunnel for its EPC-routed PDN connection
  - Simultaneous support for EPC-routed and NSWO traffic

8.2.3.1.1.4 Trusted WLAN Access Point Impacts

None.

8.2.3.1.1.5 Trusted WLAN Backhaul Impacts

Same as SaMOG Rel-11.

8.2.3.1.2 Control Plane Management

8.2.3.1.2.1 UE-Network Capability Negotiation

The UE negotiates SaMOG phase 2 capabilities with its serving TWAN during its EAP Authentication and Authorization operation. The TWAN sends UE requested SaMOG phase 2 capabilities and local TWAN configuration policies (i.e. whether supporting NSWO and/or EPC-routed) to the 3GPP AAA server over STa interface. The 3GPP AAA server takes a decision on whether or not the capabilities may apply to the UE session on the TWAN based on UE's subscription policy and local TWAN policies.

8.2.3.1.2.2 Connection related control plan interface

DHCP protocol is used as the connection related control plane interface between the UE and the TWAG. It is the control plane protocol for UE to trigger the setup/maintain and release of any PDN or NSWO access among multiple connections:

- Allows the UE to set-up (or Handover) and release a specific PDN or multiple PDNs.

- Allows the UE to set-up and release the NSWO access.

NOTE 1: For DHCPv4 Forcerenew message used for releasing an individual PDN, RFC6704 [27] "DHCP Forcerenew nonce authentication" shall be used to provide secure client/server signalling exchange .

NOTE 2: For DHCPv6, RFC 3315 [23] specifies security mechanism to protect client/server signalling exchange .

- Allows the UE to have multiple simultaneous (TWAN) connectivity services.

- Allows the UE to indicate the desired connectivity service (NSWO access/PDN), whether an initial attach or a handover is required, the PDN type, etc.

NOTE 3: 3GPP Vendor-specific Information that has been assigned by IETF for 3GPP for DHCPv4 and DHCPv6 can be used to provide DHCP enhancement as required by this solution. Hence, there is no impact to IETF.

8.2.3.1.3 User plane management

Basic assumption of SaMOG is to have point-to-point underlying transport between the UE and TWAG within the TWAN. However, when emulating multiple S2a PDNs support over TWAN, it is possible that several UE's serving PDN GWs could allocate the same private IP(v4) address to an UE. Hence, a user plane connection identifier is required to support multiplexing multiple PDNs over the point-to-point link between the UE and the TWAG to support TWAN connectivity service i.e. EPC-routed traffic.

In the following two clauses, two alternatives are proposed for the user plane connection identifier.

Editor's note: For which of these two alternatives needs to be chosen is FFS.

8.2.3.1.3.1 Alternative 1: GRE over IP

8.2.3.1.3.1.1 Point-to-point link model and multiple PDN connections support

In this alternative, a unique pair of per-UE based GRE Keys in the uplink and in downlink direction is required for differentiating individual PDN.

As there is no need to manage bearers over the WLAN access, a GRE Key at the user plane interface between the UE and the TWAG, corresponds to an entire PDN. When different GTP-u bearers are used on S2a for a given PDN, it is the same mechanism used in Rel-11 SaMOG to determine the GTP-u bearer to be used to carry a given packet i.e. the usage of UL-TFT at the UE and DL-TFT at the PGW.

NOTE 1: The figures in the following clauses depict the case of a PDN using a single bearer over S2a.

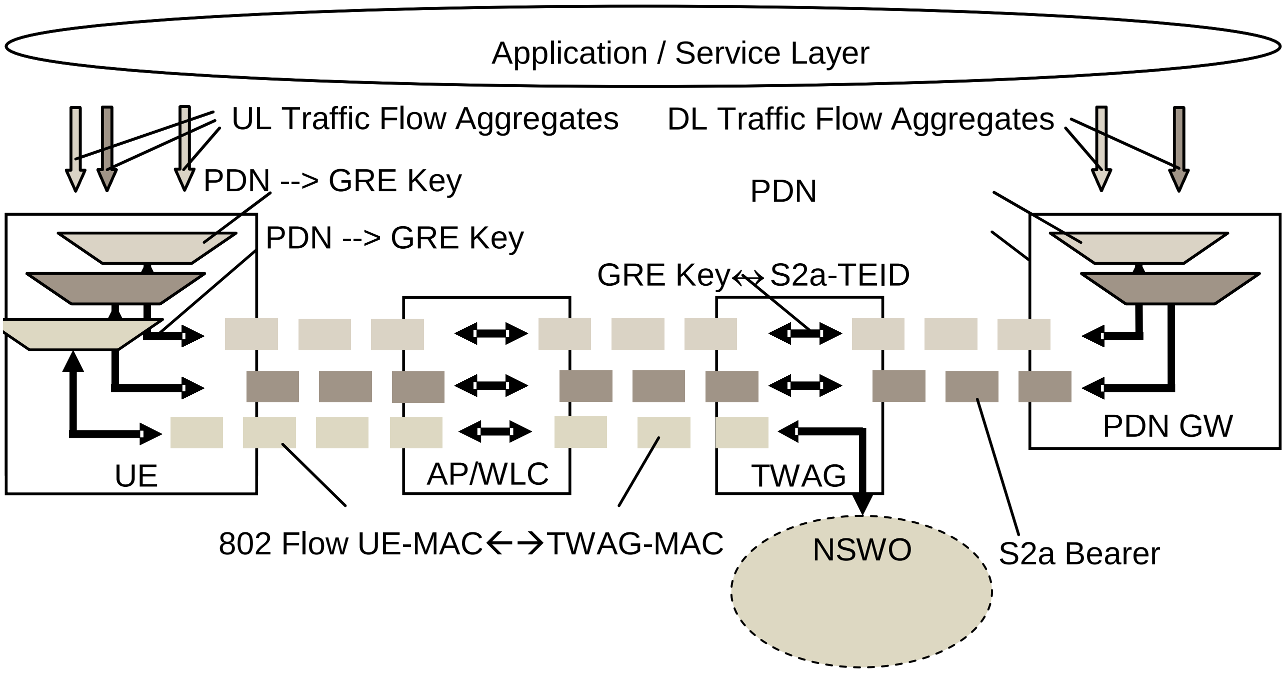

Application / Service Layer
UL Traffic Flow Aggregates
DL Traffic Flow Aggregates
PDN --> GRE Key
PDN
PDN --> GRE Key
GRE Key↔S2a-TEID
UE
AP/WLC
TWAG
PDN GW
802 Flow UE-MAC←→TWAG-MAC
NSWO
S2a Bearer

Figure 8.2.3.1.3.1.1-1: Point-to-point link model for PDN and NSWO access based on distinct GRE Key

As depicted in the Figure 8.2.3.1.3.1.1-1 above, there are separate uplink and downlink GRE Keys. The virtual point-to-point link corresponding to a given connectivity service is realized as enforcing the packet forwarding of uplink and downlink traffic from different PDNs of which the IP packets are identified by specific GRE Key.

The solution described above supports one or multiple PDN(s) corresponding with one or more APN(s).

8.2.3.1.3.1.2 GRE over IP tunnelling establishment

It is assumed that a given 3GPP UE is always hosted by only one TWAG within the TWAN. Both the UE and the TWAG guarantees the uniqueness of GRE Key across all the 3GPP UE's PDNs. Each PDN is identified by both uplink GRE Key and downlink GRE Key.

Figure 8.2.3.1.3.1.2 -1 shows the user data encapsulated in GRE tunnel.

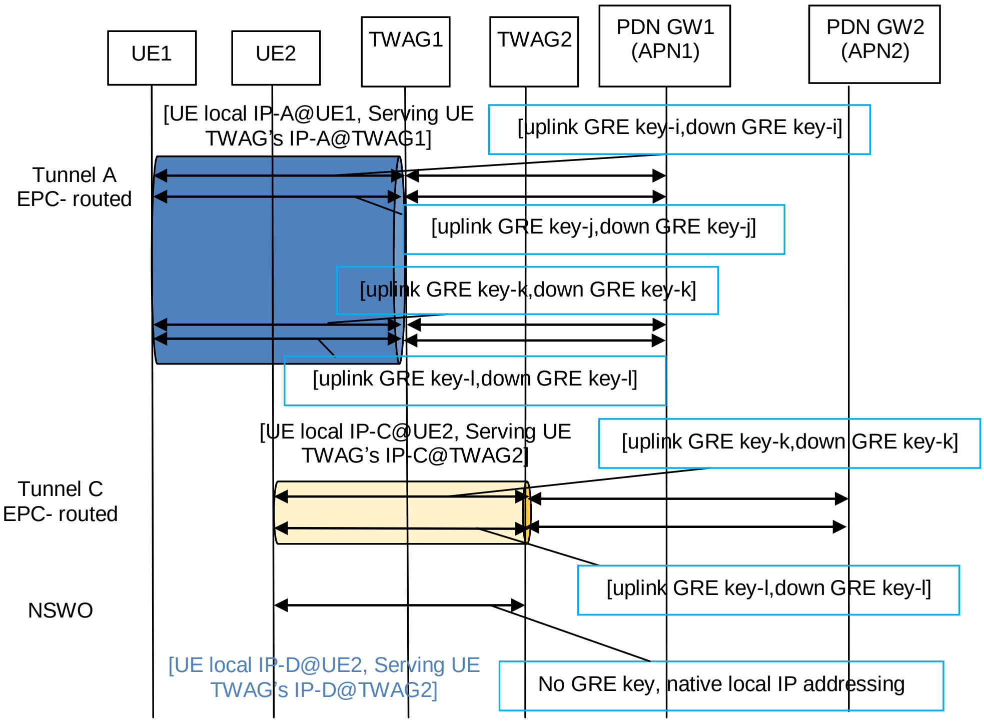

UE1
UE2
TWAG1
TWAG2
PDN GW1 (APN1)
PDN GW2 (APN2)
[UE local IP-A@UE1, Serving UE TWAG's IP-A@TWAG1]
[uplink GRE key-i,down GRE key-i]
Tunnel A EPC- routed
[uplink GRE key-j,down GRE key-j]
[uplink GRE key-k,down GRE key-k]
[uplink GRE key-l,down GRE key-l]
[UE local IP-C@UE2, Serving UE TWAG's IP-C@TWAG2]
[uplink GRE key-k,down GRE key-k]
Tunnel C EPC- routed
[uplink GRE key-l,down GRE key-l]
NSWO
[UE local IP-D@UE2, Serving UE TWAG's IP-D@TWAG2]
No GRE key, native local IP addressing

Figure 8.2.3.1.3.1.2-1: Encapsulation of UE EPC-routed Traffic in GRE Tunnel

8.2.3.1.3.2 Alternative 2: TWAG virtual MAC Address

In this alternative, a TWAG virtual MAC address in the uplink and in downlink direction is required for differentiating individual PDN.

As there is no need to manage bearers over the WLAN access, a TWAG virtual MAC address at the user plane interface between the UE and the TWAG, corresponds to an entire PDN. When different GTP-u bearers are used on S2a for a given PDN, it is the same mechanism used in Rel-11 SaMOG to determine the GTP-u bearer to be used to carry a given packet i.e. the usage of UL-TFT at the UE and DL-TFT at the PGW. On the UL direction, the TWAG uses both the source MAC address and the TWAG virtual MAC address to identify the S2a bearer on which the packet is to be forwarded. Two different UEs served by the same TWAG can share the same TWAG virtual MAC address.

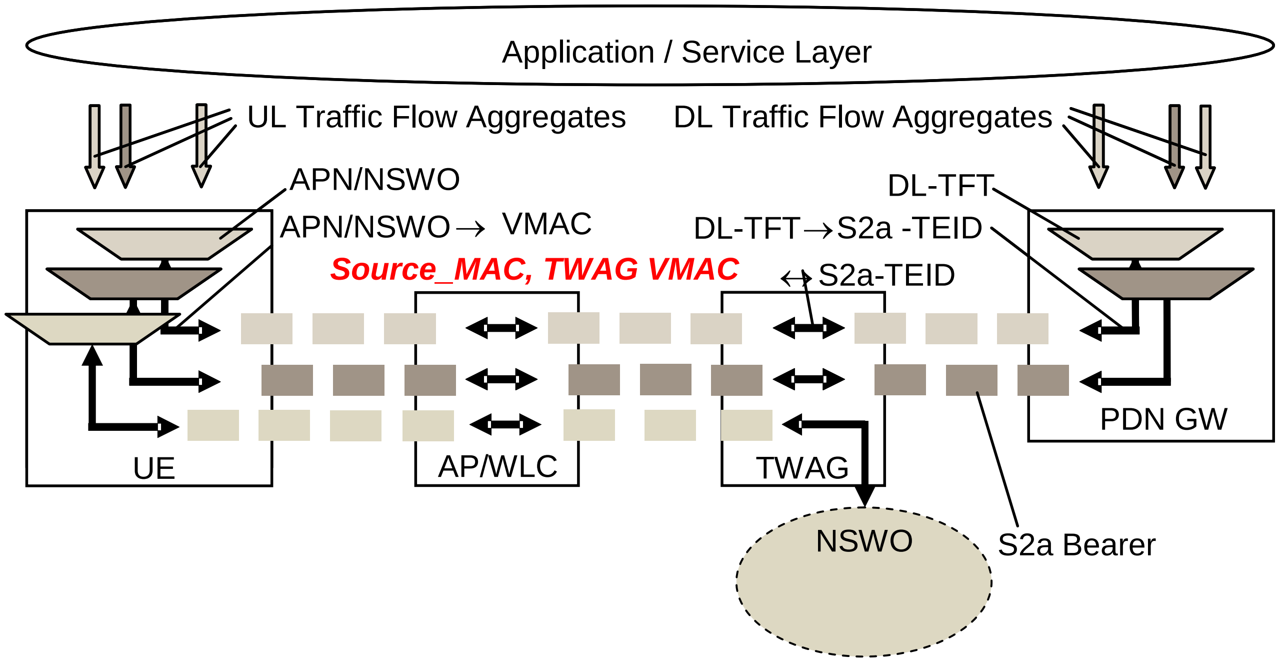


Figure 8.2.3.1.3.2-1: Point-to-point link model for PDN and NSWO access based on TWAG VMAC

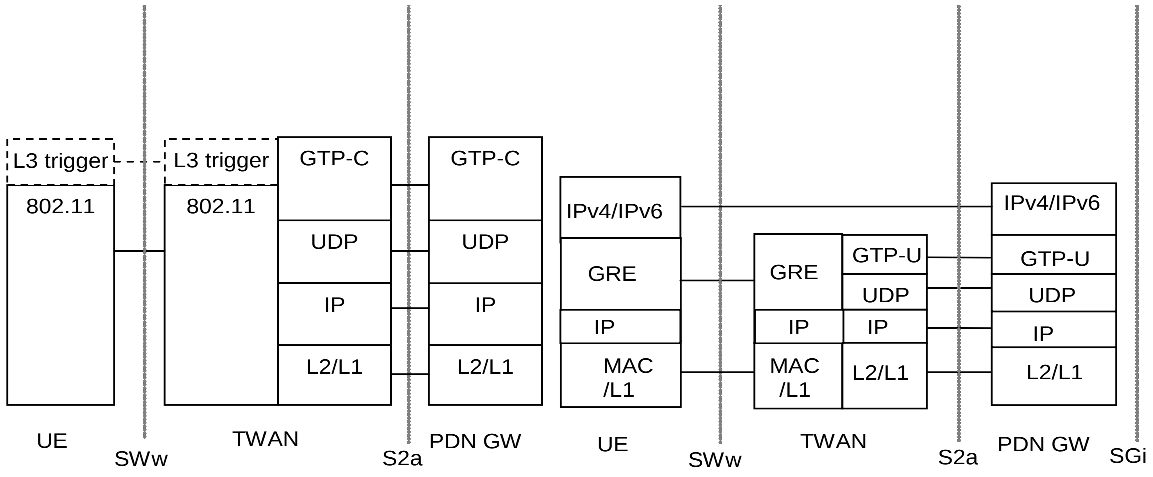
8.2.3.1.4 Protocol stack

The following mobility protocols are supported over S2a:

- GTP.
- PMIPv6.

The link model as well as IPv4 address and IPv6 prefix allocation considerations are equally valid for GTP and PMIPv6 S2a options.

The figure below illustrates the control plane for Tunnel Management and the user plane for GTP option.



Control Plane for Tunnel Management **User Plane for Tunnel Management**

Legend:

802.11: This refers to Layer 1 and Layer 2 defined by IEEE Std 802.11-2007 [5].

L3 trigger: This refers to DHCPv4/DHCPv6 which is used as mandatory attach trigger.

GRE: The GPE tunnels user data between UE and the Trusted WLAN Access Gateway over the SWw interface, which identifies specific the data per PDN connection by different GRE key.

GTP-C: The GPRS Tunnelling Protocol control plane consists of signalling messages between the Trusted WLAN Access Gateway and the PDN- GW over the S2a interface. It is defined in TS 29.274 [25].

GTP-U: The GPRS Tunnelling Protocol user plane tunnels user data between the Trusted WLAN Access Gateway and the PDN GW over the S2a interface. It is defined in TS 29.281 [26].

UDP: This is the transport layer protocol onto which both GTP-C and GTP-U are layered.

Figure 8.2.3.1.4-1: Link Model for GTP-based S2a

When PMIP based S2a is used with Trusted WLAN, the PMIPv6 protocol stacks described in TS 23.402 [3] clause 6.1.1 apply.

8.2.3.1.5 IP addressing support for SaMOG phase-2

This clause describes the IP addressing support for SaMOG phase-2 based on the stateful DHCP-based solution. The main scenarios for IP address/prefix assignment to UE are:

a) The IP address allocated by TWAN which is used for NSWO access

b) The IP address allocated by TWAN for GRE over IP tunnelling the EPC routed traffic,

c) The IPv4 address/IPv6 prefix allocated by PGW which is used for EPC routed.

8.2.3.1.5.1 IP address assignment for NSWO

If the requested connectivity is for NSWO and the NSWO connectivity is allowed by the user subscription, the TWAN shall assign a NSWO IP address or prefix via DHCPv4 or DHCPv6 procedures.

8.2.3.1.5.2 IP address assignment for GRE over IP tunnel

In the case when additional PDN connection is requested, and the multiple PDN connectivity is allowed, the TWAN shall assign the tunnel IP address via DHCPv4 if TWAN support IPv4; otherwise, the TWAN supports IPv6, the UE may generate link local address to be used for GRE over IP tunnelling.

8.2.3.1.5.3 IP address assignment for EPC-routed

The IPv4 address and/or IPv6 prefix is allocated to the UE by PDN GW or external PDN when a new PDN connection is established. In order to enable IPv4 or IPv6 connectivity, the TWAN shall support DHCPv4 and DHCPv6 server functionality for IP parameter configuration and IPv4 address and/or IPv6 prefix allocation as specified in IETF RFC 2131 [9] and IETF RFC 3315 [23].

The way that the UE sets the requested PDN type is as specified in clause 5.3.1.1 of TS 23.401 [6].

The following IP address allocation procedure applies to the following conditions accordingly:

- If the requested PDN type is allowed by the user subscription, the TWAN requests the PDN connectivity towards EPC as requested.

- If the requested PDN type is IPv4v6, but the subscription data allows only PDN type IPv4 or only PDN type IPv6, the TWAN requests IPv4 address or IPv6 prefix in the Proxy Binding Update or GTP Create Session Request from the PDN GW according to the subscribed value. The TWAN shall return the assigned PDN type to the UE. In this case the UE shall not request another PDN connection to the same APN for the other IP version. The IPv4 address or IPv6 prefix is delivered to the TWAN during the PMIPv6 or GTP tunnel establishment.

  a). When the UE requests the IPv4 address via DHCPv4, and if the subscription data allows PDN type IPv4, the TWAN delivers the received IPv4 address to the UE within DHCPv4 signalling after the PMIPv6 or GTP tunnel is established between the TWAN and the PDN GW. Otherwise, the subscription data allows only PDN type IPv6, TWAN will reject the request with a cause value that PDN type IPv6 only.

  b). When the UE requests the IPv6 prefix via DHCPv6, and if the subscription data allows PDN type IPv6, the TWAN delivers the received IPv6 address to the UE within DHCPv6 signalling after the PMIPv6 or GTP tunnel is established between the TWAN and the PDN GW. Otherwise, the subscription data allows only PDN type IPv4, TWAN will reject the request with a cause value that PDN type IPv4 only.

- If the requested PDN type is IPv4 or IPv6, and if either the requested PDN type or PDN type IPv4v6 are subscribed, the TWAN requested the PDN connectivity from the PDN GW as requested. Otherwise the requested PDN connection request is rejected with the appropriate cause value.

- If the requested PDN type is IPv4v6, and both IPv4 and IPv6 PDN types are allowed by subscription but not IPv4v6, the TWAN shall decide for which the PDN type that it will request and such decision is operator's implementation decision.

8.2.3.2 Procedures

Editor's note: The call flows are described in this clause.

8.2.3.2.1 Initial Attach in WLAN on S2a

8.2.3.2.1.1 Initial Attach in WLAN on GTP/PMIP S2a

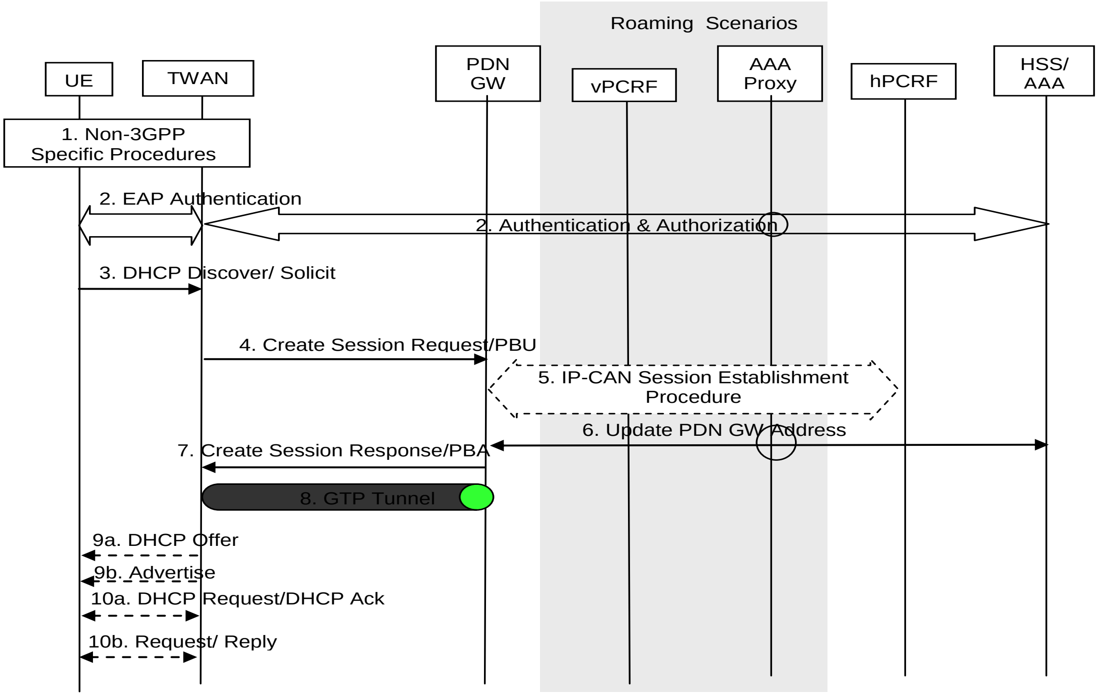

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. DHCP Discover/ Solicit
4. Create Session Request/PBU
5. IP-CAN Session Establishment Procedure
6. Update PDN GW Address
7. Create Session Response/PBA
8. GTP Tunnel
9a. DHCP Offer
9b. Advertise
10a. DHCP Request/DHCP Ack
10b. Request/ Reply

Figure 8.2.3.2.1.1-1: Initial attachment in WLAN on GTP/PMIP S2a for roaming, LBO and non-roaming scenarios

The scenario is defined as the TWAN using the layer 3 attach request, including a DHCPv4 or DHCPv6 message, sent by the UE as the attach trigger.

1. The step is same as step 1 in TS 23.402 [3] clause 16.2.1.

2. In this step, the UE indicates its capability (i.e. Rel-12 SaMOG capability) to the AAA server during the authentication procedure. Based on the UE capability provided by AAA server, the TWAN decides to use L3 trigger.

3. The UE shall send a DHCPv4 Discover as per IETF RFC 2131 [9], or DHCPv6 Solicit as per IETF RFC 3315[23] to TWAN, including the following information:

   - The requested APN

   - An indication on the requested access (EPC via S2a access or the use of NSWO access)

   - And in the former case, an APN optionally.

   - For alternative 1, downlink GRE key may be inserted in 3GPP Vendor Specific information for IPv4, IPv6 or IPv4v6 connection.

   - Requested PDN type - one of IPv4, IPv6 or IPv4v6

   Based on HSS/AAA authorization and the received UE EPC/NSWO access indication whether or not to establish S2a, TWAN can decide to allow EPC access or not. All the UE traffic through the TWAG is blocked unless the UE is granted NSWO/PDN access. The following steps 4-8 proceed according to the considerations below.

   If UE doesn't provide an APN to TWAN, then:

   A. If the TWAN decides NSWO access, steps 4-8 below are skipped. Instead, the TWAN assigns an IPv4 address and/or IPv6 address from its local address pool to the UE (depending on the L3 attach request in step 3) and the NSWO traffic will be forwarded/received without traversing EPC.

B. If the TWAN decides S2a access, the TWAN assigns an IPv4 address and/or IPv6 address from its local address pool to the UE (depending on the L3 attach request in step 3). The TWAN shall request to PDN GW for an IPv4 address and/or IPv6 address and PDN GW shall return an IPv4 address and/or IPv6 address to the TWAN during steps 4-8.

If UE provides its requested APN to TWAN, and the TWAN determines that S2a shall be established, the TWAN assigns an IPv4 address and/or IPv6 address from its local address pool to the UE (depending on the L3 attach request in step 3). The TWAN proceeds according to steps 4-8 below.

4. TWAN decides PDN type according to requested PDN type and subscribed PDN type from HSS, and sets the Dual Address Bearer Flag when the PDN type is set to IPv4v6. The TWAN sends a Create Session Request/PBU message to the PDN GW, including PDN type, Dual Address Bearer Flag.

5. The step is same as step 10 in TS 23.402 [3] clause 16.2.1.

6. The 3GPP AAA Server decides whether or not to update PDN GW identification according to the UE capability, which has been provided at the authentication phase. If the UE supports IP address preservation, the 3GPP AAA Server shall update PDN GW identity towards the HSS.

7-8. These steps are the same as steps 6-7 in TS 23.402 [3] clause 16.2.1. If Dual Address Bearer Flag is set, the PDN GW shall return IPv4 address and IPv6 address to TWAN.

9a. For DHCPv4, TWAN returns DHCP offer message to UE, TWAG virtual MAC address is included if alternative 2 is used.

9b. For DHCPv6, TWAN returns Advertise message to UE, TWAG virtual MAC address is included if alternative 2 is used.

10a. UE sends DHCP Request (for DHCPv4) to TWAN, and TWAN returns DHCP Ack message to the UE, including the indication on whether EPC access or NSWO access has been granted to the UE and UE IP allocated by PDN GW.

(a) Alternative 1: For EPC access, GRE tunnelling information is included to UE, where GRE tunnel information includes uplink GRE key and UE's local IP address which are allocated by TWAN for tunnelling data for the given PDN. For NSWO, GRE tunnelling information isn't required.

(b) Alternative 2: Both UE and TWAN maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address. For NSWO, no dedicated virtual MAC address is needed.

All NSWO traffic and control messages between UE and TWAG use TWAG's MAC address.10b. UE sends Request (for DHCPv6) to TWAN, and TWAN returns Reply message to the UE, including the indication on whether EPC access or NSWO access has been granted to the UE and UE IP allocated by PDN GW.

(a) Alternative 1: For EPC access, GRE tunnelling information is included to UE where GRE tunnel information includes uplink GRE key and UE's local IP address which are allocated by TWAN for tunnelling data for the given PDN. For NSWO, GRE tunnelling information isn't required..

(b) Alternative 2: Both UE and TWAN will maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address. For NSWO, no dedicated virtual MAC address is needed.

All NSWO traffic and control messages between UE and TWAG are using TWAG's MAC address. When PDN type is IPv4, steps 9a and 10a apply.

When PDN type is IPv6, steps 9b and 10b apply.

When PDN type is IPv4v6, there are two subsequent cases:

- **Alternative 1:**

1) If UE requests IPv4 address first, TWAN shall implement steps 9a and 10a and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send solicit message encapsulated by the GRE key which is allocated in step 10a to TWAN, TWAN and UE shall implement steps 9b and 10b which are encapsulated by the GRE key which is allocated in step 10a.

2) If UE requests IPv6 address first, TWAN shall implement steps 9b and 10b and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message encapsulated by the GRE key which is allocated in step 10b to TWAN, TWAN and UE shall implement steps 9a and 10a which are encapsulated by the GRE key which is allocated in step 10b.

- **Alternative 2:**

1) If UE requests IPv4 address first, TWAN shall implement steps 9a and 10a and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send solicit message with TWAG virtual MAC address which is allocated in step 9a to TWAN, TWAN and UE shall implement steps 9b and 10b.

2) If UE requests IPv6 address first, TWAN shall implement steps 9b and 10b and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message with TWAG virtual MAC address which is allocated in step 9b to TWAN, TWAN and UE shall implement steps 9a and 10a.

8.2.3.2.2 UE-initiated Connectivity to Additional PDN

8.2.3.2.2.1 UE-initiated Connectivity to Additional PDN on GTP S2a

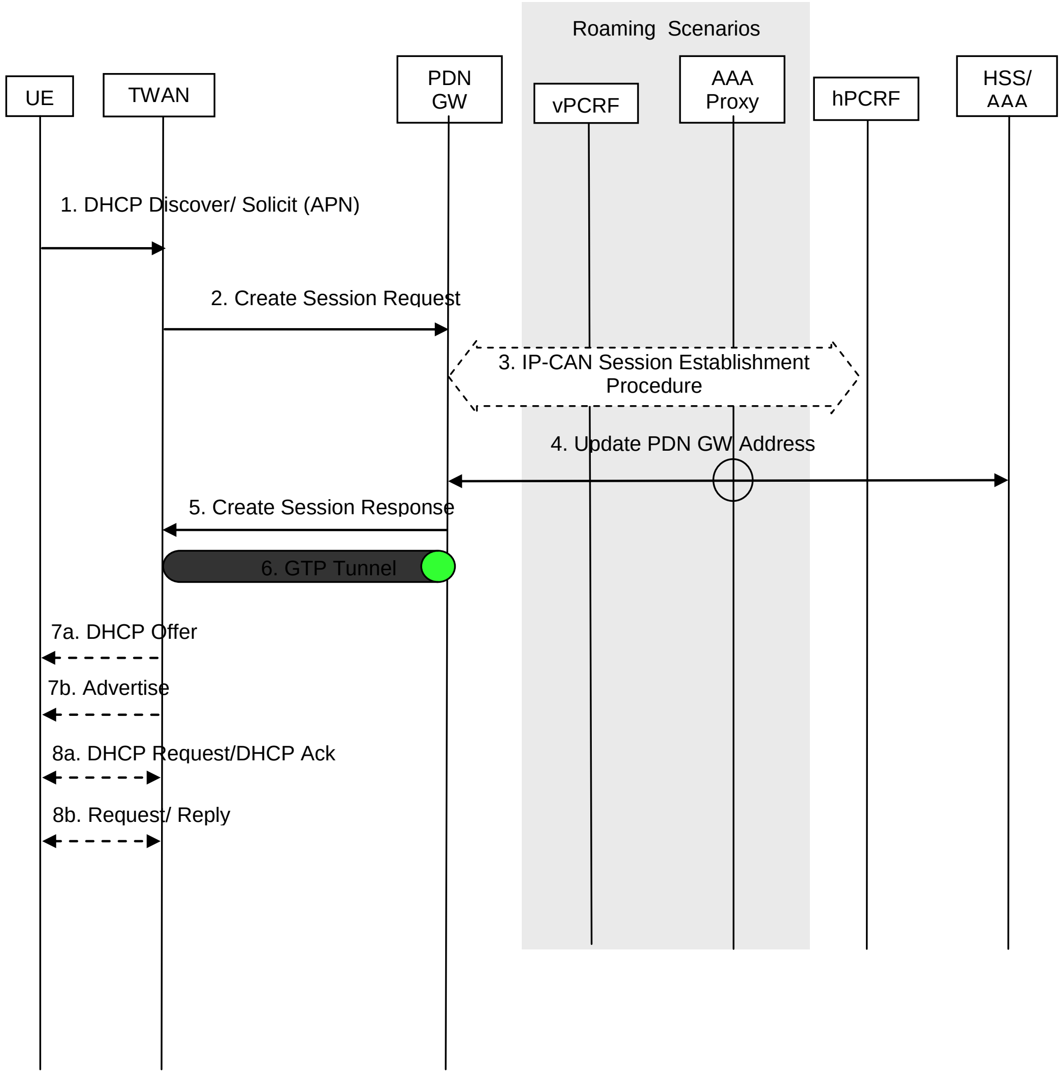

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCP Discover/ Solicit (APN)
2. Create Session Request
3. IP-CAN Session Establishment Procedure
4. Update PDN GW Address
5. Create Session Response
6. GTP Tunnel
7a. DHCP Offer
7b. Advertise
8a. DHCP Request/DHCP Ack
8b. Request/ Reply

Figure 8.2.3.2.2.1-1: UE-initiated connectivity to additional PDN from Trusted WLAN Access with GTP

The scenario is defined as the TWAN using the layer 3 attach request, including DHCPv4 or DHCPv6 message, sent by the UE as the PDN trigger. NSWO is a special PDN.

For DHCPv4 messaging and security handling, RFC 6704 shall be applied.

1. The UE shall send layer 3 attach request to the TWAN, (e.g. a DHCPv4 discover as per IETF RFC 2131 [9], DHCPv6 Solicit as per IETF RFC3315 [23]),including requested APN, requested PDN type and an indication on the requested access (EPC via S2a access or the use of NSWO access), and for alternative 1, the downlink GRE key if EPC via S2a access.

   If UE doesn't send UE requested APN to TWAN, the TWAN determines whether or not to grant NSWO connectivity based on the authorization result during initial attach:

   - If TWAN determines NSWO and there isn't a existing NSWO access, TWAN forwards the traffic without traversing EPC. Otherwise, the NSWO access isn't allowed.
   - If UE provides its requested APN to TWAN, and the TWAN determines that S2a shall be established, the TWAN proceeds according to steps 2-6 below.

2. TWAN decides PDN type according to requested PDN type and subscribed PDN type from HSS, and sets the Dual Address Bearer Flag when the PDN type is set to IPv4v6. The TWAN sends a Create Session Request message to the PDN GW, including PDN type, Dual Address Bearer Flag.

3. The step is same as step 10 in TS 23.402 [3] clause 16.2.1.

4. The 3GPP AAA Server decides whether or not to update PDN GW identification according to the UE capability, which has been provided at the authentication phase. If the UE supports IP address preservation, the 3GPP AAA Server shall update PDN GW identity towards the HSS.

5-6. These steps are the same as steps 6-7 in TS 23.402 [3] clause 16.2.1. If Dual Address Bearer Flag is set, the PDN GW shall return both IPv4 address and IPv6 address to TWAN.

7a. For DHCPv4, TWAN returns DHCP offer message to UE, TWAG virtual MAC address is included if alternative 2 is used.

7b. For DHCPv6, TWAG returns Advertise message to UE, TWAG virtual MAC address is included if alternative 2 is used.

8a. UE sends DHCP Request (for DHCPv4) to TWAN, and TWAN returns DHCP Ack message to the UE, including the indication on whether EPC access or NSWO access has been granted to the UE and UE's IP allocated by its serving PDN GW.

   1) Alternative 1: For EPC access, GRE tunnelling information included to UE where GRE tunnel information includes uplink GRE key allocated by TWAN for tunnelling data for the given PDN. For NSWO, GRE tunnelling information isn't required.

   2) Alternative 2: Both UE and TWAN maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address. For NSWO, no dedicated virtual MAC is needed.

   All NSWO traffic and control messages between UE and TWAG are using TWAG's MAC address.

8b. UE sends Request (for DHCPv6) to TWAN, and TWAN returns Reply message to the UE, including the indication on whether EPC access or NSWO access has been granted to the UE and UE's IP address allocated by its serving PDN GW.

   1) Alternative 1: For EPC access, GRE tunnelling information and UE's IP address allocated by its serving PDN GW are included to UE where GRE tunnel information includes uplink GRE key which is allocated by TWAN for tunnelling support in the case of multiple PDNs. For NSWO, GRE tunnelling information isn't required.

   2) Alternative 2: Both UE and TWAN maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address etc.. For NSWO, no dedicated virtual MAC address is needed.

   All NSWO traffic and control messages between UE and TWAG are using TWAG's MAC address.

   When PDN type is IPv4, steps 7a and 8a apply.

   When PDN type is IPv6, steps 7b and 8b apply.

   When PDN type is IPv4v6, there are two following cases:

- **Alternative 1:**

  1) If UE requests IPv4 address first, TWAN shall implement steps 7a and 8a and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send solicit message encapsulated by the GRE key which is allocated in step 8a to TWAN, TWAN and UE shall implement steps 7b and 8b which are encapsulated by the GRE key which is allocated in step 8a.

  2) If UE requests IPv6 address first, TWAN shall implement steps 7b and 8b and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message encapsulated by the GRE key which is allocated in step 8b to TWAN, TWAN and UE shall implement steps 7a and 8a which are encapsulated by the GRE key which is allocated in step8b.

- **Alternative 2:**

  1) If UE requests IPv4 address first, TWAN shall implement steps 9a and 10a and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send solicit message with TWAG virtual MAC address which is allocated in step 9a to TWAN, TWAN and UE shall implement steps 9b and 10b.

  2) If UE requests IPv6 address first, TWAN shall implement steps 9b and 10b and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message with TWAG virtual MAC address which is allocated in step 9b to TWAN, TWAN and UE shall implement steps 9a and 10a.

8.2.3.2.2.2 UE-initiated Connectivity to Additional PDN on PMIP S2a

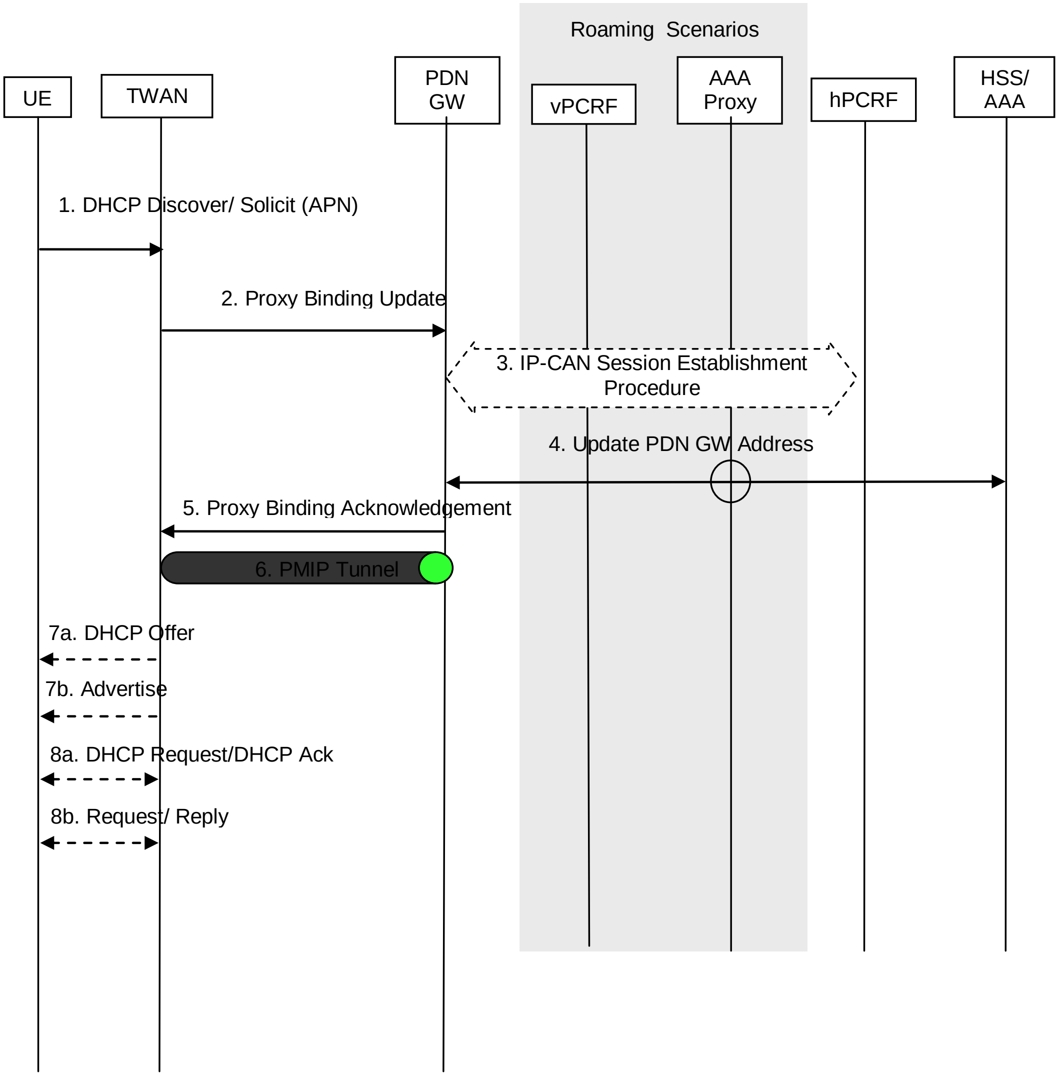


Figure 8.2.3.2.2.2-1: UE-initiated connectivity to additional PDN from Trusted WLAN Access with PMIP

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.2.1 above, with the following differences:

- Step 2 is a Proxy Binding Update. The parameters in the Proxy Binding Update message are same as step 5 in clause 8.2.3.2.2.1.
- Step 5 is a Proxy Binding Acknowledgement. The parameters in t he Proxy Binding Acknowledgement message are same as step 6 in clause 8.2.3.2.2.1.

8.2.3.2.3 Detach and PDN disconnection in WLAN on S2a

8.2.3.2.3.1 Detach and PDN disconnection in WLAN on GTP S2a

8.2.3.2.3.1.1 UE/TWAN requested single PDN Disconnection Procedure in WLAN on GTP S2a

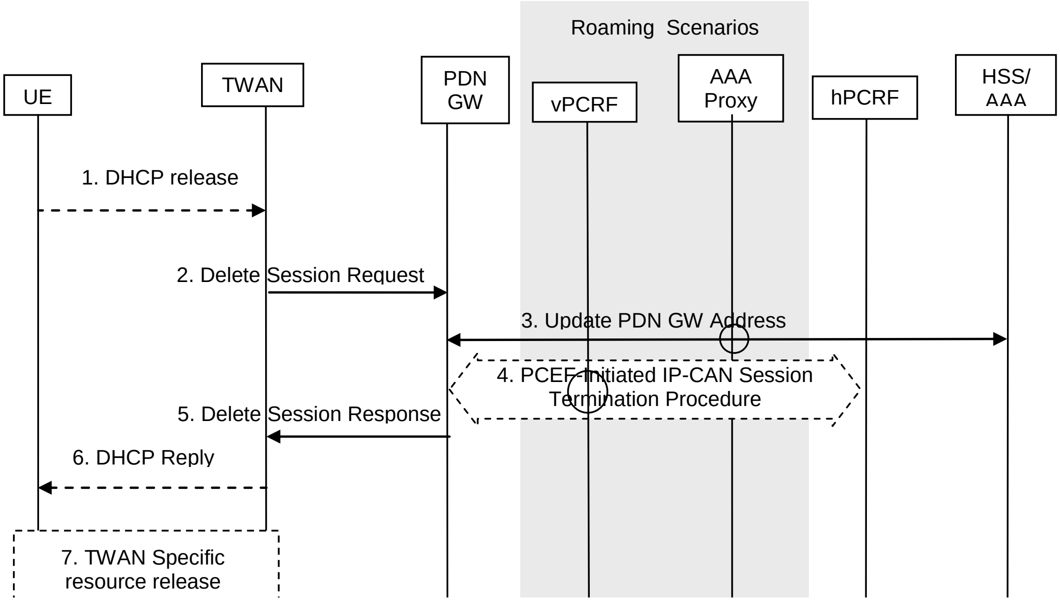

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCP release
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. DHCP Reply
7. TWAN Specific resource release

Figure 8.2.3.2.3.1.1-1: UE/ TWAN requested single PDN Disconnection on GTP S2a

1. If the PDN Type is IPv4, UE releases the IPv4 address using DHCPv4 release message or IPv4 address lease time expires in TS 23.402 [3] clause 16.3. And if the PDN Type is IPv6, UE releases the IPv6 address using DHCPv6 release message or IPv6 address lease time expires. If the PDN Type is IPv4v6, UE shall releases the IPv4 address and IPv6 address by the first DHCP release session, i.e. DHCPv4 release message or DHCPv6 release message, with PDN Type for IPv4v6 is included in the message.

   - **Alternative 1:**

     For DHCPv4 release message, a specific GRE key or a client id is used for identifying specific PDN.

     For DHCPv6 release message, a specific GRE key or IAID is used for identifying specific PDN.

   - **Alternative 2:**

     For DHCPv4 release message, TWAG virtual MAC address is used for identifying specific PDN.

     For DHCPv6 release message, TWAG virtual MAC address is used for identifying specific PDN.

     If there is no traffic received from the UE for a configurable duration and the TWAN detects the UE has left based on unanswered probes (e.g., ARP Request, Neighbour Solicitation message), the TWAN triggers PDN disconnection.

2-5. After TWAN receives DHCP release message, it shall detect if the PDN supports IPv4v6 dual stack and PDN type for IPv4v6 is included in the message. If so, TWAN shall send delete session request message to PDN GW, in order to indicate PDN GW for deleting the PDN. Steps 3-5 are same as the steps 2-5 in TS 23.402 [3] clause 16.3.1.1.

6. TWAN shall remove the associated contexts corresponding to specific PDN, and send Reply message to inform UE of removing associated contexts in the case of DHCPv6.

7. If TWAN requested Single PDN Disconnection, TWAN shall send a DHCPv4 FORCERENEW message as per IETF RFC 3203 [24] and RFC6704[27], and/or DHCPv6 Reconfigure message as per IETF RFC 3315 [23]. When the UE proceeds with renewing the address lease for single PDN, the TWAN shall in turn refuse the request and notify to the UE that the PDN has been disconnected.

NOTE: For PDN type is IPv4v6, it is FFS.

8.2.3.2.3.1.2 UE/TWAN requested one IPv4 Address or one IPv6 address release for a dual stack PDN in WLAN on GTP S2a

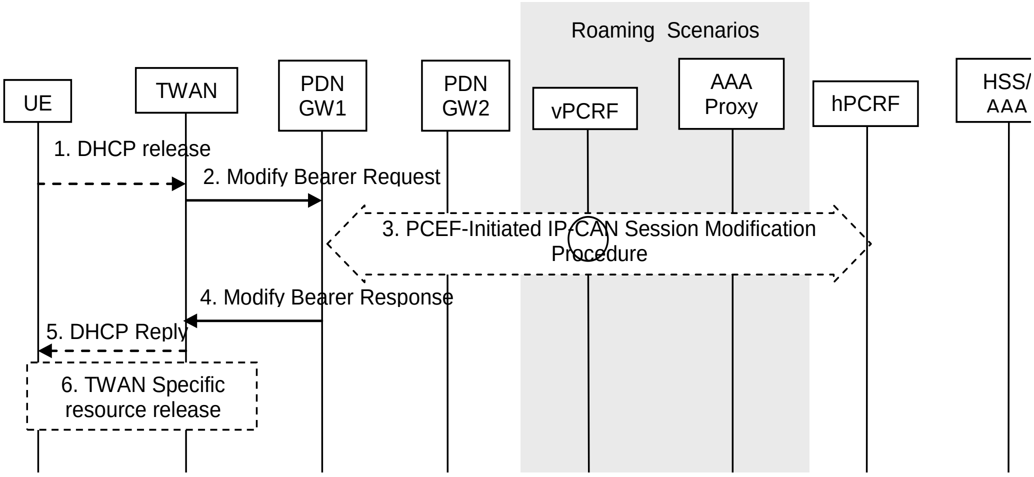


Figure 8.2.3.2.3.1.2-1: UE/ TWAN initiated release for one IPv4 Address or one IPv6 Address for dual stack PDN in WLAN on GTP S2a

When the PDN Type is IPv4v6, UE shall release the IPv4 address using DHCPv4 release message or IPv4 address lease time expires in TS 23.402 [3] clause 16.3, and release the IPv6 address using DHCPv6 release message or IPv6 address lease time expires separately.

The scenario applies that UE/TWAN deletes one IPv4 address or one IPv6 address for a Dual Stack PDN first, and subsequently, UE/TWAN deletes the PDN.

1. UE sends DHCPv4 release message to TWAN if UE releases IPv4 address first, including PDN Type for IPv4.

   - **Alternative 1:**

     Specific GRE key or client id is used for identifying specific PDN to be deleted, and TWAN can detect that only IPv4 address shall be deleted according to PDN Type for IPv4 in DHCPv4 release message.

     UE sends DHCPv6 release message to TWAN, specific GRE key or IAID is used for identifying specific PDN to be deleted, if UE releases IPv6 address first.

   - **Alternative 2:**

     TWAG virtual MAC address is used for identifying specific PDN to be deleted, and TWAN can detect that only IPv4 address shall be deleted according to PDN Type for IPv4 in DHCPv4 release message.

     UE sends DHCPv6 release message to TWAN, TWAG virtual MAC address is used for identifying specific PDN to be deleted, if UE releases IPv6 address first.

2. In case that TWAN receives DHCPv4 release message, then, IP type is IPv4 and TWAN indicates PDN GW for deleting IPv4 address from the PDN. In case that TWAN receives DHCPv6 release message, then, IP type is IPv6 and TWAN indicates PDN GW for deleting IPv6 address from the PDN.

   If TWAN requested IP release, TWAN decides the order of deleting IPv4 address and IPv6 address, If TWAN decides to delete IPv4 first, TWAN sets the IP type to be IPv4 and indicates PDN GW for deleting IPv4 address from the PDN. If TWAN decides to delete IPv6 address first, TWAN sets the IP type to be IPv6 and indicates PDN GW for deleting IPv6 address from the PDN.

TWAN checks there are two associated IPv4 address and IPv6 address for the PDN, and sends modify Bearer Request to PDN GW, including the indication for IP type to be deleted, in order to indicate PDN GW for deleting this type of IP from the PDN.

3. PDN GW initiates the IP-CAN Session Modification Procedure with the PCRF.

4. PDN GW sends modify Bearer response to TWAN.

   If there are multiple bearers corresponding to the PDN, then steps 2-4 are repeated.

5. TWAN shall remove the associated contexts corresponding to specific PDN, send Reply message in the case of DHCPv6, and inform UE of removing associated contexts.

6. If TWAN requested IP release, TWAN shall send a DHCPv4 FORCERENEW message as per IETF RFC 3203 [24] and RFC6704 [27], or DHCPv6 Reconfigure message as per IETF RFC 3315 [23]. When the UE proceeds with renewing the IPv4 address or IPv6 address lease, the TWAN shall in turn refuse to do so, notifying to the UE that the IPv4 address or IPv6 address has been released.

   Subsequently, when UE sends DHCPv6 release (if DHCPv4 release is sent in step 1) or DHCPv4 release (if DHCPv6 release is sent in step 1) message, TWAN shall disconnect the PDN. If TWAN requested IP release, then TWAN shall send delete session request message to PDN GW, in order to disconnect the PDN.

8.2.3.2.3.1.3 UE/TWAN requested Detach Procedure in WLAN on GTP S2a

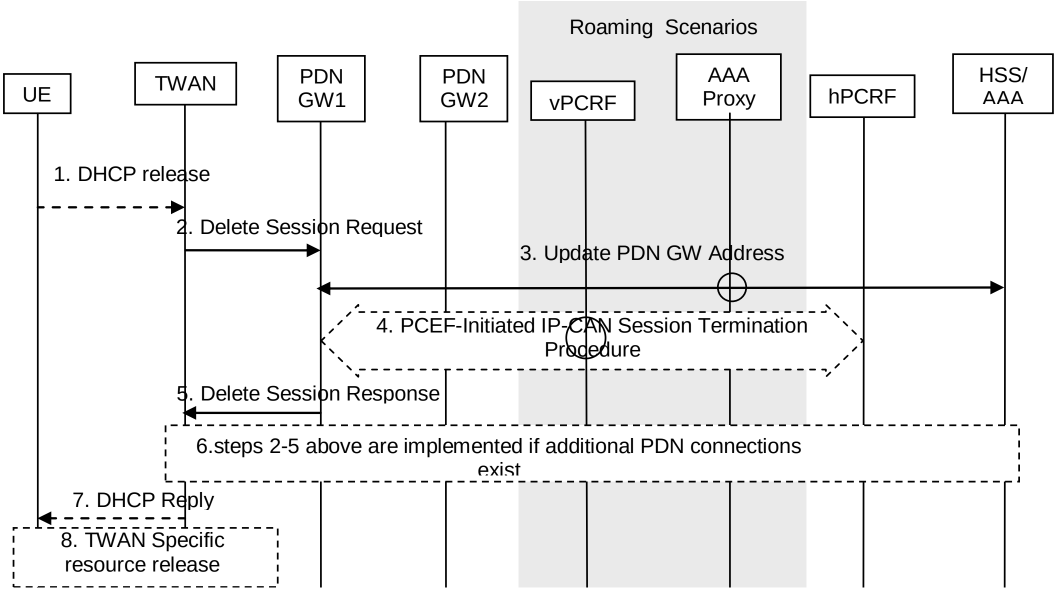

Roaming Scenarios
UE
TWAN
PDN GW1
PDN GW2
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCP release
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6.steps 2-5 above are implemented if additional PDN connections exist
7. DHCP Reply
8. TWAN Specific resource release

Figure 8.2.3.2.3.1.3-1: UE/ TWAN requested Detach on GTP S2a

1. If the PDN Type is IPv4, UE releases the IPv4 address using DHCPv4 release message or IPv4 address lease time expires in TS 23.402 [3] clause 16.3. And if the PDN Type is IPv6, UE releases the IPv6 address using DHCPv6 release message or IPv6 address lease time expires. If the PDN Type is IPv4v6, UE shall releases the IPv4 address and IPv6 address by the first DHCP release session, i.e. DHCPv4 release message or DHCPv6 release message.

   For DHCPv4 release message, the UE MAC address is included in the option of "chaddr". By the option, UE indicates detach to TWAN.

   For DHCPv6 release message, the UE MAC address is included in the option of "client id". By the option, UE indicates detach to TWAN.

2-5. TWAN sends delete Session Request to PDN GW, in order to indicate PDN GW for deleting one PDN. The steps 2-5 are same as steps 2-5 in TS 23.402 [3] clause 16.3.1.1.

6. Repeat steps 2-5 above for remainder PDNs if multiple PDNs are established.

7. TWAN shall de-authenticate and de-associate the UE at layer 2 according to IEEE STD 802.11-207 [5] , send Reply message to UE in the case of DHCPv6 and informing UE of removing associated contexts.

8. If TWAN requested Detach, the TWAN locally removes the UE contexts and de-authenticates and disassociates the UE at Layer 2 according to IEEE Std. 802.11-2007 [5].

8.2.3.2.3.1.4 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a

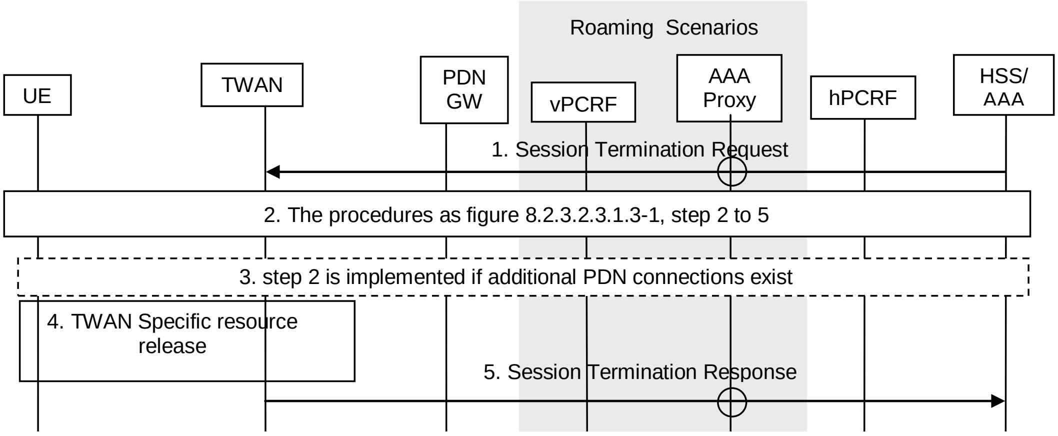

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as figure 8.2.3.2.3.1.3-1, step 2 to 5
3. step 2 is implemented if additional PDN connections exist
4. TWAN Specific resource release
5. Session Termination Response

Figure 8.2.3.2.3.1.4-1: HSS/AAA Initiated Detach on GTP S2a

The procedure for HSS/AAA Initiated Detach from TWAN is represented in Figure 8.2.3.2.3.1.4-1 and described below.

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

1) The HSS/AAA sends a Session Termination Request message to the TWAN to detach a specific UE.

2) The step 2 to 5 of the UE/TWAN Initiated Detach procedure described in clause 8.2.3.2.3.1.3 above are followed.

3) If additional PDNs exist, step 2 is implemented for each PDN.

4) During the step, TWAN shall de-authenticate and de-associate the UE at layer 2 according to IEEE STD 802.11-207 [5], and inform UE to remove the associated contexts.

5) TWAN sends a Session Termination Response message to 3GPP AAA Server, respectively. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2 of TS 23.402 [3]. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3 of TS 23.402 [3].

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the GTP tunnels on S2a, since the TWAN is responsible for removing the GTP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

8.2.3.2.3.2 Detach and PDN disconnection in WLAN on PMIP S2a

8.2.3.2.3.2.1 UE/TWAN requested single PDN Disconnection Procedure in WLAN on PMIP S2a

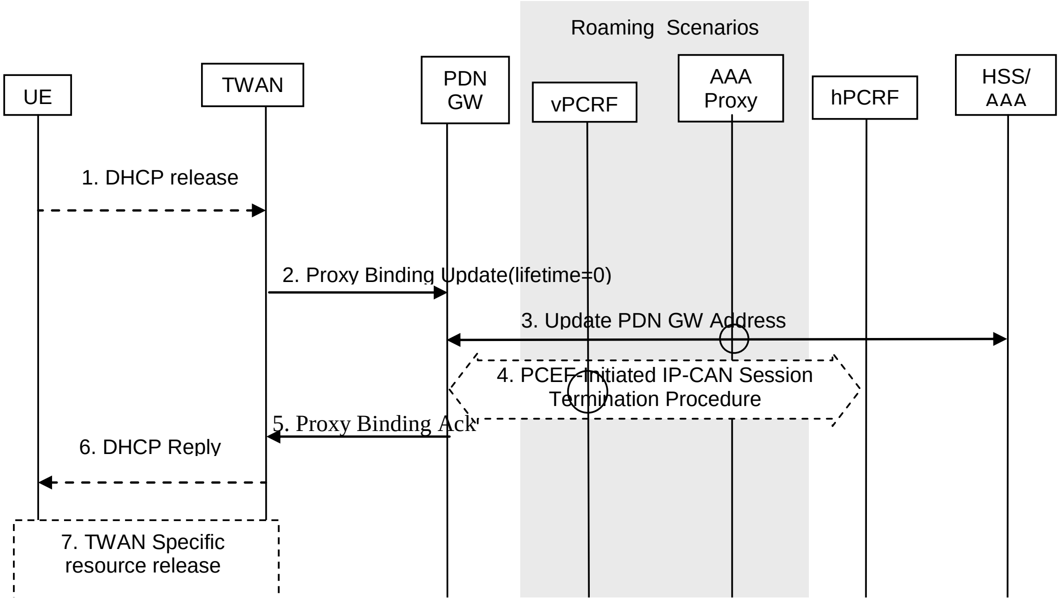


Figure 8.2.3.2.3.2.1-1: UE/ TWAN requested single PDN Disconnection on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.3.1.1, with the following differences:

- Step 2 is a Proxy Binding Update. The parameters in the Proxy Binding Update message are same as step 2 in clause 8.2.3.2.3.1.1.
- Step 5 is a Proxy Binding Acknowledgement. The parameters in the Proxy Binding Acknowledgement message are same as step 5 in clause 8.2.3.2.3.1.1.

8.2.3.2.3.2.2 UE/TWAN requested multiple PDN Disconnection Procedure in WLAN on PMIP S2a

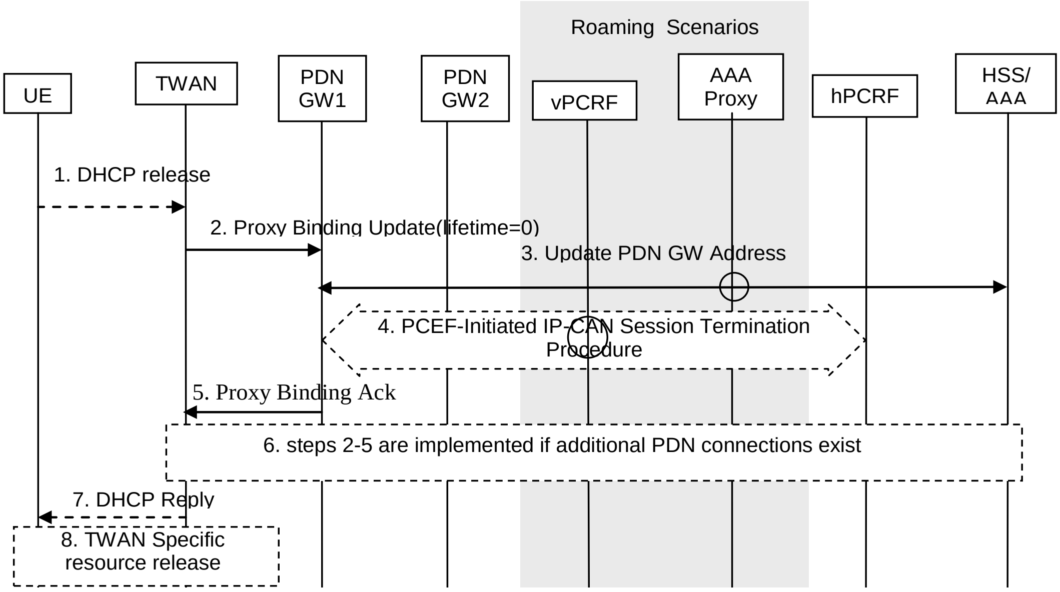

Roaming Scenarios
UE
TWAN
PDN GW1
PDN GW2
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCP release
2. Proxy Binding Update(lifetime=0)
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Proxy Binding Ack
6. steps 2-5 are implemented if additional PDN connections exist
7. DHCP Reply
8. TWAN Specific resource release

Figure 8.2.3.2.3.2.2-1: UE/ TWAN requested multiple PDN Disconnection on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.3.1.2, with the following differences:

- Step 2 is a Proxy Binding Update. The parameters in the Proxy Binding Update message are same as step 2 in clause 8.2.3.2.3.1.2.
- Step 5 is a Proxy Binding Acknowledgement. The parameters in the Proxy Binding Acknowledgement message are same as step 5 in clause 8.2.3.2.3.1.2.

8.2.3.2.3.2.3 UE/TWAN requested Detach Procedure in WLAN on PMIP S2a

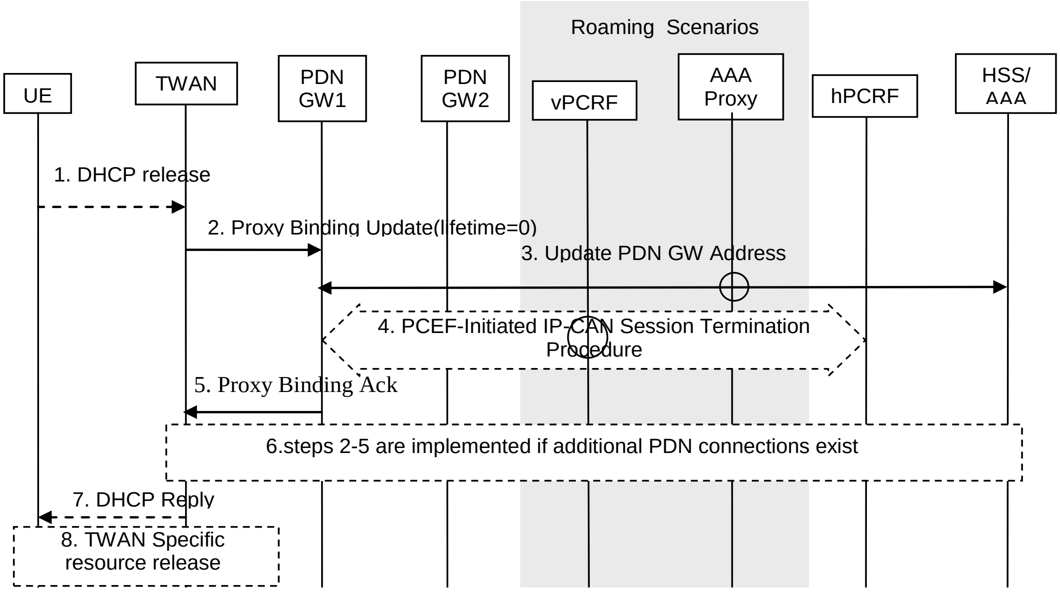

Roaming Scenarios
UE
TWAN
PDN GW1
PDN GW2
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCP release
2. Proxy Binding Update(lifetime=0)
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Proxy Binding Ack
6.steps 2-5 are implemented if additional PDN connections exist
7. DHCP Reply
8. TWAN Specific resource release

Figure 8.2.3.2.3.2.3-1: UE/ TWAN requested Detach on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.3.1.3, with the following differences:

- Step 2 is a Proxy Binding Update. The parameters in the Proxy Binding Update message are same as step 2 in clause 8.2.3.2.3.1.3.
- Step 5 is a Proxy Binding Acknowledgement. The parameters in the Proxy Binding Acknowledgement message are same as step 5 in clause 8.2.3.2.3.1.3.

8.2.3.2.3.2.4 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a

Same as the procedure for SaMOG R11, refer to TS 23.402 [3] clause 16.3.1.2.

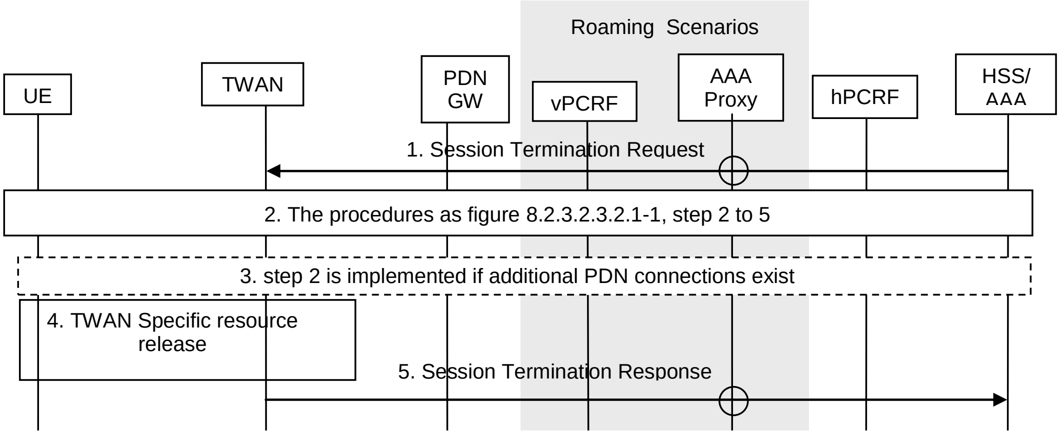

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as figure 8.2.3.2.3.2.1-1, step 2 to 5
3. step 2 is implemented if additional PDN connections exist
4. TWAN Specific resource release
5. Session Termination Response

Figure 8.2.3.2.3.2.4-1: HSS/AAA Initiated Detach on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.3.1.4, the difference is that steps 2 and 3 refer to figure 8.2.3.2.3.2.3-1.

8.2.3.2.4 PDN GW initiated Resource Allocation Deactivation in WLAN on S2a

Same as the procedure for SaMOG R11, refer to TS 23.402 [3] clause 16.4.

8.2.3.2.4.1 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, e.g. due to IP-CAN session modification requests from the PCRF. If the default S2a bearer belonging to a PDN is deactivated, the PDN GW deactivates all S2a bearers belonging to the PDN.

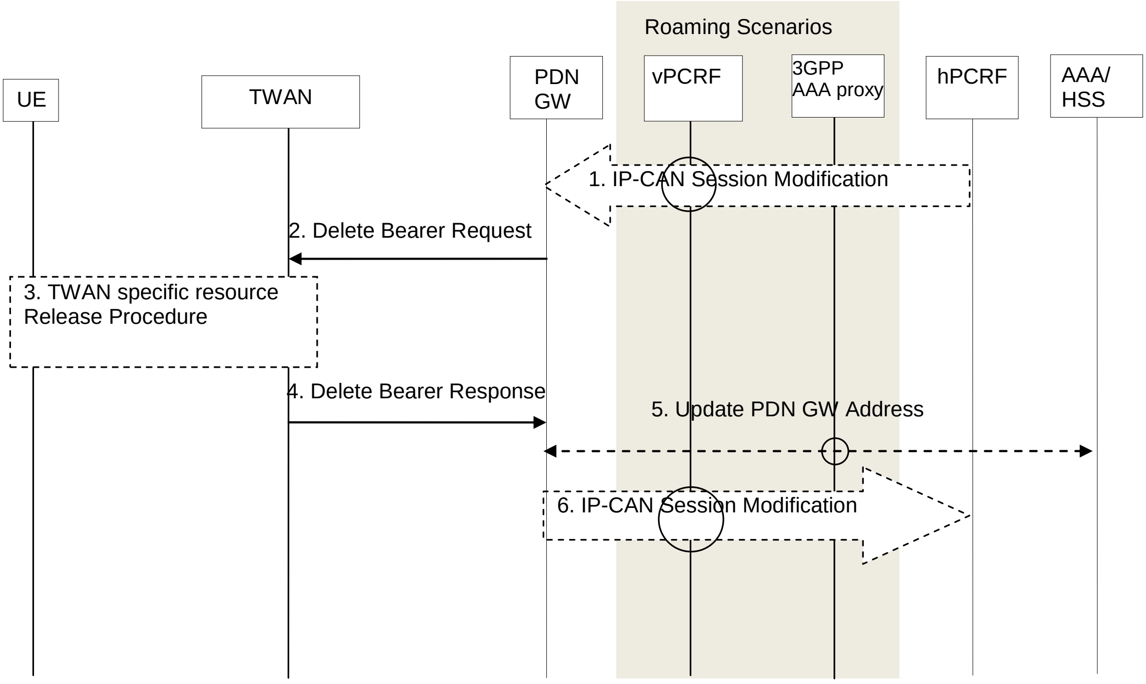

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
3GPP AAA proxy
hPCRF
AAA/ HSS
1. IP-CAN Session Modification
2. Delete Bearer Request
3. TWAN specific resource Release Procedure
4. Delete Bearer Response
5. Update PDN GW Address
6. IP-CAN Session Modification

Figure 8.2.3.2.4.1-1: 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 16..4.1-1 occur only if dynamic policy provisioning is deployed. Otherwise policy may be statically configured within the PDN GW.

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

2. The PDN GW sends a Delete Bearer Request message (EPS Bearer Identity, Cause) to the TWAN. This message can include an indication that all bearers belonging to that PDN shall be released.

3. If supported by the TWAN, the TWAN shall remove the associated contexts corresponding to specific PDNs, and inform UE to remove the associated contexts.

4. The TWAN deletes the bearer contexts related to the Delete Bearer Request message, and acknowledges the bearer deactivation to the PDN GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

5. In the case of the resources corresponding to the PDN 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.

8.2.3.2.4.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a

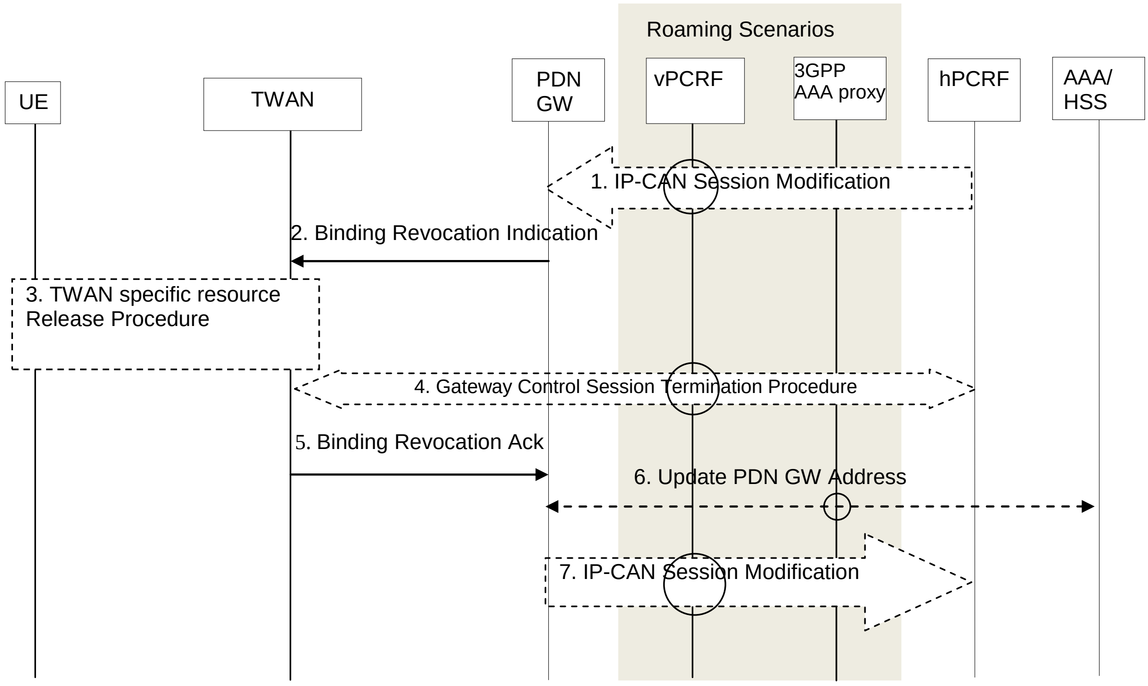

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
3GPP AAA proxy
hPCRF
AAA/ HSS
1. IP-CAN Session Modification
2. Binding Revocation Indication
3. TWAN specific resource Release Procedure
4. Gateway Control Session Termination Procedure
5. Binding Revocation Ack
6. Update PDN GW Address
7. IP-CAN Session Modification

Figure 8.2.3.2.4.2-1: PDN GW Initiated Bearer Deactivation with PMIP on S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.4.1, with the following differences:

- Step 2 is a Binding Revocation Indication message. The parameters in the Binding Revocation Indication message are same as step 2 in clause 8.2.3.2.4.1.
- Step 4. If the resources are released in the TWAN, the TWAN initiates a Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [4].
- Step 5 is a Binding Revocation Acknowledgement message. The parameters in t he Binding Revocation Acknowledgement message are same as step 4 in clause 8.2.3.2.4.1.

8.2.3.2.5 Dedicated bearer activation in WLAN on GTP S2a

Same as the procedure for SaMOG R11, refer to TS 23.402 [3] clause 16.5.

8.2.3.2.6 Network-initiated bearer modification in WLAN on GTP S2a

Same as the procedure for SaMOG R11, refer to TS 23.402 [3] clause 16.6.

8.2.3.2.7 Handover from 3GPP Access to Trusted WLAN Access

8.2.3.2.7.1 Handover from 3GPP Access to Trusted WLAN Access on GTP S2a

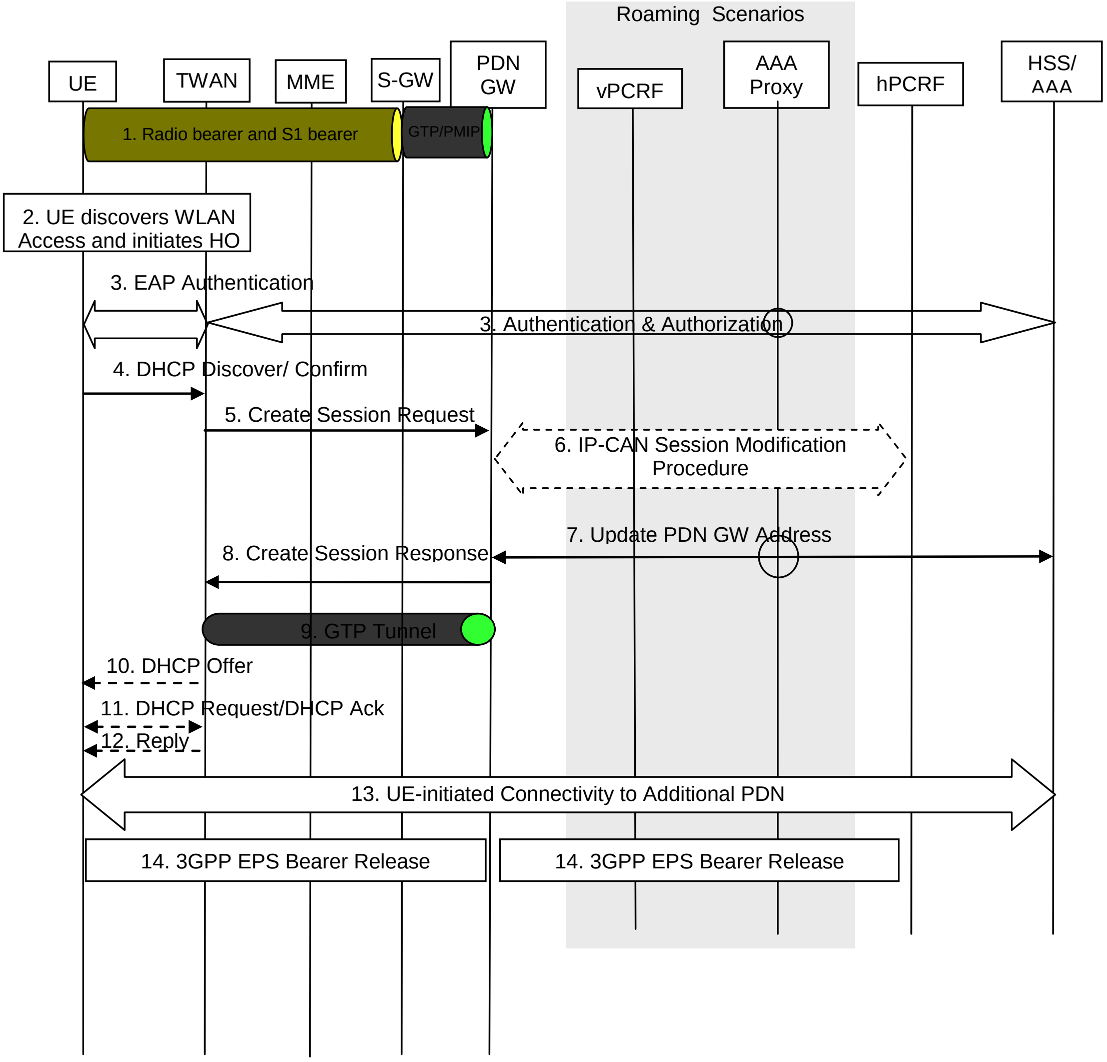

Roaming Scenarios
UE
TWAN
MME
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Radio bearer and S1 bearer
GTP/PMIP
2. UE discovers WLAN Access and initiates HO
3. EAP Authentication
3. Authentication & Authorization
4. DHCP Discover/ Confirm
5. Create Session Request
6. IP-CAN Session Modification Procedure
7. Update PDN GW Address
8. Create Session Response
9. GTP Tunnel
10. DHCP Offer
11. DHCP Request/DHCP Ack
12. Reply
13. UE-initiated Connectivity to Additional PDN
14. 3GPP EPS Bearer Release
14. 3GPP EPS Bearer Release

Figure 8.2.3.2.7.1-1: Handover from 3GPP Access to Trusted WLAN Access on GTP S2a

1-2) These steps are the same as steps 1-3 in TS 23.402 [3], clause 8.2.2.

3. In this step, indication on whether the UE indicates its capability (i.e. Rel-12 SaMOG capability) to the AAA server during the authentication procedure. Based on the UE capability provided by AAA server, the TWAN decides to use L3 trigger.

4. The UE shall send a DHCPv4 Discover as per IETF RFC 2131 [9], or DHCPv6 confirm as per IETF RFC 3315 [23] to TWAN with "requested IP address" included in DHCPv4 Discover message (option 50)/ DHCPv6 Confirm message (option IA_NA) with all previously assigned UE IP addresses prior to its handover. TWAN determines IP address preservation by the presence of the "requested IP address" option. APN, PDN Type and downlink GRE key (for alternative 1) shall also be included.

5. The TWAN sends a Create Session Request (APN PDN address, Handover Indication) message to the PDN GW. The PDN Address shall be set according to requested IP address for DHCP request message in step 4， and sent to the PDN GW. The TWAN sets the 'Handover Indication' to allow the PDN GW to re-allocate the same IPv4 address and/or IPv6 address that was assigned to the UE while it was connected to 3GPP IP access and to initiate an IP CAN Session Modification Procedure with the PCRF. Both the APN and PDN Address are used by the PDN GW to determine which PDN to establish connectivity for, in the case that the PDN GW supports multiple PDN connectivity.

6) This steps is same as steps 7A-7B in TS 23.402 [3], clause 8.2.2.

7) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN and obtains authorization information from the 3GPP AAA Server. The 3GPP AAA Server decides whether or not to update PDN GW identification according to the UE capability, which has been provided at the authentication phase. If the UE supports IP address preservation, the 3GPP AAA Server shall update PDN GW identity towards the HSS.

8. The PDN GW responds with a Create Session Response to the TWAN. The Create Session Response contains the IPv4 address and/or the IPv6 address that were assigned to the UE while it was connected to the 3GPP IP access.

9. GTP tunnel is setup between TWAN and PDN GW.

10. For DHCPv4, TWAN returns DHCP offer message to UE, TWAG virtual MAC address is included if alternative 2 is used.

11. UE sends DHCP Request (for DHCPv4) to TWAN, and TWAN returns DHCP Ack message to the UE and UE IP allocated by PDN GW.

    a) Alternative 1: GRE tunnelling information is included to UE, where GRE tunnel information includes uplink GRE key and UE's local IP address which are allocated by TWAN for tunnelling support in the case of one or multiple PDNs.

    b) Alternative 2: Both UE and TWAN maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address.

12. TWAN returns Reply message to the UE, and UE IP allocated by PDN GW.

    a) Alternative 1: GRE tunnelling information is included to UE, where GRE tunnel information includes uplink GRE key and UE's local IP address which are allocated by TWAN for tunnelling support in the case of one or multiple PDNs.

    b) Alternative 2: Both UE and TWAN maintain the relations of TWAG virtual MAC address and associated UE information, including IMSI, APN, UE IP address.

    When PDN type is IPv4, steps 10-11 apply.

    When PDN type is IPv6, step 12 apply.

    When PDN type is IPv4v6, there are two following cases:

- **Alternative 1:**

    (a) If UE requests IPv4 address first, TWAN shall implement steps 10-11 and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send confirm message encapsulated by the GRE key which is allocated in step 11 to TWAN, TWAN shall implement steps 12 which are encapsulated by the GRE key which is allocated in step 11.

    (b) If UE requests IPv6 address first, TWAN shall implement steps 12 and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message encapsulated by the GRE key which is allocated in step 12 to TWAN, TWAN and UE shall implement steps 10-11 which are encapsulated by the GRE key which is allocated in step 12.

- **Alternative 2:**

    (a) If UE requests IPv4 address first, TWAN shall implement steps 10-11 and return IPv4 address to UE. Subsequently, when UE requests IPv6 address, it shall send confirm message with TWAG virtual MAC address which is allocated in step 10 to TWAN, TWAN shall implement steps 12.

    (b) If UE requests IPv6 address first, TWAN shall implement steps 12 and return IPv6 address to UE. Subsequently, when UE requests IPv4 address, it shall send DHCP discovery message with TWAG virtual MAC address which is allocated in step 12 to TWAN, TWAN and UE shall implement steps 10-11.

Both uplink and downlink GRE key corresponds to the specific PDN. And subsequently, user data for the PDN shall be encapsulated by corresponding GRE tunnel.

13. For connectivity to multiple PDNs, the UE establishes connectivity to all the remain PDNs that are being transferred from 3GPP access besides the PDN, and steps 3 to 12 are repeated for per PDN, with the following exception:

    - Handover indication isn't included in step 5.

14. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 in TS 23.402 [3] for PMIP S5/S8 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1 for GTP-S5/S8.

8.2.3.2.7.2 Handover from 3GPP Access to Trusted WLAN Access on PMIP S2a

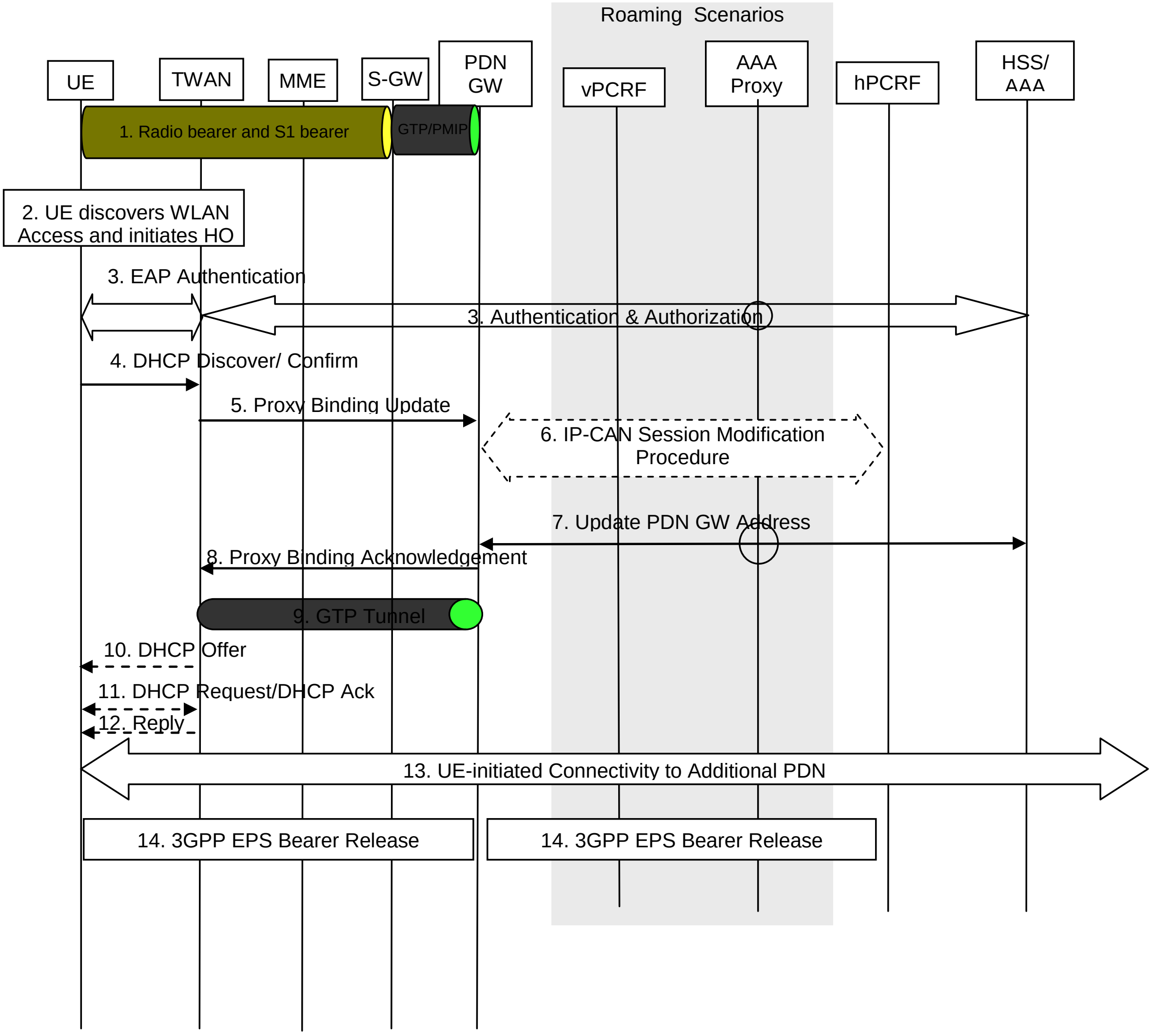

Roaming Scenarios
UE
TWAN
MME
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Radio bearer and S1 bearer
GTP/PMIP
2. UE discovers WLAN Access and initiates HO
3. EAP Authentication
3. Authentication & Authorization
4. DHCP Discover/ Confirm
5. Proxy Binding Update
6. IP-CAN Session Modification Procedure
7. Update PDN GW Address
8. Proxy Binding Acknowledgement
9. GTP Tunnel
10. DHCP Offer
11. DHCP Request/DHCP Ack
12. Reply
13. UE-initiated Connectivity to Additional PDN
14. 3GPP EPS Bearer Release
14. 3GPP EPS Bearer Release

Figure 8.2.3.2.7.2-1: Handover from 3GPP Access to Trusted WLAN Access on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 8.2.3.2.7.1, with the following differences:

- Step 5 is a Proxy Binding Update. The parameters in the Proxy Binding Update message are same as step 5 in clause 8.2.3.2.7.1.
- Step 8 is a Proxy Binding Acknowledgement. The parameters in the Proxy Binding Acknowledgement message are same as step 8 in clause 8.2.3.2.7.1.

8.2.3.3 Impacts on existing nodes or functionality

8.2.3.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 as well as simplicity of implementation in the UE should be evaluated.

The following aspects are considered and evaluated for the solution:

i) Impacts to existing network deployment:

a) There is no requirement for WLAN APs compared to Rel-11.

b) For TWAG, it shall support DHCP enhancement, EAP enhancement, and the association of IPv4 session and IPv6 session for same PDN for dual stack scenario.

ii) Impacts to UE:

a) For UE, it shall support DHCP enhancement, EAP enhancement, and the association of IPv4 session and IPv6 session for same PDN for dual stack scenario.

NOTE 1: Required the support of Stateful DHCP as described in RFC 3315 with also the 3GPP vendor specific extensions

NOTE 2: Required additional security support for DHCP Force renew as described in RFCs 3203 and 6704

NOTE 3: The IPv4 and IPv6 sessions association for dual-stack support is common to all SaMOG proposed solutions and is not specific to Solution 3.

b) UE is required to support GRE-over-IP encapsulation if alternative 1 is used.

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA'):

The following protocols are extended:

a) UE network capability negotiation is enhanced for EAP protocol.

b) Session Management (APN, PDN type, GRE tunnel information(for alternative 1), UE IP), is enhanced for DHCP protocol.

c) 3GPP Vendor-specific Information can be used for enhanced information in DHCP protocol

iv) Impacts to protocols defined by other SDOs (e.g. DHCP):

No impact on other SDOs.

v) Control plane

a) The latency/load can increase in the following procedures:

1) For first PDN and handover procedures, EAP (once for first PDN) and DHCP messages are implemented.

2) For additional PDN, DHCP messages are implemented.

b) There is no impact on other network element, e.g. AAA signalling etc.

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements:

a) Co-existence with Rel-11 SaMOG

b) Support for IP address preservation during handover

c) Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDNs

vii) Other functional limitations:

There is no other functional limitation.

8.2.4 Solution 4

8.2.4.1 Functional Description

8.2.4.1.1 P2P link

A per UE point-to-point link between the UE and the TWAG is assumed.

The TWAG performs unicast layer 2 forwarding even when layer 3 is multicast address (e.g. Router Advertisement, RFC 6085).

Editor's note: Handling of unsolicited IPv6 Router Advertisement for PDN connections is FFS.

Editor's note: How to support multiple IPv4 PDN connections when same private IPv4 addresses are allocated from different PDN connections with per UE point-to-point link is FFS.

In IPv4 case, the multiple PDN may use the same IP multicast address for different services, the source IP address in general could be used to disambiguate the multicast services.

Editor's note: If the source IP address is same, how to distinguish the services are FFS.

8.2.5 Solution 5: Associating APN/PDN with Virtual IP Interface

8.2.5.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.5.1.1 General

This clause describes in general the point-to-point link/IP forwarding and the control sequence for associating an APN/NSWO to a point-to-point link. The session control protocol carries the APN/PDN signalling attributes and uses distinct Gateway interface (gateway IP address, MAC address) for the connection to associate the APN in IP configuration signalling (DHCP for IPv4, stateless autoconfiguration for IPv6).

Point-to-Point Link

The point-to-point link in this solution uses the distinct MAC address per APN/NSWO at the gateway as described in clause 8.2.2.1.1.2 for packet forwarding. In addition to a distinct MAC address, this solution has a distinct TWAG Gateway Interface per APN/NSWO connection. A TWAG Gateway Interface for a connection consists of an IP address and a MAC address - each of which is distinct for connections to a UE.

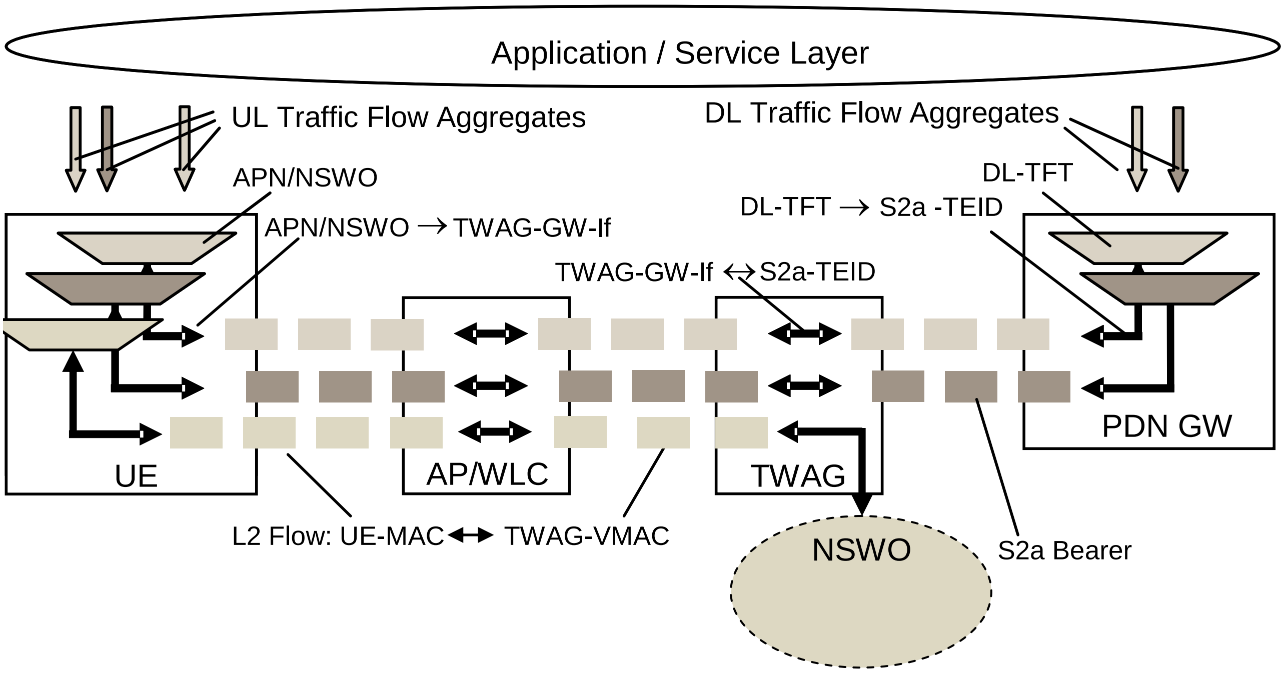

Application / Service Layer
UL Traffic Flow Aggregates
DL Traffic Flow Aggregates
APN/NSWO
APN/NSWO → TWAG-GW-If
DL-TFT
DL-TFT → S2a -TEID
TWAG-GW-If ↔ S2a-TEID
UE
AP/WLC
TWAG
PDN GW
L2 Flow: UE-MAC ↔ TWAG-VMAC
NSWO
S2a Bearer

Figure 8.2.5.1.1-1: Point-to-Point Link

PDN Control Protocol

The PDN control protocol is used to signal APN/PDN information between UE TWAN. This protocol also associates the APN/NSWO connection request to a distinct gateway IP address/MAC address prior to IP configuration using DHCP, RS/RA. The gateway IP address is derived from the MAC address and there is a 1:1 association between the distinct gateway MAC address and the gateway IP address. For IP configuration signalling using DHCP or RS/RA, the TWAG can uniquely associate a UEs PDN connection using UE MAC address (or IPv6 link layer address) and this gateway interface (IP address, virtual MAC address) that is distinct for each PDN connection of the UE.

For IPv4 stateful address configuration, the UE provides a PDN connection request and the TWAG returns this distinct gateway IP address as input for server-identity in DHCP request. In the subsequent DHCP Request from UE, the server-identity is populated with this distinct gateway IP address as a means for the TWAG to identify the PDN connection.

For IPv6 stateless address configuration, the UE provides an PDN connection request and the TWAG returns this distinct gateway IP address and also populates the same gateway IP address in a Router Advertisement that follows. For cases where the UE needs to send a Router Solicitation (optional), the TWAG also returns a transient multicast address corresponding to this PDN connection that the TWAG listens to. The UE may send a Router Solicitation with destination address set to this transient multicast address that is distinct for this PDN connection.

If UE request handover from 3GPP to WLAN access, it indicates handover attach in the control protocol.

If the UE needs to setup a second PDN connection, this can be signalled in a subsequent connection setup request. For disconnection of a PDN connection, either the UE or the TWAN may notify the other about an IP address/prefix that is released. The notified entity can then release the local connection resources.

The PDN Control Protocol described above consists of requests / responses or notification messages and requires a transport for these messages. Two alternative transport protocols are considered here:

- **Alternative A: ICMP Echo Payload**

  ICMP Echo [RFC 792] is typically used to verify if another host is active. However, it is possible to add an arbitrary data payload following the ICMP header as long as it is echoed back, and this solution uses the data payload to carry binary encoded connection control messages each of which is an ICMP Echo Request and Response. The PDN Control Protocol is identified by a unique sequence identifier (e.g. 0xFCFCFC) that follows the ICMP Echo message and precedes the PDN control protocol frame. The data payload of the ICMP Echo messages maybe authenticated (message authentication) using a hashed key each for UE and TWAG (established during EAP-AKA). Only one set of keys are established between UE - TWAG and either the link local address or the NSWO IP connection may be used for this signalling.

Reliability of this control sequence is provided by virtue of receiving the echoed message. For re-transmission, this method re-uses the DHCP re-transmission timer value. No support for fragmentation is provided and is not necessary for the control protocol.

The ICMP Echo payload mechanism uses existing ICMP protocol semantics and does not violate IETF RFC 792. Only the control messages need to be standardized (in 3GPP).The mechanism is basic and is efficient enough even if messages are echoed back since only a limited amount of control signalling required and is always across one IP hop.

- **Alternative B: 802.11 GAS frame**

  802.11 GAS frames can be used to carry the PDN control protocol frames similar to the transport of ANQP/GAS between UE - WLAN Access Point. These control frames could then be carried to the TWAG over RADIUS or other similar protocol. The control protocol semantics are the same as in Alternative A above.

  Reliability of this control sequence is provided using 802.11 GAS and the backhaul protocol (e.g. RADIUS). Re-transmission timers re-use the DHCP re-transmission timer value. No fragmentation is expected as the signalling is expected to be well below the size of an Ethernet frame.

  The PDN Control protocol would be defined as a new GAS protocol in WFA as part of HS2.0 Rel-3 specifications. The protocol would use the WMM Notification Action frames as a L2 transport for the 802.11 air interface. In addition, RADIUS protocol messages Accept-Request/Response (for PDN Request/Response) and Change-of-Authorization (for Notification) should carry this protocol from AP - TWAN controllers. This underlying mechanism provides a reliable control protocol transport. As in the case above, DHCP re-transmission timer values may be used.

Editor's note: Selection of one of the control transport protocols is FFS.

Editor's note: For uplink broadcasts signalling (e.g. IPv6 RS, IPv6 ND, ARP, and service discovery requests (e.g. DLNA) generally sent using a L2 (MAC) broadcast address:

- when the destination MAC address used over WLAN is a broadcast address and not the TWAG MAC address associated with a TWAN connectivity service, a specific handling would be required at the TWAN to handle such traffic or
- the UE uses a unicast MAC addressing for such traffic as described in RFC 6085 "Address Mapping of IPv6 Multicast Packets on Ethernet " for the IPv6 case. Using such technique for IPv4 is FFS.

8.2.5.2 Procedures

Editor's note: The call flows are described in this clause.

8.2.5.2.2 Connection Establishment Procedure

The connection establishment procedures below support both PDN connection establishment and NSWO connections. In the case of PDN connections, the signalling from UE to TWAN explicitly provides the APN that the UE wishes to connect to. For NSWO connections, the UE indicates NSWO request or signal that it wants a local IP address.

The figures below outline GTP S2a, PMIP S2a and NSWO connection setup.

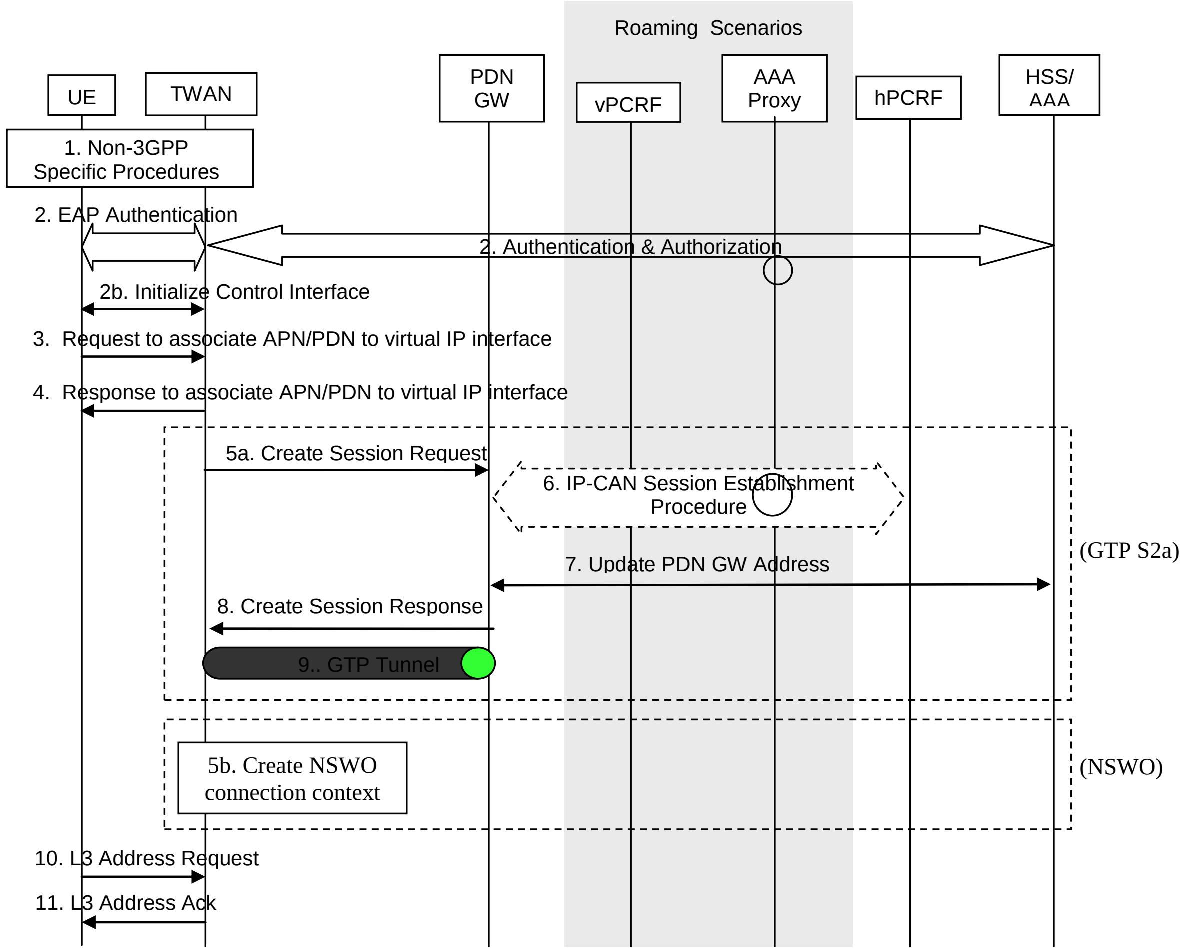

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
2b. Initialize Control Interface
3. Request to associate APN/PDN to virtual IP interface
4. Response to associate APN/PDN to virtual IP interface
5a. Create Session Request
6. IP-CAN Session Establishment Procedure
7. Update PDN GW Address
8. Create Session Response
9.. GTP Tunnel
(GTP S2a)
5b. Create NSWO connection context
(NSWO)
10. L3 Address Request
11. L3 Address Ack

Figure 8.2.5.2.2-1: Attach Procedure for PDN and NSWO for GTP based S2a

The procedure to attach PDN or NSWO for a trusted WLAN access is represented in Figure 8.2.5.2.2-1 and described below:

1. The initial TWAN specific L2 procedures are performed. These procedures are TWAN specific and outside the scope of 3GPP.

2. EAP authentication procedures are performed. During this sequence, support of Phase 2 by the UE and TWAG are conveyed using EAP-AKA (IETF RFC 4187 [22] extensions. If the UE, TWAG are Phase 2 compliant, the UE and TWAG setup and exchange keys to be used to provide integrity protection (e.g. checksum hash) for the subsequent signalling setup messages.

After successful authentication, in step 2b, for ICMP Payload transport of PDN signalling protocol, the UE sets up a link-local address for IPv4 (RFC 3927), or follows the procedure in IETF RFC 4861 [11] to setup an IPv6 link local address. The TWAG replies with a control-initialize message with source router IP, MAC address that UE can use in subsequent requests.

3. The UE sends a request with APN, other PDN signalling parameters (e.g. initial attach) to the TWAN to setup a PDN/NSWO connection. The signalling may be transported using ICMP Echo Payload (alternative 1) or 802.11 GAS (alternative 2).

4. The TWAN assigns a distinct IPv4 gateway address corresponding to the APN/NSWO and responds with this address in server-identity and router address for IPv4. For IPv6, the TWAN assigns a distinct IPv6 gateway address (source address in Router Advertisement) and transient multicast address for router solicitation if needed.

Editor's note: The choice of a control protocol transport in steps 3-4 is FFS.

Steps 5 - 9are performed as specified in TS 23.402 [3], clause 16.2.1, steps 3 - 7 for PDN connection establishment for GTP S2a.

For NSWO connection, step 5b, the TWAG assigns local connection resources (gateway IP address, subnet, etc.) for the connection.

10. The UE sends a layer 3 attach request.

For IPv4, the UE sends a DHCP Request with server-identity option set to the distinct gateway IP address obtained in step 4.

For IPv6, the UE may optionally send a Router Solicitation with destination address set to the transient multicast address obtained in step 4.

11. The TWAN responds to the layer 3 attach.

For IPv4, the TWAG sends a DHCP Ack with server-identity, router option set to the distinct gateway IP address for the APN/NSWO. The IP address in the message is in yiaddr.

For IPv6, the TWAG sends a Router Advertisement when a Create Session Response (step 8) is received for this PDN connection or it receives Router Solicitation in step 10. The Router Advertisement is sent with source address set to the distinct gateway IP address configured for this APN/NSWO in step 4.

The UE can determine the L2 address of the router interface by sending an ARP Request (IPv4) or Neighbour Solicitation (IPv6)

For subsequent PDN / NSWO connections, steps 3 - 11 are repeated.

Establishing a second connection (IP address/interface) corresponding to an already signalled/established APN/NSWO session is straightforward using this method. In step 3 above, the explicit parameters that are conveyed between UE and TWAG can include the means to indicate if a second connection is being requested.

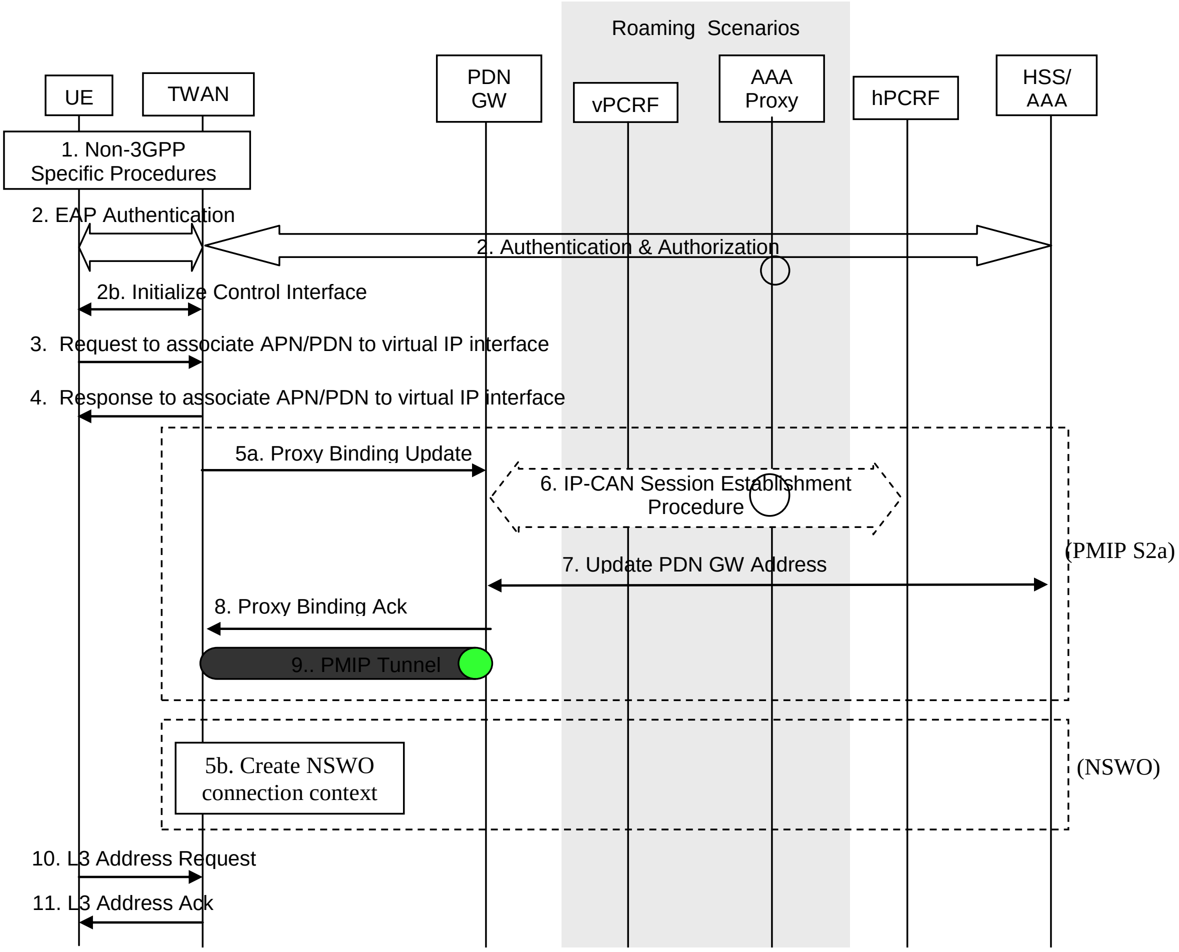

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
2b. Initialize Control Interface
3. Request to associate APN/PDN to virtual IP interface
4. Response to associate APN/PDN to virtual IP interface
5a. Proxy Binding Update
6. IP-CAN Session Establishment Procedure
7. Update PDN GW Address
(PMIP S2a)
8. Proxy Binding Ack
9.. PMIP Tunnel
5b. Create NSWO connection context
(NSWO)
10. L3 Address Request
11. L3 Address Ack

Figure 8.2.5.2.2-2: Attach Procedure for PDN and NSWO for PMIP based S2a

The procedure for attach using PMIP based S2a is similar to the sequence for GTP. However, steps 5a and 8 for PMIP consist of Proxy Binding Update (5a) and Proxy Binding Ack (8).

8.2.5.2.3 UE Initiated Disconnection Procedure

The disconnection sequence in the figure below supports UE triggered disconnection of one connection (while the rest of the session remains unchanged). If the last connection (or all connections) is being released, all session resources are cleaned up also.

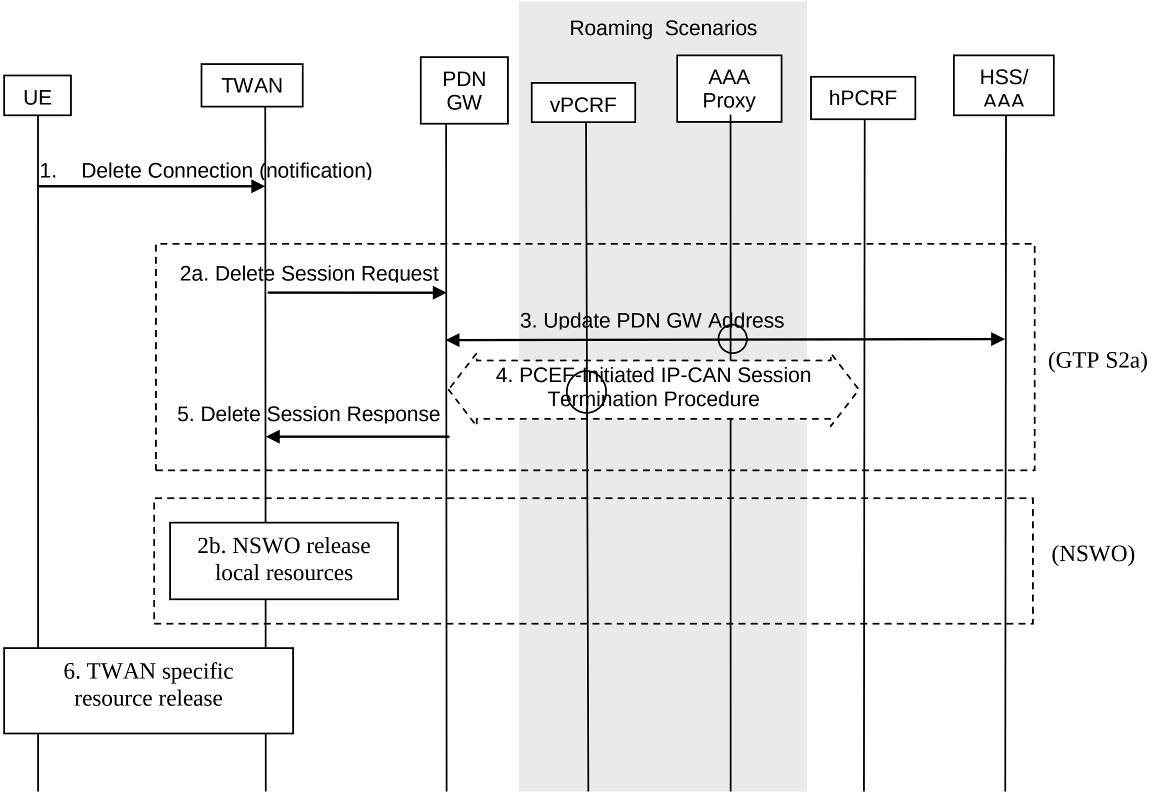

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Delete Connection (notification)
2a. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
(GTP S2a)
2b. NSWO release local resources
(NSWO)
6. TWAN specific resource release

Figure 8.2.5.2.3-1: Disconnection Procedure for PDN and NSWO for GTP based S2a

The procedure to disconnect a PDN /NSWO session for GTP based S2a is shown in the figure above.

1. The UE sends a delete connection notification with the IP address and gateway IP address for the connection to trigger disconnection.

2. If the IP address to be released is not an NSWO connection, the TWAG initiates a Delete Session Request with the IP address of the PDN connection. (2a).

   For NSWO, the TWAN releases local connection resources (2b).

   Steps 3, 4 are as defined in TS 23.402 [3], clause 16.3.1.1, steps 3, 4.

5. The PDN GW acknowledges with Delete Session Response (cause).

6. Connection resources in TWAG and UE are released.

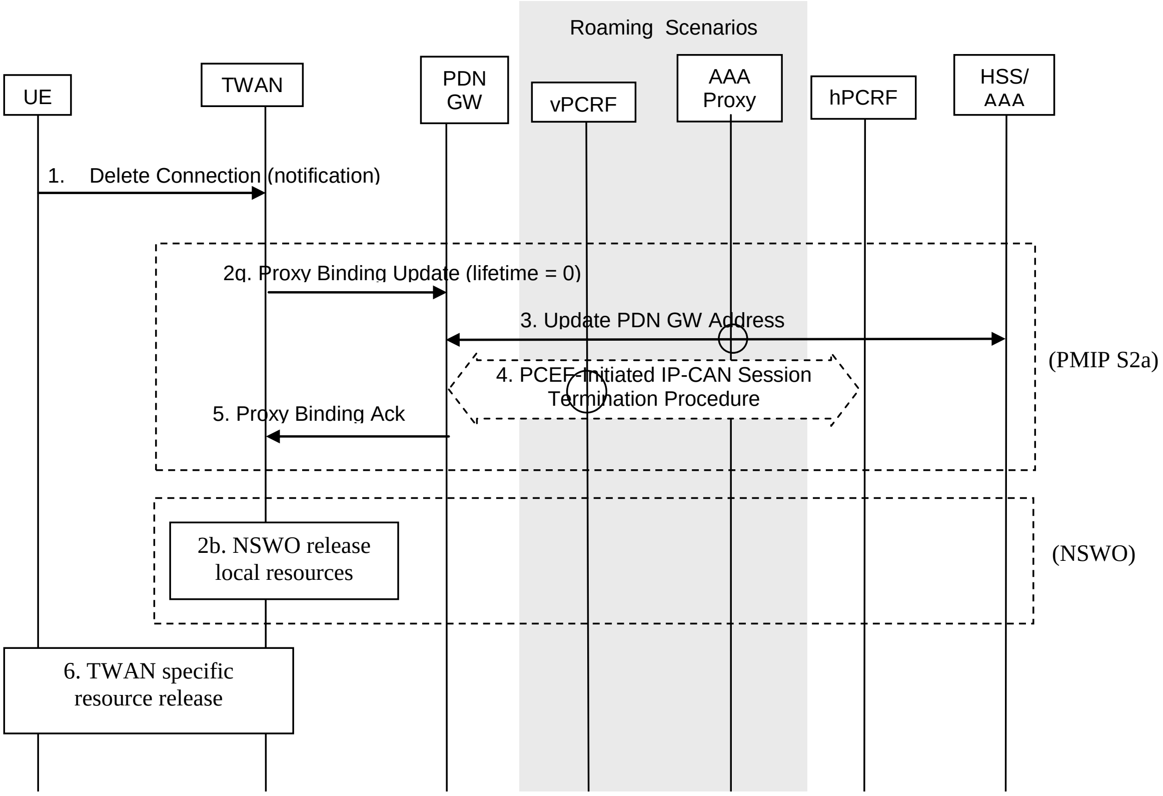

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Delete Connection (notification)
2a. Proxy Binding Update (lifetime = 0)
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Proxy Binding Ack
(PMIP S2a)
2b. NSWO release local resources
(NSWO)
6. TWAN specific resource release

Figure 8.2.5.2.3-2: Disconnection Procedure for PDN and NSWO for PMIP based S2a

The procedure for disconnection using PMIP based S2a is similar to the sequence for GTP. However, steps 2a and 5 for PMIP consist of Proxy Binding Update with lifetime set to zero (2a) and Proxy Binding Ack (5).

8.2.5.2.4 HSS/AAA Initiated Disconnection Procedure

The disconnection sequence in the figure below supports disconnection of one connection triggered by the HSS/AAA (while the rest of the session remains unchanged). If the last connection (or all connections) is being released, all session resources are cleaned up also.

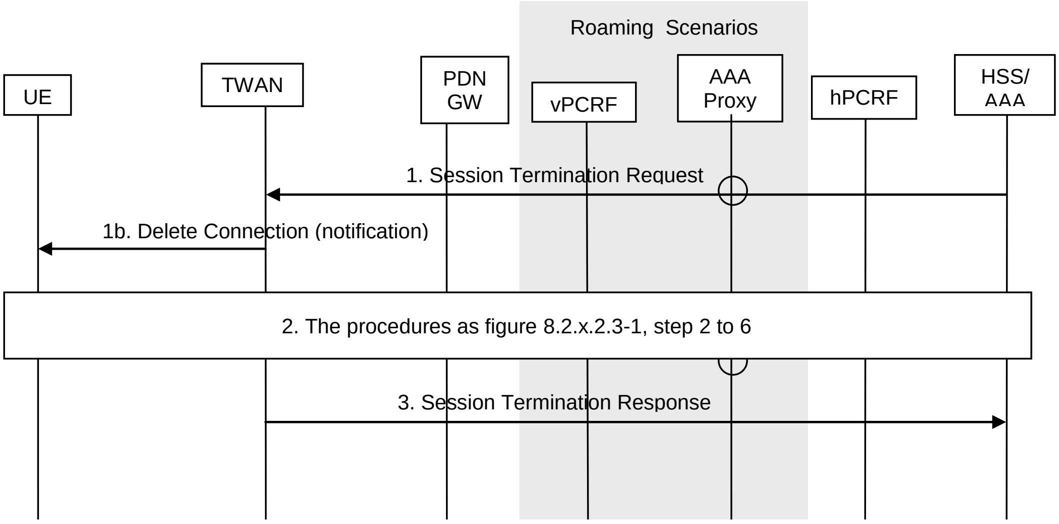

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
1b. Delete Connection (notification)
2. The procedures as figure 8.2.x.2.3-1, step 2 to 6
3. Session Termination Response

Figure 8.2.5.2.4-1: Disconnection Procedure for GTP based S2a

The procedure to disconnect a PDN /NSWO session for GTP based S2a when triggered by HSS/AAA is shown in the figure above.

1. The HSS/AAA sends a Session Termination Request message to the TWAN to detach a specific UE.

In (1b), the TWAG sends a delete connection notification message with the IP address and gateway IP address of the connection to trigger release of connection resources at UE.

2. The procedures in 8.2.5.2.3, steps 2 - 6 are followed.

3. Step 3 defined in TS 23.402 [3], clause 16.3.1.2 is followed.

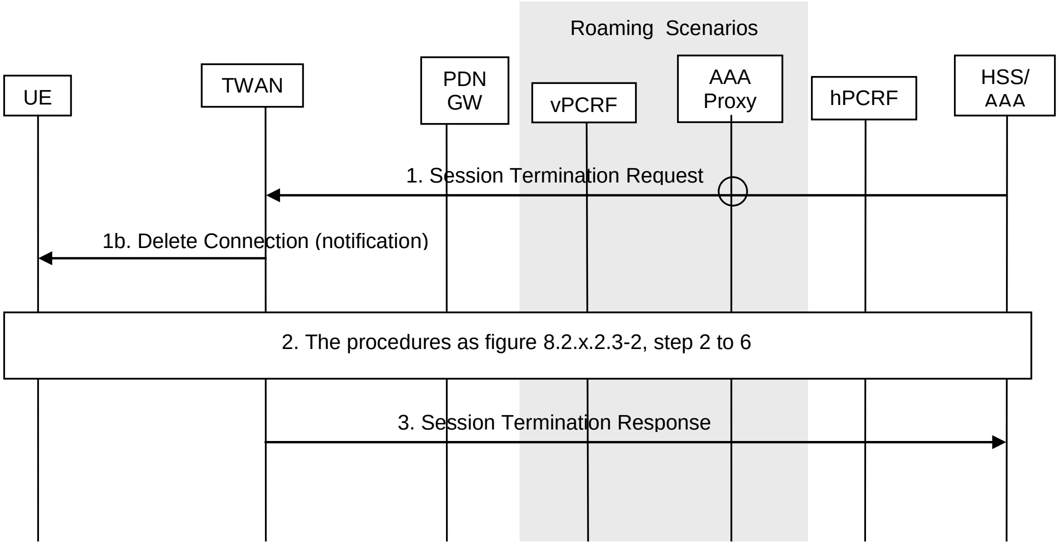

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
1b. Delete Connection (notification)
2. The procedures as figure 8.2.x.2.3-2, step 2 to 6
3. Session Termination Response

Figure 8.2.5.2.4-2: Disconnection Procedure for PMIP based S2a

The procedure for disconnection using PMIP based S2a is similar to the sequence for GTP. Step 2 in the figure is based on 8.2.5.2.3 for PMIP.

8.2.5.2.5 Handover procedure between 3GPP access and WLAN on GTP S2a

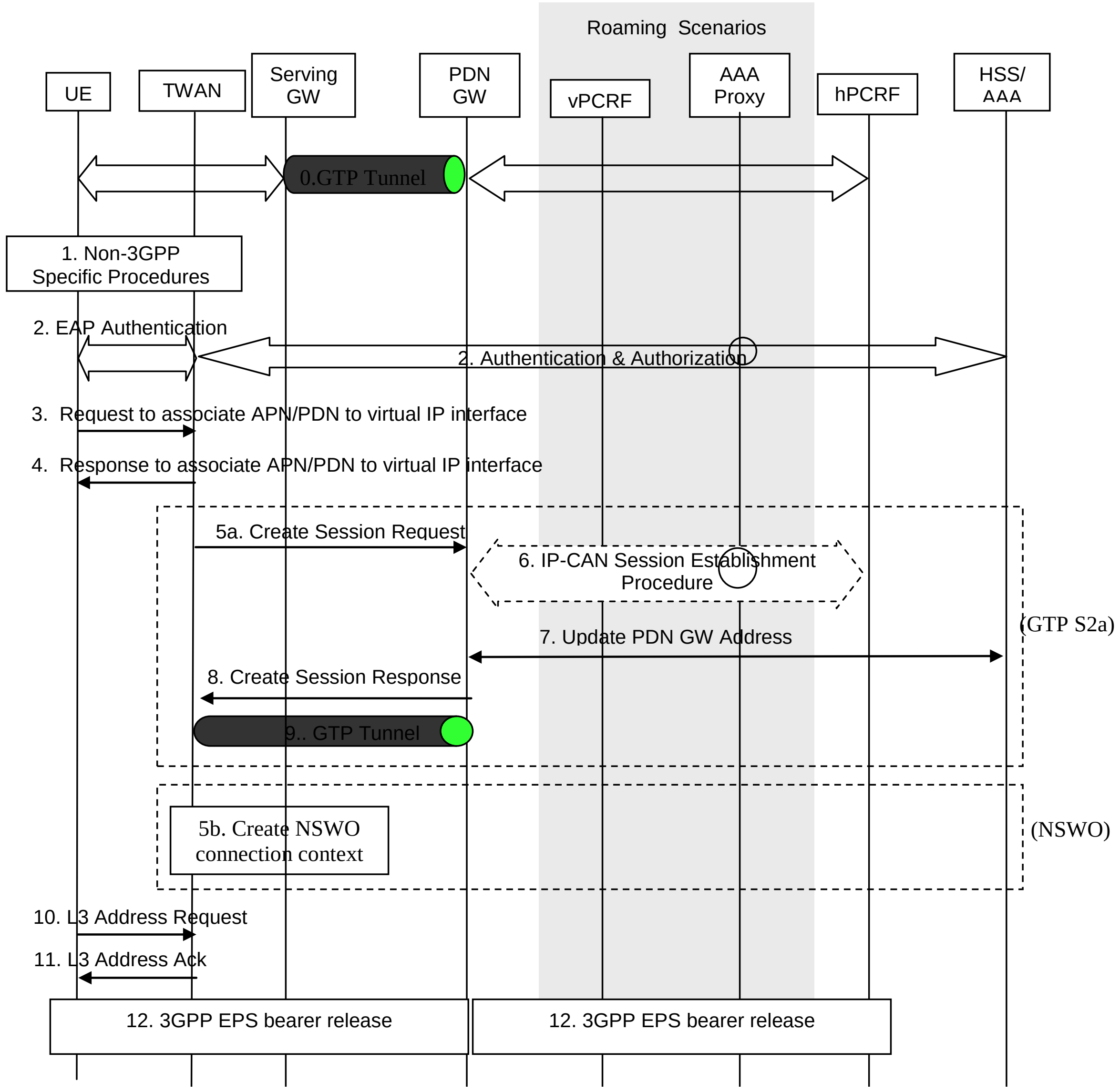

Roaming Scenarios
UE
TWAN
Serving GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0.GTP Tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Request to associate APN/PDN to virtual IP interface
4. Response to associate APN/PDN to virtual IP interface
5a. Create Session Request
6. IP-CAN Session Establishment Procedure
7. Update PDN GW Address
(GTP S2a)
8. Create Session Response
9.. GTP Tunnel
5b. Create NSWO connection context
(NSWO)
10. L3 Address Request
11. L3 Address Ack
12. 3GPP EPS bearer release
12. 3GPP EPS bearer release

Figure 8.2.5.2.6-1: Handover from 3GPP access to Trusted WLAN on GTP S2a

The handover procedure is based on the Connection Establishment Procedure in 8.2.5.2.2 with the following additions:

0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.

1. The initial TWAN specific L2 procedures are performed. These procedures are TWAN specific and outside the scope of 3GPP.

2. If the handover establishes the first PDN connection in WLAN of the UE, EAP procedure is performed in this step.

3. The UE sets up an IP interface to perform initial PDN signalling with the TWAN. During this sequence, if UE and TWAG are Phase 2 compliant, i.e. supporting EPC-routed , handover and multiple PDN connections, the UE sends a request with APN and handover indication, to setup a PDN connection.

4. The TWAN assigns a distinct IPv4 gateway address corresponding to the APN and responds with this address in server-identity and router address for IPv4. For IPv6, the TWAN assigns a distinct IPv6 gateway address (source address in Router Advertisement) and transient multicast address for router solicitation if needed.

5. The TWAN sends a Create Session Request (APN, handover indication) message to the PDN GW. The APN and handover indication is set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF-

Initiated IP-CAN Session Modification Procedure with the PCRF. The APN is used by the PDN GW to determine which PDN connection(s) to handover, in the case that the UE has established multiple PDN connections to different APNs.

Steps 6 - 11 are performed as Connection Establishment Procedure in 8.2.5.2.2.

12. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.5.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

This solution minimizes the impact to existing IP configuration procedures - both DHCP, stateless IPv6 auto-configuration by moving all PDN connection signalling to a new protocol that only handles PDN connection aspects.

For transporting the new PDN connection signalling, ICMP Echo payload proposed here has low impact in terms of implementation on the UE and TWAG. The ICMP messages are echoed back to be compliant with RFC 792 and this adds a response (echo) by definition. Echoing the message takes additional network capacity for the echo message, but does not require significant processing in the TWAN/UE. Two such echoes are needed for each PDN connection setup. A full implementation of L3 control protocol would be more flexible and complete if the time and effort to develop it is acceptable - including its support on UE and TWAG.

If GAS frames are the chosen method to transport PDN connection signalling, it requires UEs that support WFA/HS2.0 and standards extensions in WFA/HS2.0. This method also requires APs to map the PDN signalling over GAS to backhaul protocol (e.g. RADIUS).

Editor's note: The implications of using RADIUS to transport the control protocol between AP - TWAN is FFS.

8.2.5.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 as well as simplicity of implementation in the UE should be evaluated.

8.2.6 Solution 6: X

This solution has been merged with the solution in clause 8.2.1

8.2.7 Solution 7: PPP over Ethernet (PPPoE)

8.2.7.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.7.1.1 Overview

The solution described in this clause does not require any new protocols. It is based on the well-known PPP and PPP over Ethernet (PPPoE) protocols, specified in RFC1661 and RFC2516, respectively. These protocols are used to implement both the control plane and the user plane.

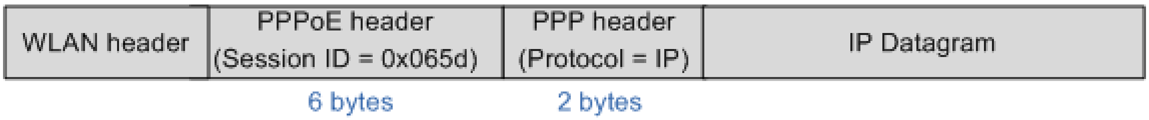
In summary, the solution is characterized by the following:

1. The solution supports two classes of UEs: (i) single-PDN UEs that support only a single PDN connection or NSWO over a trusted WLAN and (ii) multi-PDN UEs that support multiple simultaneous PDN connections over a trusted WLAN, in parallel to NSWO.

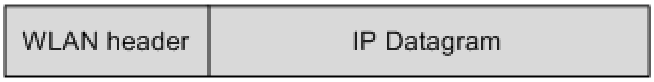
 1a. Single-PDN UEs do not support any new protocols for PDN connection management. These UEs support the Initial/Handover Attach procedure described in clause 8.2.7.2.1 but do not support the UE-Requested PDN connection establishment procedure described in clause 8.2.7.2.2. On the contrary, multi-PDN UEs must support the UE-Requested PDN connection establishment procedure by using the PPPoE/PPP protocols.

1b. A UE-Requested PDN Connection over a trusted WLAN (TWAN) is created by establishing a PPPoE/PPP session between the UE and TWAG (Trusted WLAN Access Gateway).

2. The PPPoE protocol is used to create a virtual point-to-point link between the UE and TWAG.
3. The UE encapsulates all traffic pertaining to a PDN connection into PPPoE frames (as shown below). These frames include a PPPoE session ID, which differentiates traffic between different PDN connections.



4. The TWAG binds a PPPoE session ID with a PDN connection. Traffic arrived from a certain PPPoE session ID is forwarded to the linked PDN connection and vice versa.
5. The TWAG behaves as an Access Concentrator that terminates both PPP and PPPoE protocols. It is very similar to a Broadband Remote Access Server (BRAS) function used in fixed broadband networks.
6. The UE needs to implement the PPP and PPPoE protocols only when it is multi-PDN capable. Both of these protocols are already available in most smartphone platforms. Note that there are already applications available which enable the user to establish PPPoE connections on a smartphone.
7. A Non-Seamless WLAN Offload (NSWO) connection does not use PPP or PPPoE. So, NSWO traffic is transmitted directly over WLAN without any PPPoE encapsulation (as shown below).



8. Since NSWO traffic does not use PPPoE, it does not necessarily need to be routed through TWAG. Instead, it can be optimally routed without going through TWAG. This allows TWAG to be offloaded from NSWO traffic. It also allows the WLAN network and the UE to support NSWO traffic with the currently deployed means (i.e. without any changes). However, the solution allows the AP to tunnel NSWO traffic to TWAG, if this is required.
9. There is no impact on the WLAN AP and on other legacy WLAN components. If the AP supports QoS on the WLAN air interface, it is assumed that the AP can still map between DSCP and WLAN QoS parameters.

The solution requires the following protocol extensions:

1. The EAP-AKA protocol is enhanced (as proposed by other solutions too) so that during the initial or handover attach to TWAN, the UE can indicate (i) its single-PDN /multi-PDN capability, (ii) whether it wants NSWO or EPC access and (iii) the desired APN, the PDN type and attach type. This can be easily supported by defining new 3GPP-specific EAP-AKA attributes as already done for other attributes (see e.g. AT_TRUST_IND, AT_IPMS_IND, AT_IPMS_RES).
2. To support the UE-Requested PDN Connection, the PPPoE protocol should be enhanced in order to enable the UE and TWAG to negotiate PDN connectivity parameters (such as APN, attach type) when a new PPPoE session is created. The Service-Name Tag within PPPoE could be used to transfer APN information and the Vendor-Specific tag could be specified for other parameters. This way the UE can also indicate the requested PDN type (IPv4/IPv6/IPv4v6), the attach type, etc.

The figure below illustrates the user-plane operation for a UE that concurrently has a NSWO connection and two PDN connections. Each of these PDN connections is established after the initial attach by executing the UE-Requested PDN connection procedure (see clause 8.2.7.2.1). Note that traffic for PDN connections is encapsulated in PPPoE frames while NSWO traffic does not require such encapsulation. Note also that each PPPoE frame carries a Session ID which is associated with a single PDN connection.

There is no requirement for NSWO traffic (i.e. traffic which does not traverse EPC) to be routed to TWAG. This enables TWAG offload and a single TWAG could support a larger number of UEs.

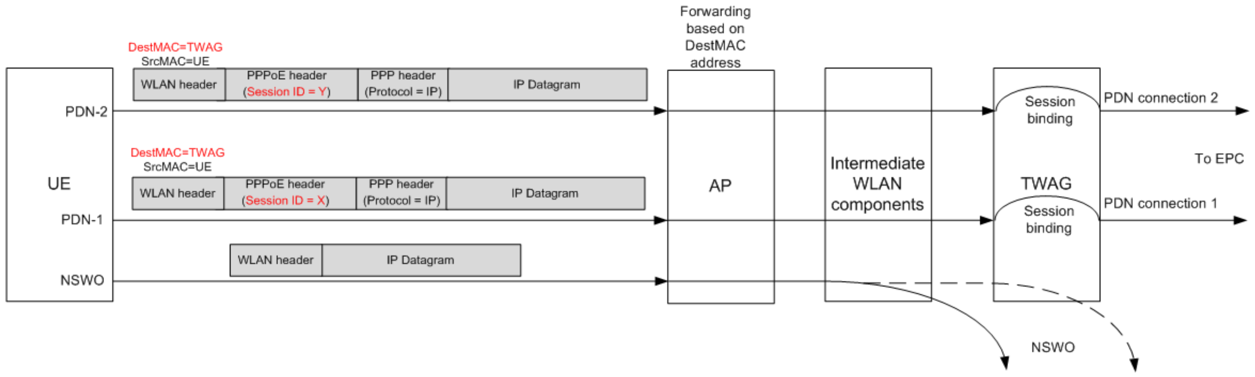


Figure 8.2.7.1.1-1: User plane operation when the UE has a NSWO connection and two PDN connections

The figure below shows a simplified UE protocol architecture for a UE that supports the UE-Requested PDN connection procedure and which concurrently has a NSWO connection and two PDN connections. Each PDN connection requires a PPPoE/PPP instance. NSWO traffic in the UE can be supported without the need for any new protocols.

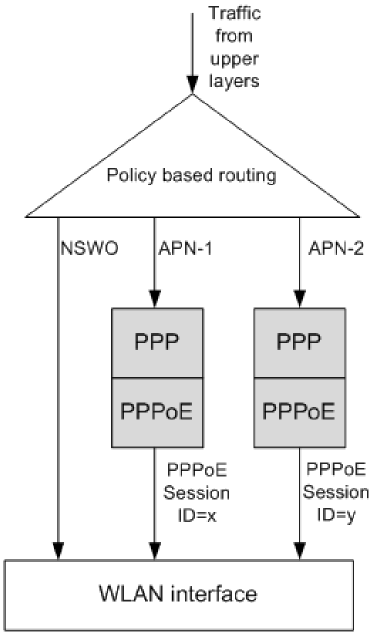


Figure 8.2.7.1.1-2: Simplified UE architecture with a non-seamless WLAN offload (NSWO) connection and two concurrent PDN connections

8.2.7.2 Procedures

8.2.7.2.1 Initial or Handover Attach over TWAN

The initial or handover attach is supported by single-PDN UEs and multi-PDN UEs.

During the initial or handover attach, the UE indicates to the network whether it is a single-PDN or a multi-PDN UE. If it is a single-PDN UE, it requests also a NSWO connection or a PDN connection. If it is a multi-PDN UE, it may request a NSWO connection. Note that multi-PDN UEs do not request a PDN connection during initial or handover attach. These UEs can use the UE-requested PDN connection establishment procedure (see clause 8.2.7.2.2) to request PDN connections.

The figure below illustrates a typical initial attach procedure for a multi-PDN UE that requests NSWO. Note that the request for NSWO is optional.

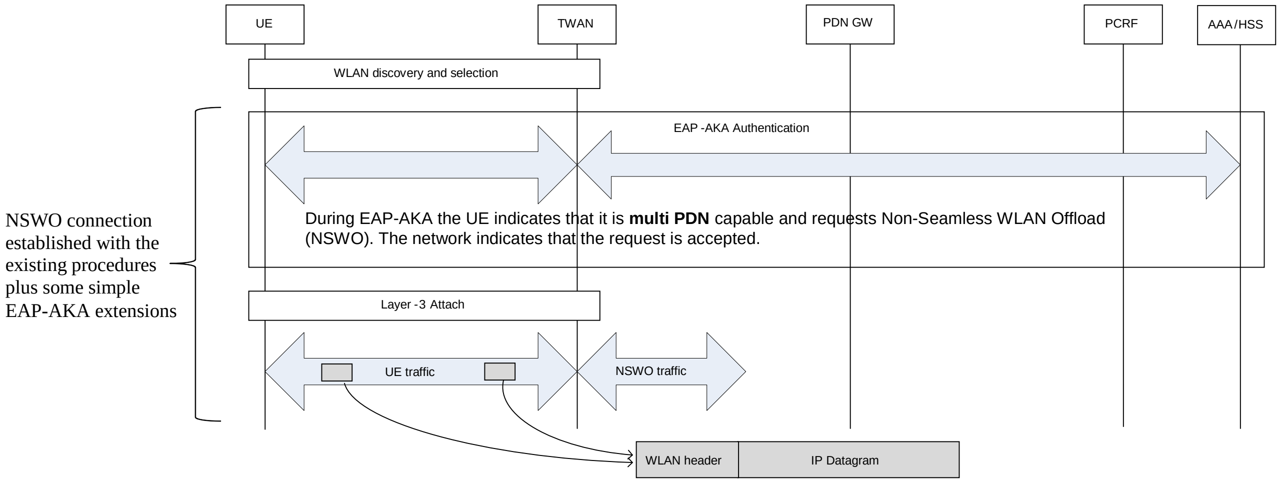

UE
TWAN
PDN GW
PCRF
AAA/HSS
WLAN discovery and selection
EAP-AKA Authentication
During EAP-AKA the UE indicates that it is **multi PDN** capable and requests Non-Seamless WLAN Offload (NSWO). The network indicates that the request is accepted.
NSWO connection established with the existing procedures plus some simple EAP-AKA extensions
Layer-3 Attach
UE traffic
NSWO traffic
WLAN header
IP Datagram

Figure 8.2.7.2.1-1: Initial attach for a multi-PDN UE that requests Non-seamless WLAN offload.

The initial or handover attach for a single-PDN UE that requests NSWO is shown in the figure 8.2.7.2.1-2.

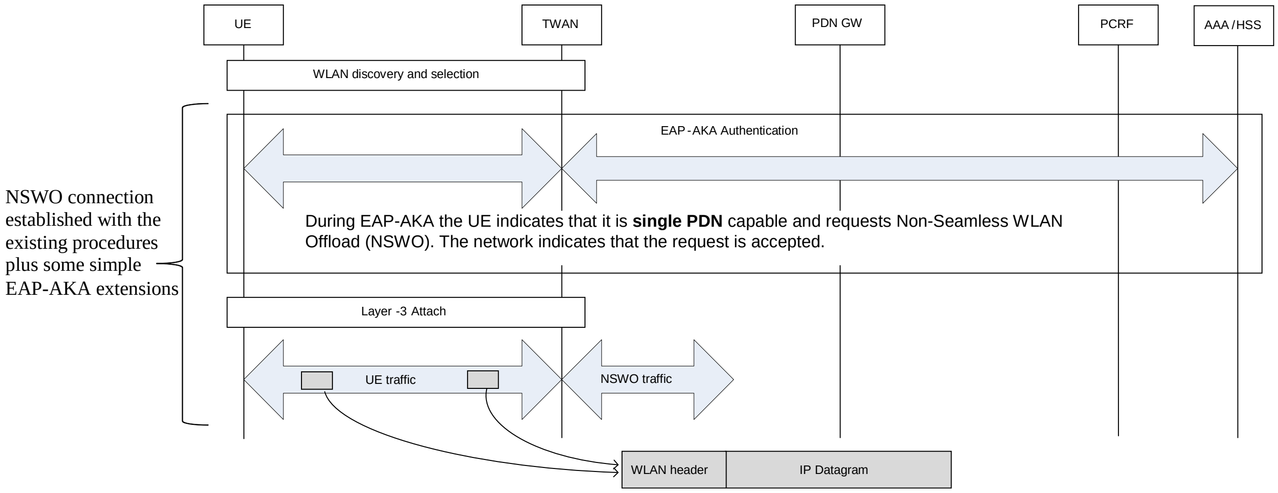

UE
TWAN
PDN GW
PCRF
AAA/HSS
WLAN discovery and selection
EAP-AKA Authentication
During EAP-AKA the UE indicates that it is **single PDN** capable and requests Non-Seamless WLAN Offload (NSWO). The network indicates that the request is accepted.
NSWO connection established with the existing procedures plus some simple EAP-AKA extensions
Layer-3 Attach
UE traffic
NSWO traffic
WLAN header
IP Datagram

Figure 8.2.7.2.1-2: Initial attach for a single-PDN UE that requests Non-seamless WLAN offload.

Figure 8.2.7.2.1-3 shows an initial or handover attach for a single-PDN UE that requests EPC access. The UE requests the associated PDN connectivity parameters, e.g. APN, PDN type and attach type (e.g. "initial attach" or "handover attach"). The request for EPC access and the associated PDN connectivity parameters are negotiated during EAP-AKA authentication with new 3GPP-specific attributes. Note that the figure 8.2.7.2.1-3 shows a case when a layer-3 trigger is used for initiating the PDN connection in the network. However, layer-2 triggers can be easily supported too.

It is noted that the single-PDN UE is not involved in the PDN connection establishment. Thus, during initial or handover attach the UE does not need to support any new protocols for explicitly requesting a PDN connection. The UE only provides the requested PDN connectivity parameters during EAP-AKA and lets the trusted WLAN to setup the PDN connection.

When a single-PDN UE detaches from the WLAN, its PDN connection can be either released (as specified in TS 23.402 [3], clause 16.3) or can be handed over to 3GPP access (by using existing non3GPP-to-3GPP handover procedures specified in TS 23.402 [3]).

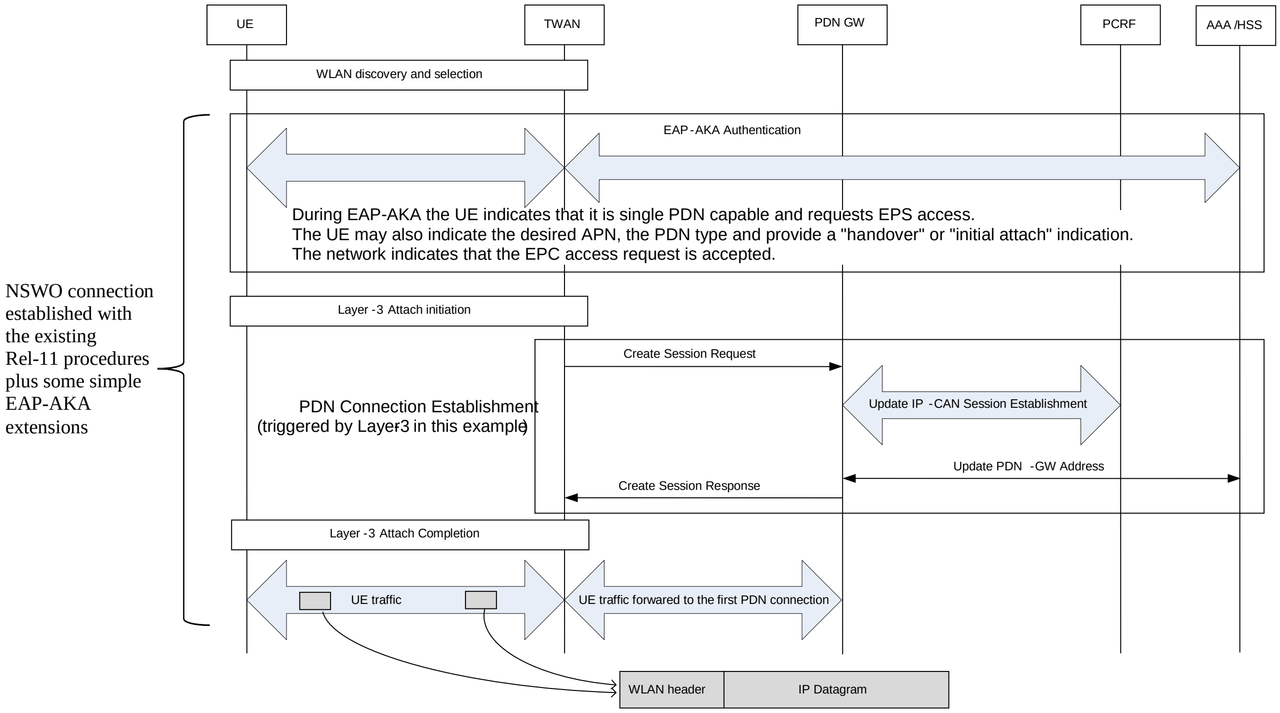

UE
TWAN
PDN GW
PCRF
AAA /HSS
WLAN discovery and selection
EAP-AKA Authentication
During EAP-AKA the UE indicates that it is single PDN capable and requests EPS access.
The UE may also indicate the desired APN, the PDN type and provide a "handover" or "initial attach" indication.
The network indicates that the EPC access request is accepted.
NSWO connection established with the existing Rel-11 procedures plus some simple EAP-AKA extensions
Layer -3 Attach initiation
Create Session Request
PDN Connection Establishment (triggered by Layer-3 in this example)
Update IP -CAN Session Establishment
Update PDN -GW Address
Create Session Response
Layer -3 Attach Completion
UE traffic
UE traffic forwarded to the first PDN connection
WLAN header
IP Datagram

Figure 8.2.7.2.1-3: Initial or handover attach for a single-PDN UE that requests EPC access

8.2.7.2.2 UE-Requested PDN Connection Establishment

The UE-requested PDN connection establishment procedure is supported only by multi-PDN UEs.

After the initial attach or handover attach, a multi-PDN UE may use the PPPoE/PPP protocols to explicitly request a PDN connection to EPC. This PDN connection will co-exist with the NSWO connection (if any) established during the initial or handover attach.

As shown in figure 8.2.7.2.2-1, the UE-requested PDN connection establishment procedure is invoked when the UE needs to establish a PDN connection after the initial/handover attach. Only in this case the UE must use the PPPoE/PPP protocols.

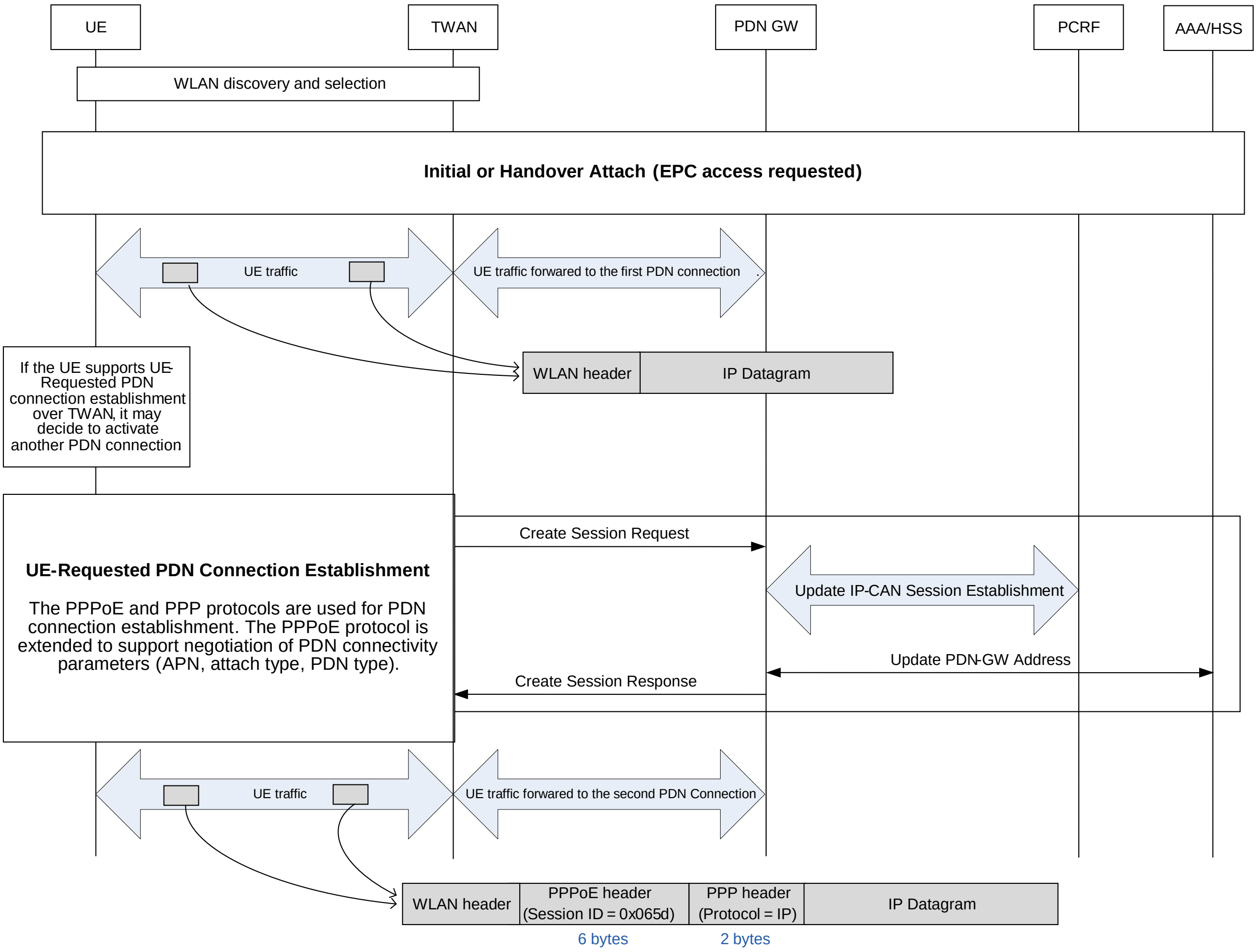

UE
TWAN
PDN GW
PCRF
AAA/HSS
WLAN discovery and selection
Initial or Handover Attach (EPC access requested)
UE traffic
UE traffic forwarded to the first PDN connection
WLAN header
IP Datagram
If the UE supports UE-Requested PDN connection establishment over TWAN, it may decide to activate another PDN connection
UE-Requested PDN Connection Establishment
The PPPoE and PPP protocols are used for PDN connection establishment. The PPPoE protocol is extended to support negotiation of PDN connectivity parameters (APN, attach type, PDN type).
Create Session Request
Update IP-CAN Session Establishment
Update PDN-GW Address
Create Session Response
UE traffic
UE traffic forwarded to the second PDN Connection
WLAN header
PPPoE header (Session ID = 0x065d)
PPP header (Protocol = IP)
IP Datagram
6 bytes
2 bytes

Figure 8.2.7.2.2-1: Initial attach followed by UE-Requested PDN connection establishment.

The figure 8.2.7.2.2-2 illustrates the details of the UE-requested PDN connection procedure and shows how a PDN connection can be established by negotiating the PDN connectivity parameters with the PPPoE protocol.

When a multi-PDN UE decides to activate a PDN connection (with type IPv4) over the TWAN, it uses the normal PPPoE procedures to discover the TWAG and to establish a new PPPoE session with the TWAG. A new session ID is allocated by TWAG to this PPPoE session (for example Session ID=0x065d, as shown in figure 8.2.7.2.2-2). In the PPPoE Discovery Request message the UE includes in the existing Service-Name tag (see RFC2516) the requested APN. Also, in a Vendor-Specific tag (the details of which should be specified by 3GPP) the UE includes the attach type and the requested PDN type. After the PPPoE session is established, the TWAG may start the GTP/PMIP tunnel over S2a establishment, which can result in fast PDN connection creation.

After the PPPoE session is established the UE initiates the normal PPP session establishment procedures. Note that after the LCP negotiation:

- The standard PPP authentication could be used if the requested PDN connection is needed for "Non-Transparent access to an Intranet or ISP" (see TS 29.061); or
- The standard PPP authentication could be skipped, if the requested PDN connection is needed for "Transparent access to the Internet" (see TS 29.061). In this case, even when the UE sends a PPP authentication request the TWAG may always accept it.

After the LCP negotiation, the UE requests configuration data with the IPCP protocol and/or with the IPv6 Control Protocol (IPV6CP), as specified in RFC 5072, "IPv6 over PPP". If the negotiated PDN Type is IPv4v6, the UE establishes two PPP sessions, one with IPCP and another with IPV6CP.

For establishing a PDN connection with type IPv6, the UE uses the IPV6CP protocol. With IPV6CP, the UE negotiates an "Interface-Identifier" (a 64-bit interface identifier) to be used for address autoconfiguration. On the established PPP session the UE receives a Router Advertisement and, based on its content, the UE uses either stateless or stateful autoconfiguration. Since the Router Advertisement is sent to UE over a PPPoE point-to-point link, it is possible to use stateless autoconfiguration in a similar manner as used over 3GPP RAN, i.e. the UE can receive the /64 IPv6 prefix in the RA message. Moreover it is also possible to use stateful autoconfiguration for some UEs (although this is not typically needed).

As noted above, the established PDN connection is associated with an underlying PPPoE session, identified by a unique PPPoE session ID. Any uplink packets transmitted by the UE with this PPPoE session ID are forwarded to the associated PDN connection. Also, any downlink packets received by TWAN for the associated PDN connection are forwarded to UE with the corresponding PPPoE session ID.

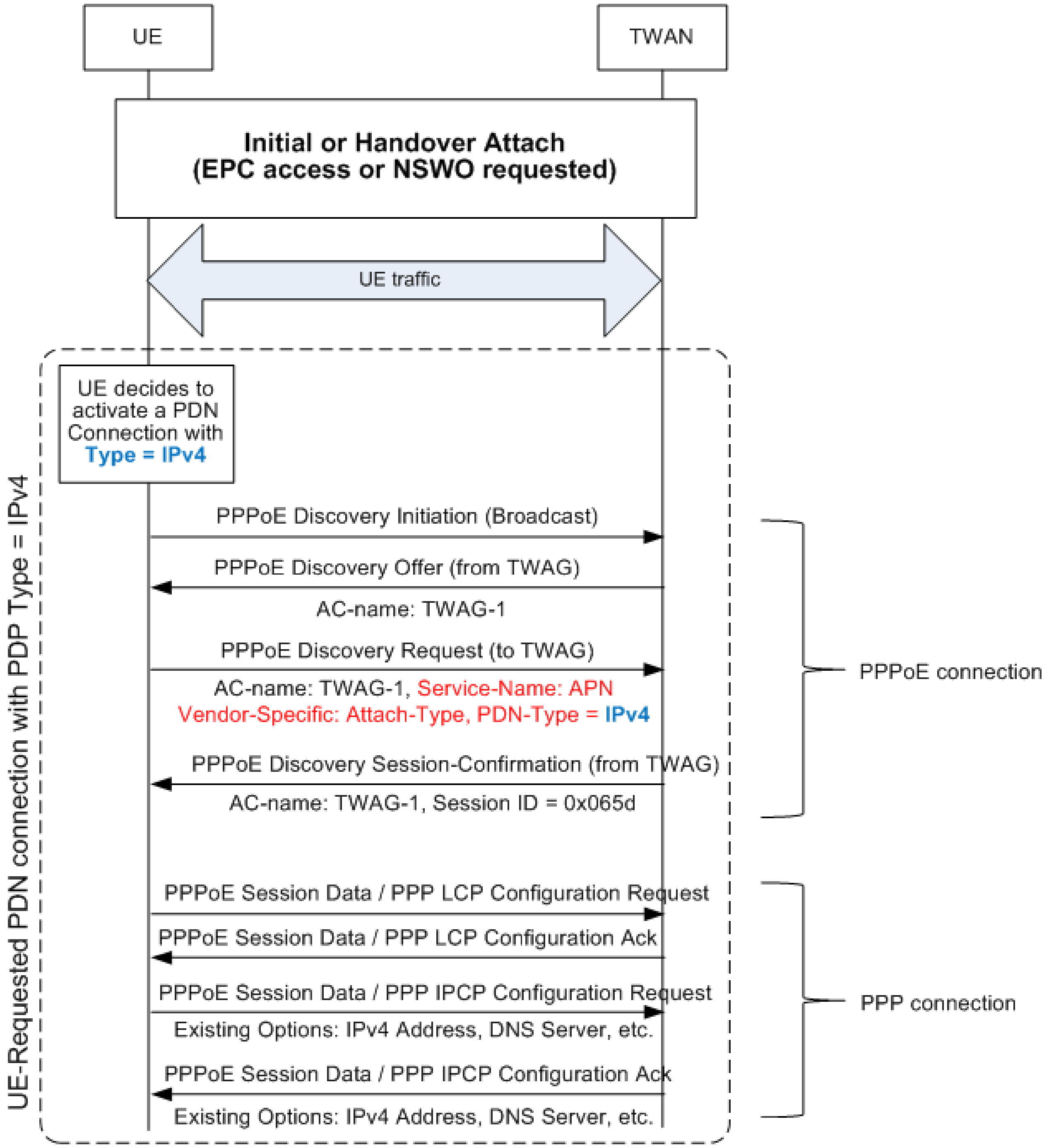

UE
TWAN
Initial or Handover Attach
(EPC access or NSWO requested)
UE traffic
UE-Requested PDN connection with PDP Type = IPv4
UE decides to activate a PDN Connection with Type = IPv4
PPPoE Discovery Initiation (Broadcast)
PPPoE Discovery Offer (from TWAG)
AC-name: TWAG-1
PPPoE Discovery Request (to TWAG)
AC-name: TWAG-1, Service-Name: APN
Vendor-Specific: Attach-Type, PDN-Type = IPv4
PPPoE Discovery Session-Confirmation (from TWAG)
AC-name: TWAG-1, Session ID = 0x065d
PPPoE connection
PPPoE Session Data / PPP LCP Configuration Request
PPPoE Session Data / PPP LCP Configuration Ack
PPPoE Session Data / PPP IPCP Configuration Request
Existing Options: IPv4 Address, DNS Server, etc.
PPPoE Session Data / PPP IPCP Configuration Ack
Existing Options: IPv4 Address, DNS Server, etc.
PPP connection

Figure 8.2.7.2.2-2: UE-Requested PDN connection establishment

The signalling flow shown in the figure above is based on known steps already used in practice. The only extension required is the new PPPoE extensions that allow the negotiation of PDN connectivity parameters between the UE and TWAG.

8.2.7.2.3 UE-Requested and Network-Requested PDN Connection Release

PDN connections established with the UE-requested PDN connection establishment procedure can be released either by the UE or by the network with the procedures specified below.

The figure below illustrates the control-plane signalling flow when the UE initiates a PDN connection release. The UE simply terminates the corresponding PPP session and subsequently terminates the associated PPPoE session too.

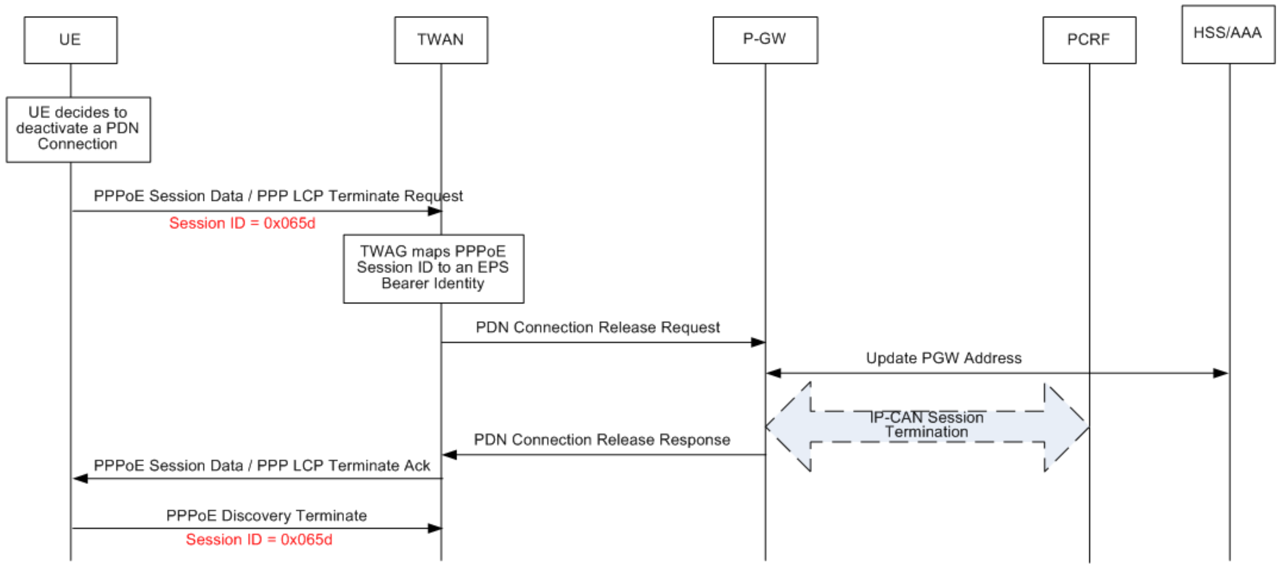

UE
TWAN
P-GW
PCRF
HSS/AAA
UE decides to deactivate a PDN Connection
PPPoE Session Data / PPP LCP Terminate Request
Session ID = 0x065d
TWAG maps PPPoE Session ID to an EPS Bearer Identity
PDN Connection Release Request
Update PGW Address
IP-CAN Session Termination
PDN Connection Release Response
PPPoE Session Data / PPP LCP Terminate Ack
PPPoE Discovery Terminate
Session ID = 0x065d

Figure 8.2.7.2.3-1: PDN connection release initiated by UE.

The figure below illustrates the control-plane signalling flow when the P-GW initiates a PDN connection release. Note that the TWAN could also initiate the PDN connection release. In this case, the TWAN terminates the PPP session with the UE and sends the Delete Session Request to P-GW.

The TWAG may use the standard LCP Echo Request/Reply procedure (or other link management facilities provided by PPPoE) to determine when a UE becomes unreachable. In this case, the TWAG may detach the UE from EPC by releasing all its PDN connections.

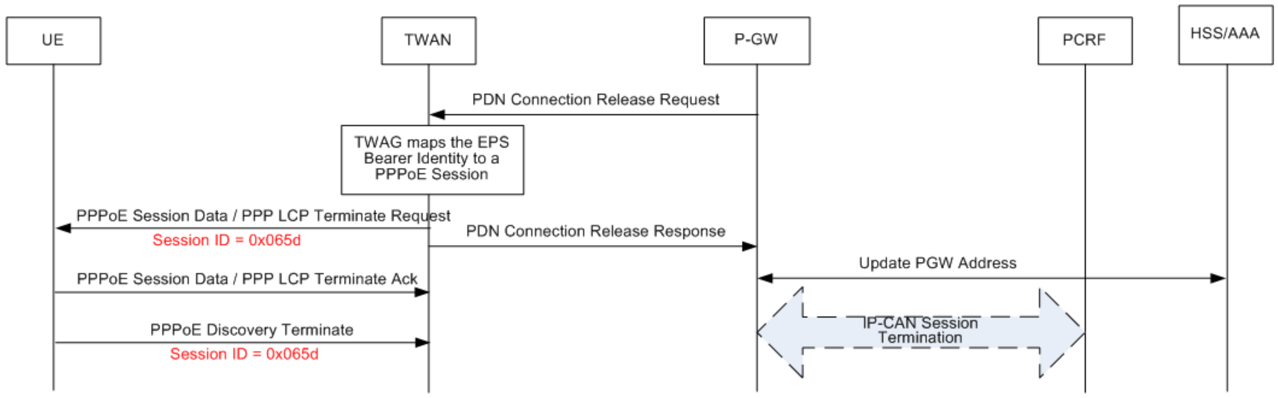

UE
TWAN
P-GW
PCRF
HSS/AAA
PDN Connection Release Request
TWAG maps the EPS Bearer Identity to a PPPoE Session
PPPoE Session Data / PPP LCP Terminate Request
Session ID = 0x065d
PDN Connection Release Response
PPPoE Session Data / PPP LCP Terminate Ack
Update PGW Address
IP-CAN Session Termination
PPPoE Discovery Terminate
Session ID = 0x065d

Figure 8.2.7.2.3-2: PDN connection release initiated by P-GW.

8.2.7.2.4 Handover from 3GPP access to WLAN

A single-PDN UE can handover a PDN connection from 3GPP access to WLAN with a handover attach, as specified in clause 8.2.7.2.1. A multi-PDN UE can handover a PDN connection from 3GPP access to WLAN with a UE-Requested PDN connection procedure, as specified in clause 8.2.7.2.2. In the single-PDN case, the UE provides the associated APN and "attach type = handover" during the EAP-AKA procedure. In the multi-PDN case, the UE provides the associated APN and "attach type = handover" during the PPPoE session establishment. In both cases, existing procedures are used (e.g. procedures specified in TS 23.402 [3] for IP address preservation) to make sure that the PDN connection over the trusted WLAN uses the same PGW and the same IP address that was used over 3GPP access.

8.2.7.2.5 Handover from TWAN to 3GPP access

The existing procedures specified in TS 23.402 [3], clause 8, can be used to support handover from TWAN to 3GPP access.

8.2.7.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

8.2.7.4 Evaluation

This solution can support deployments with *single-PDN* UEs and *multi-PDN* UEs. A Rel-12 network has to support these types of UEs.

i) Impacts to existing network deployment

a. New requirements on WLAN APs compared to Rel-11

None

b. Additional assumptions on AP-TWAG link

None beyond those of SAMOG Rel11

ii) Impacts to UE

Single-PDN UEs must support EAP-AKA' extensions

In addition, multi-PDN UEs must support the PPPoE/PPP protocols, including the specified PPPoE extensions

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA')

EAP-AKA' should be extended with additional attributes to support capability negotiation and PDN connectivity parameters (e.g. APN, etc.) negotiation

iv) Impacts to protocols defined by other SDOs (e.g. DHCP)

None

v) Control plane

a. Latency/load of first/additional PDN connections setup and handover procedures

NSWO traffic does not need to go through TWAG. This enables TWAG offload and can lead to deployments with reduced cost.

NSWO traffic is transmitted without any encapsulation. This improves air-interface utilization and reduces complexity.

There is no need for special signalling to establish tunnels / point-to-point connections for NSWO traffic. This improves efficiency and reduces complexity.

For single-PDN UEs, the PDN connection is established during the initial/handover attach to TWAN without any UE involvement, other than providing the requested PDN connectivity parameters during EAP-AKA'. The simplicity of this PDN connection establishment can greatly simplify the implementation of single-PDN UEs.

For multi-PDN UEs, the PDN connection is established with a regular PPP LCP and IPCP (or IPV6CP) exchange. The existing PPPoE protocol is used for TWAG discovery and negotiation of PDN parameters. The PDN connection establishment can be expedited since the requested PDN parameters are provided early during the PPPoE session establishment phase.

b. Network element impacts (e.g. AAA signalling etc.)

AAA to relay some information of EAP-AKA' signalling at initial/handover attach. No new message exchange required to support at AAA level.

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements

a. Co-existence with Rel-11 SaMOG

b. Support for IP address preservation during handover

c. Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDN connections

d. Compliant with all requirements

vii) Others functional limitations

None

In summary, the solution supports the following capabilities:

1. For single-PDN UEs the PDN connection can be established during initial attach with minimal UE involvement (maintaining the simplicity of Rel-11).

   a) Supports one or more concurrent PDN connections for multi-PDN UEs.. Each PDN connection requires a PPP/PPPoE protocol instance in the UE and in the TWAG.

2. Supports NSWO traffic and concurrently EPC traffic (via one or more PDN connections).

3. Supports IPv4, IPv6 and IPv4v6 PDN connections.

4. Supports IPv6 stateless autoconfiguration. It does not mandate stateful DHCPv6, thus simplifies UE implementation.

5. Supports PDN connection handover from 3GPP to TWAN with IP address preservation.

6. Supports TWAG discovery by means of standard PPPoE procedures.

7. Supports PDN connections for "Non-Transparent access to an Intranet or ISP" and for "Transparent access to the Internet" (see TS 29.061). Standard PPP authentication can be used to authenticate PDN connections for "Non-Transparent access to an Intranet or ISP".

8. Supports SaMOG phase-2 capable UEs and "legacy" (pre-Rel-12) UEs on the same TWAN (and on the same SSID).

The solution is also characterized by the following features:

1. It is based on the well-known PPP/PPPoE protocols. Thus avoids the effort to standardize and implement new protocols in the UE and in the network. In addition, it minimizes the need for new conformance specifications; only conformance testing against the new PPPoE configuration options and EAP-AKA attributes is required.

2. The PPP/PPPoE protocols are already supported by many smartphones (typically as build-in or loadable kernel modules). Thus, UE modifications are minimized. UE modifications are further minimized for single-PDN UEs which are not required to support new protocols, not even PPPoE/PPP.

3. Standard PPP/PPPoE procedures can be used to monitor the link between the UE and TWAG. For example, the TWAG may use the standard LCP Echo Request/Reply procedure to determine when a UE becomes unreachable and then trigger Detach procedures.

4. The standard PPP LCP protocol can be used to negotiate an MTU for each PDN connection.

5. The standard PPP Compression Control Protocol (CCP) can be used to enable data compression between the UE and TWAG. Although CCP is not considered necessary over WLAN, it is a readily available option for deployment.

6. It is supported by existing WLAN APs. PPPoE frames can traverse existing WLAN APs without any modification. When the AP supports QoS on the WLAN air interface, it is expected that the AP can still map between DSCP and WLAN QoS parameters.

The solution requires the following protocol extensions:

1. The EAP-AKA protocol should be enhanced so that during the initial or handover attach to TWAN, the UE can indicate (i) its single-PDN/multi-PDN capability, (ii) whether it wants NSWO or EPC access and (iii) the desired APN, PDN type, attach type. This can be easily supported by defining new 3GPP-specific EAP-AKA attributes as already done for other attributes (see e.g. AT_TRUST_IND, AT_IPMS_IND, AT_IPMS_RES).
2. The PPPoE protocol should be enhanced in order to enable the UE and TWAG to negotiate PDN connectivity parameters (such as APN, PDN type, attach type) when a new PPPoE session is created.

8.2.8 Solution 8: Solution using new 3GPP specific LLC/SNAP header settings

8.2.8.1 Functional Description

8.2.8.1.1 General

This solution addresses the user plane problem of supporting multiple PDN connections between the UE and the TWAG.

The solution has the following aspects:

a) Works both for the case where an AP only supports 802.11 ↔ Ethernet II bridging or where it supports 802.3 ↔ 802.11 bridging.

b) The LLC Address field on the wireless link (and optionally on the 802.3 LAN, if 802.3 is used) is always set to indicate that a SNAP header is present.

c) The OUI (Organisationally Unique Identifier) of the SNAP header on the wireless link (and optionally on the 802.3 LAN, if 802.3 is used) is set to the value used in RFC 1042 (00 00 00).

d) 3GPP requests x (TBD) new EtherType values from the IEEE Registration Authority (note that: a request to IEEE RA for 12 EtherType values would be sufficient for supporting up to the maximum of 11 PDN connections per UE with one spare for support of a 3GPP control plane protocol if needed). These EtherTypes will be sufficient in number to provide differentiation between PDN connections as well as differentiation of any 3GPP control plane protocol that needs to be supported.

e) These new EtherType values are directly mapped onto the SNAP Protocol Type field on the 802.11 network. On an Ethernet II network these new EtherType values are used to populate the EtherType field (and there is a one to one mapping between 802.11 Protocol Type and Ethernet II EtherType). On an 802.3 fixed network the EtherType values are used to populate the Protocol Type field (and there is a one to one mapping between SNAP Protocol Type on 802.11 and SNAP Protocol Type on 802.3 in the bridging function).

f) In the uplink, the combination of source (device) MAC address and EtherType value can be used by the TWAG to bind the traffic to the appropriate GTP tunnel. In the downlink the TWAG binds the GTP tunnel to the appropriate Ethernet II 'link' by appropriate setting of the destination (device) MAC address and EtherType value.

g) The allocation of a particular EtherType/Protocol Type value to a particular user plane PDN connection can be established dynamically via signalling.

h) Since conventionally EtherType is used to indicate the higher layer protocol type that is associated with the payload, a method is needed by which the UE or TWAG can differentiate between IPv4 and IPv6 in the case of a dual stack PDN connection. This issue is solved at the IP layer since the UE or TWAG can inspect the first 4 bits of the payload to determine the IP type of the packet. In both IPv4 and IPv6 the first 4 bits of the payload convey 'version' of the IP packet. In IPv4 'version' takes the value '4' and in IPv6 it takes the value '6'. Note that an assumption here is that the only types of packet which need to be carried on the PDN connection are packets of type IPv4 and IPv6.

8.2.8.1.2 Protocol stack

Figure 8.2.8.1.2-1 shows an example user plane protocol stack for this solution where the AP and TWAG are implemented separately and the AP provides a bridging function to an 802.3 LAN.

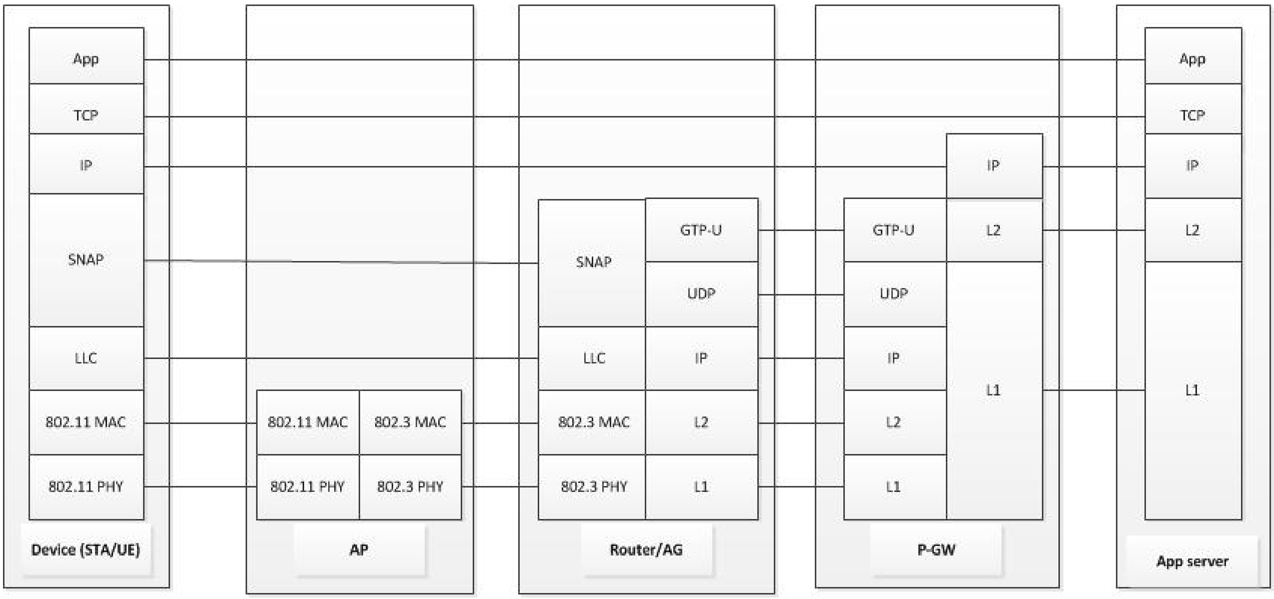


Figure 8.2.8.1.2-1: Example user plane protocol stack where 802.11 ↔ 802.3 bridging is used

Figure 8.2.8.1.2-2 shows an example user plane protocol stack where the AP and TWAG are implemented separately and the AP provides a bridging function to an Ethernet II LAN.

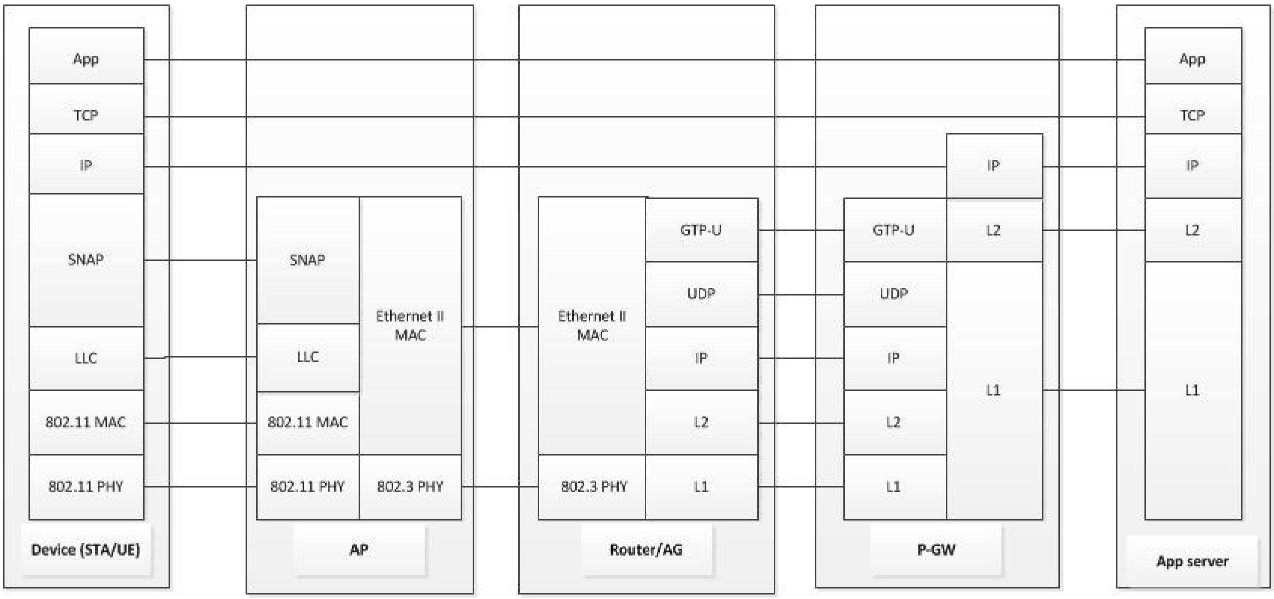
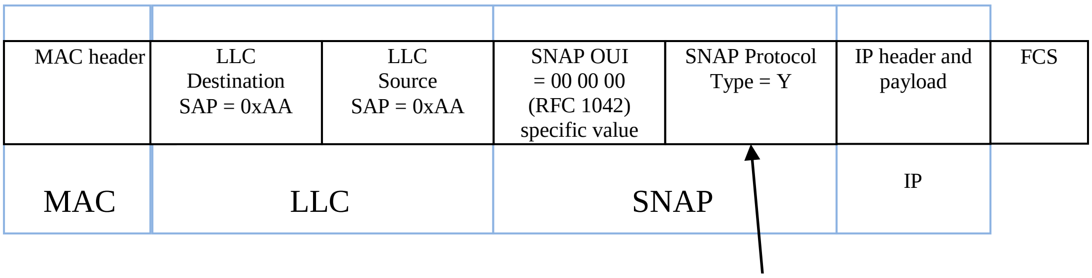


Figure 8.2.8.1.2-2: Example user plane protocol stack where 802.11 ↔ Ethernet II bridging is used

8.2.8.1.3 Protocol header

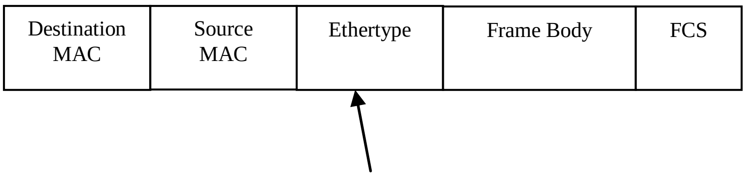
Figure 8.2.8.1.3-1 shows the population of LLC and SNAP fields on 802 (W)LAN's.



Y is an EtherType value that has been allocated to 3GPP by the IEEE Registration Authority and which may correspond to a specific PDN connection. The mapping between a given value Y and a given PDN connection is established via signalling.

Figure 8.2.8.1.3-1: User plane packet as seen on an 802 (W)LAN

Figure 8.2.8.1.3-2 shows the population of the MAC header on an Ethernet II packet.



The EtherType value would be one that has been allocated to 3GPP by the IEEE Registration Authority and which may correspond to a specific PDN connection. The mapping between a given EtherType value and a given PDN connection is established via signalling. The EtherType value is the same as that which is used in the Protocol Type field across the wireless 802.11 interface

Figure 8.2.8.1.3-2: User plane packet as seen on an Ethernet II wired interface

8.2.8.2 Procedures

An LLC/SNAP user plane solution can be used in conjunction with a variety of the signalling solutions which are described as part of other solutions in this TR. These signalling possibilities are now discussed and any modifications to those proposals which are required in order to support the LLC/SNAP based user plane solution are described.

It is worth noting that some of the signalling options presented within other solutions make use of new signalling protocols which would be defined by 3GPP. The LLC/SNAP solution can provide support for such protocols. This is achieved simply by reserving one of the 3GPP specific EtherType values for this purpose. For example an EtherType value *p* could correspond to a 3GPP specified control plane protocol that runs between the UE and the TWAG. If either the UE or the TWAG receives a frame with an EtherType value set to *p* then it would process the frame contents as a 3GPP control plane frame. Note that this reserved value *p* would be defined in a 3GPP specification and would not be dynamically changeable.

Non Seamless Wireless Offload (NSWO) could be supported by the device in the way that the device would typically use today when directly accessing the internet over WLAN (e.g. SNAP OUI set to 00 00 00 (RFC 1042) and SNAP Protocol Type set to the EtherType value corresponding to the appropriate higher layer protocol (IP=0x0800, ARP=0x0806), and with IP address locally allocated by the TWAN).

From a signalling point of view the UE needs to learn both the MAC address of the TWAG and the EtherType value that it should use for a given PDN connection. Regards the former issue, an approach which will be common to many if not all of the signalling solutions will be for the UE to determine the MAC address of the TWAG through DHCP/ARP messaging using a broadcast 802.11 MAC address. The TWAG also needs to learn the MAC address of the device and the EtherType values that should be bound with given GTP tunnels.

NOTE: Because with this proposal EtherType is encapsulated in a Protocol Type field on an 802.3 LAN or on an 802.11 WLAN, and since EtherType is always used on Ethernet II, in the remainder of this clause we will in general just use the term 'EtherType' as opposed to 'Protocol Type'.

Table 8.2.8.2-1

Solution	Signalling aspects of solution compatible with SNAP/LLC user plane solution?	Comment
Solution 1: Two Scenario Approach	Yes	The proposed UE-TWAG Wireless LAN Control Protocol (WLCP) can be supported by defining, in a 3GPP specification, one of the 3GPP specific EtherType values for use in carrying WLCP frames. As part of the 'UE initiated Connectivity to PDN in WLAN GTP S2a' procedure the TWAG allocates an EtherType value for each PDN connection which is being established and indicates this EtherType assignment and its association with a specific PDN connection to the UE using WLCP. Other procedures such as handover and PDN disconnection procedures make use of WLCP in the same way. - UE learns TWAG MAC address: DHCP/ARP on broadcast MAC addr - UE learns EtherType/PDN connection binding: WLCP - TWAG learns device MAC address: WLCP - TWAG learns GTP/EtherType binding: TWAG configures it
Solution 2: Layer 2 solution based on per-APN/NSWO VLAN marking	Yes	The first preparation step within the 'UE requested PDN or NSWO connectivity' (clause 8.2.2.1.3) procedure would be modified so that the UE can be informed, for each APN, of one EtherType value to be used for conveying user plane traffic and a second value to be used for conveying DHCP traffic that is associated with that APN. This request and response signalling takes place via extensions to EAP-AKA or ANQP. In the second execution step of this procedure the UE sends a DHCP request message using the EtherType value which has been allocated for carrying DHCP messages that is associated with the particular APN for which the IP address is being requested. When the TWAG receives this message it can determine, using the source (device) MAC address and the EtherType setting for which PDN the session is to be set up. The DHCP signalling from TWAG to the UE which carries the allocated IP address also makes use of this APN and DHCP specific EtherType header value when building the Layer 2 frame, so that the UE can associate the allocated IP address with the correct PDN connection. Similarly, PDN disconnection makes use of the same EtherType values at Layer 2 for conveying the DHCP signalling to release the IP address. If this signalling approach were to be adopted and if up to 11 APN's per device are to be supported then 3GPP would need to request 22 EtherType values from the IEEE RA. - UE learns TWAG MAC address: DHCP/ARP on broadcast MAC addr - UE learns EtherType/PDN connection binding: EAP-AKA / ANQP - TWAG learns device MAC address: During second DHCP execution step - TWAG learns GTP/EtherType binding: TWAG configures it
Solution 3: Stateful DHCP based solution	Yes	The DHCP messaging is modified so that instead of the UE / TWAG indicating GRE keys the UE /TWAG indicates the EtherType value that will be used by certain PDN connections. - UE learns TWAG MAC address: DHCP/ARP on broadcast MAC addr - UE learns EtherType/PDN connection binding: modifications to DHCP - TWAG learns device MAC address: DHCP procedure - TWAG learns GTP/EtherType binding: TWAG configures it
Solution 4	N/A	No signalling solution provided.

Solution 5: Associating APN/PDN with virtual IP interface	Partially (some aspects of the solution may be used in conjunction with SNAP/LLC based approach)	Solution 8 (SNAP/LLC based user plane) does support the use of a new 3GPP defined 'PDN Control protocol' as is defined as part of this solution. However, the methods described in Solution 5 for transporting the 'PDN Control Protocol', e.g. use of ICMP Echo payload or 802.11 GAS frame are competing methods to the approach proposed in Solution 8 (which instead would support such a 'PDN Control protocol' through the use of a specific EtherType value). (See for example comments under solution 1)
Solution 6: X	Yes	This approach proposes the use of a new 3GPP specified TSM (TWAN Session Management) control plane protocol to run between the UE and the TWAG. Solution 8 provides support for a new control plane protocol as discussed above. Instead of delineating PDN connections through VLAN ID or TWAG MAC address, if this signalling solution were to be combined with Solution 8 then Ethertype would be used to distinguish between PDN connections. These settings would be conveyed between UE and TWAG within the TSM protocol. - UE learns TWAG MAC address: DHCP/ARP on broadcast MAC addr - UE learns EtherType/PDN connection binding: TSM - TWAG learns device MAC address: TSM - TWAG learns GTP/EtherType binding: TWAG configures it
Solution 7: PPP over Ethernet (PPPoE)	No	If a PPPoE approach is adopted for signalling then it would seem logical to use it in conjunction with the PPPoE user plane solution.
Solution 8 - Solution using new 3GPP specific LLC/SNAP header	N/A	
Solution 9 - EAP based signalling solution	Yes	EAP based signalling can be used for conveying the association between a specific PDN connection and an EtherType value. - UE learns TWAG MAC address: DHCP/ARP on broadcast MAC addr or EAP - UE learns EtherType/PDN connection binding: EAP modification. - TWAG learns device MAC address: May require TWAN internal signalling to communicate this setting to the TWAG from the entity terminating EAP. - TWAG learns GTP/EtherType binding: TWAN sets it. May require TWAN internal signalling to communicate this setting to the TWAG.

8.2.8.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

8.2.8.4 Evaluation

The evaluation of this user plane solution against relevant evaluation criteria is provided below:

i) Impacts to existing network deployment

  a. New requirements on WLAN APs compared to Rel-11

    i. No new requirements

  b. Additional assumptions on AP-TWAG link

    i. No additional assumptions

ii) Impacts to UE

  a. UE needs to populate EtherType value appropriately for the given PDN connection / control plane protocol.

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA')

  a. N/A (Solution 8 defines user plane solution between UE and TWAG)

iv) Impacts to protocols defined by other SDOs (e.g. DHCP)

a. No impact to protocols.

i. 3GPP would need to ask the IEEE Registration Authority for multiple (e.g. 12) new EtherType values to be allocated for use by 3GPP.

v) Control plane

a. Latency/load of first/additional PDN connections setup and handover procedures

i. N/A (Solution 8 is a user plane solution)

b. Network element impacts (e.g. AAA signalling etc.)

i. N/A (Solution 8 is a user plane solution)

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements

a. Co-existence with Rel-11 SaMOG

i. This solution can coexist with Rel-11 SaMOG on the user plane.

b. Support for IP address preservation during handover

i. N/A (Solution 8 is a user plane solution)

c. Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDN connections

i. This is supported.

vii)Others functional limitations

i. None

8.2.9 Solution 9: EAP based signalling solution

8.2.9.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.9.1.1 General

In this solution all 3GPP specification signalling between the UE and the network is carried within EAP signalling. This solution is based on defining a new attribute for EAP to transfer 3GPP specific information (e.g. APN, handover indication) between the UE and the network. This type of new attribute for EAP is also needed if EAP is used to create the first PDN connection at initial attach, but other mechanisms are used for creating additional PDN connections as it is described e.g. in solution 1 (clause 8.2.1). The solution works in the following way.

1) How the UE triggers the creation of the new PDN Connections:

The assumption is that the UE has already been authenticated to the TWAN. When a new PDN Connection needs to be created the UE sends an IEEE 802.1X EAPoL Start message to the authenticator. The authenticator responds, as it must, with EAP-Request/Identity. The UE responds to this as expected for a re-authentication. The UE indicates the APN and other 3GPP specific parameters within the EAP-Response/AKA'-Reauthentication and EAP-Response/AKA'-Challenge messages in a new EAP attribute.

2) How the EAP-Server indicates the support for the functionality described in this solution:

The network can indicate the support for the functionality described in this solution within EAP-Request/AKA'-Reauthentication and EAP-Request/AKA'-Challenge messages in a new EAP attribute.

3) How the network indicates to the UE that the creation of the new PDN Connection failed:

A new AT_NOTIFICATION notification code has to be defined. This code is sent by the EAP-server in EAP-Request/AKA'-Notification to the UE. The general rule is that both S and P bits must be set to 0, i.e. indicating an error after a successful authentication, because the APN & PDN specific authorization failed.

4) How the network indicates to the UE that the creation of the PDN succeeded:

A network specific information prior to or during the PDN Connection establishment is sent to the UE using a success-indicating EAP-Request/AKA'-Notification (such as VLAN tags, selected APN).

5) How the UE or the network initiates a deletion of the PDN Connection.

A UE can also trigger the release of a PDN connection using the (fast) re-authentication mechanism. The UE acts like in case 1) but sends different values within the messages to the network. The network initiated PDN Connection release is done by the network requesting a (fast) re-authentication. The indication that the PDN connection is released is included in the EAP-Response/AKA' Reauthentication or EAP-Response/AKA'-Challenge messages.

The mechanism proposed does not depend on the selected user plane mechanism selected for SaMOG phase 2 as transporting EAP messages is possible in all anticipated solutions.

As the capability indication from the network side is possible, the implementation of supporting additional PDN connection establishment in the network can also be optional. As there might be deployments where the additional PDN connection support is not needed, it is proposed to make this feature optional in the specification, however the proposed solution can also be specified in a way that the support of additional PDN creation in the network is mandatory.

8.2.9.1.2 Protocol stack

The authentication procedure used in this solution follows the Authentication and key agreement procedures specified in clause 6 of TS 33.402 [28]. Beyond the proposed additional parameters no other change is needed.

Figure 8.2.9.1.2-1 shows the protocol stack that can be used together for authentication, capability negotiation and signalling for PDN connection management.

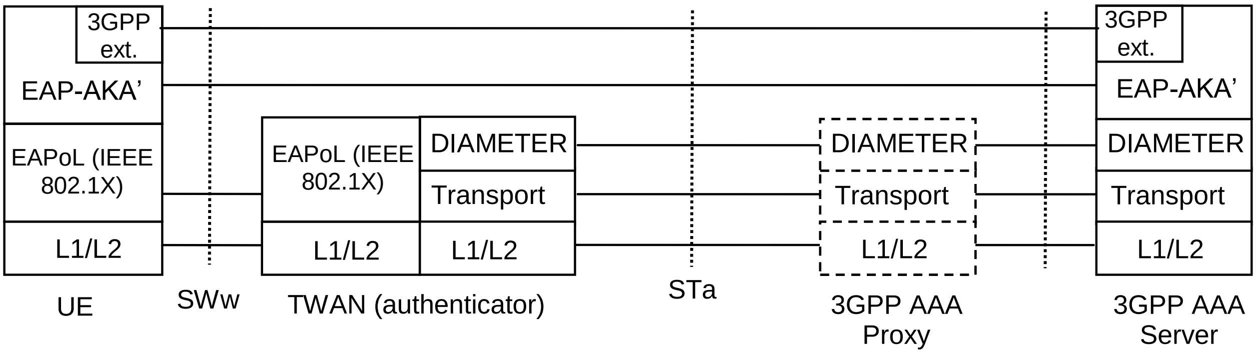


Figure 8.2.9.1.2-1: Protocol stack for authentication related signalling

3GPP access authentication based on EAP-AKA' as defined in IEEE RFC 5448 [27] (together with still necessary, 3GPP defined extensions) is performed end-to-end between UE and 3GPP AAA Server. Between UE and the TWAN/authenticator the information is transported over EAPoL (see IEEE 802.1X [5]). Between TWAN/authenticator and 3GPP AAA Server the EAP-AKA' payload is transported within Diameter messages. The following information is assumed to be exchanged newly, i.e. in addition to Rel. 11:

- handover indication (from UE to NW);
- APN (requested one from UE to NW, selected one from NW to UE):
- success/failure of PDN connection request (from NW to UE):
- PDN connection identifier (from NW to UE at PDN connection establishment or teardown. from UE to NW at PDN connection teardown)
- User plane connection identifier (e.g. VLAN tag)

However the solution is not limited in transferring the above listed parameters, other parameters could also be sent.

Some examples how EAP procedures can be used for sending session management information between the UE and TWAN are presented. The principle is that the TWAN can read the parameters sent by the UE from EAP messages, but cannot modify them. This is possible as during EAP-AKA' the EAP messages are integrity protected, but not encrypted. When the TWAN needs to send a parameter to the UE, it inserts it in the Diameter message sent to the 3GPP AAA server and then the 3GPP AAA server moves the received parameter from the Diameter message to the consecutive EAP message.

8.2.9.1.3 Signalling information from UE to the network

In Figure 8.2.9.1.3-1 an example is presented how the UE can send the requested APN to the TWAN during a fast re-authentication when a new PDN connection is established and how the network can send back the selected APN to the UE. Other session management parameters (e.g. handover indication, VLAN tags) can be sent in a similar manner

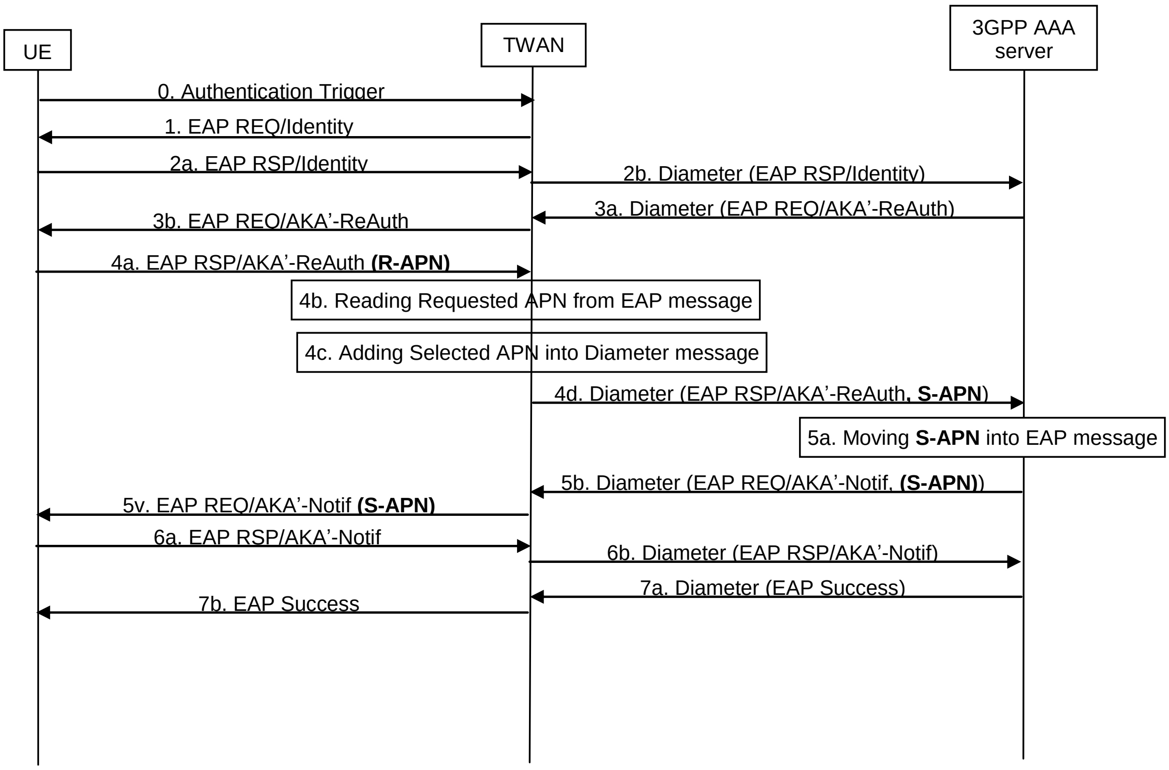

UE
TWAN
3GPP AAA server
0. Authentication Trigger
1. EAP REQ/Identity
2a. EAP RSP/Identity
2b. Diameter (EAP RSP/Identity)
3a. Diameter (EAP REQ/AKA'-ReAuth)
3b. EAP REQ/AKA'-ReAuth
4a. EAP RSP/AKA'-ReAuth **(R-APN)**
4b. Reading Requested APN from EAP message
4c. Adding Selected APN into Diameter message
4d. Diameter (EAP RSP/AKA'-ReAuth, **S-APN**)
5a. Moving **S-APN** into EAP message
5b. Diameter (EAP REQ/AKA'-Notif, **(S-APN)**)
5v. EAP REQ/AKA'-Notif **(S-APN)**
6a. EAP RSP/AKA'-Notif
6b. Diameter (EAP RSP/AKA'-Notif)
7a. Diameter (EAP Success)
7b. EAP Success

Figure 8.2.9.1.3-1: Sending the requested APN to the TWAN

- Step 0. The UE triggers a new EAP authentication.

Editor's note: It is FFS how the UE can trigger a new authentication, especially if IEEE 802.1X EAPoL Start message can trigger a new EAP authentication.

- Step 1-3: These steps are performed as in TS 33.402 [28].

- Step 4: The UE adds the requested APN (and other session management parameters) into the EAP message into a new EAP information element. The TWAN reads the requested APN from the EAP message and adds the selected APN (and other session management parameters including the indication of success or failure of the PDN connection establishment) as a Diameter information element to the Diameter message sent to the 3GPP AAA server. Note that the requested APN is not removed from the EAP message as the TWAN cannot modify the EAP message.

- Step 5: The 3GPP AAA server extracts the selected APN from the Diameter message and inserts it into the EAP message in a new information element. Note that the 3GPP AAA server ignores the requested APN received in the EAP message and does not interpret the selected APN received in Diameter, it just copies the Selected APN value from the received Diameter message into the EAP message to be sent. The UE receives the selected APN (and other session management parameters) within the EAP message.

- Step 6-7: these steps are performed as in TS 33.402 [28].

8.2.9.1.4 Signalling information from the network to the UE

In Figure 8.2.9.1.4-1 an example is presented how the network can send an indication to the UE that a PDN connection is released during a fast re-authentication. Other parameters (e.g. handover indication) can be sent in a similar manner.

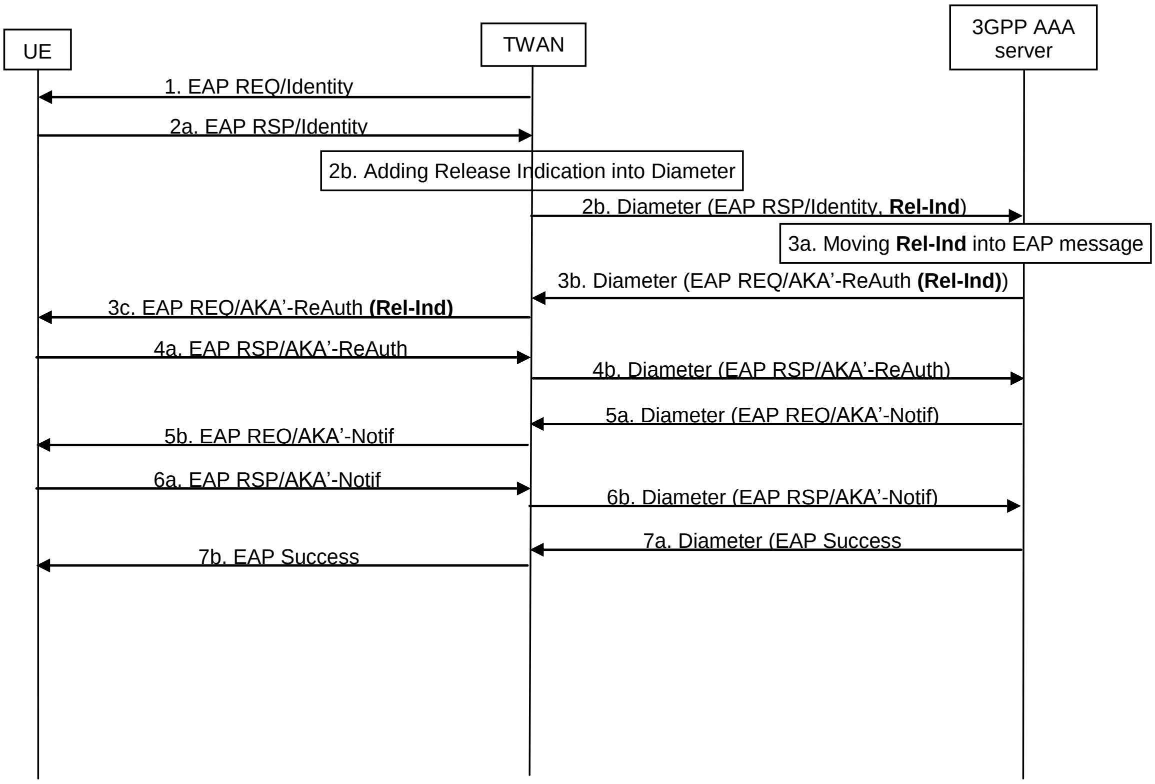

UE
TWAN
3GPP AAA server
1. EAP REQ/Identity
2a. EAP RSP/Identity
2b. Adding Release Indication into Diameter
2b. Diameter (EAP RSP/Identity, **Rel-Ind**)
3a. Moving **Rel-Ind** into EAP message
3b. Diameter (EAP REQ/AKA'-ReAuth **(Rel-Ind)**)
3c. EAP REQ/AKA'-ReAuth **(Rel-Ind)**
4a. EAP RSP/AKA'-ReAuth
4b. Diameter (EAP RSP/AKA'-ReAuth)
5a. Diameter (EAP REQ/AKA'-Notif)
5b. EAP REQ/AKA'-Notif
6a. EAP RSP/AKA'-Notif
6b. Diameter (EAP RSP/AKA'-Notif)
7a. Diameter (EAP Success
7b. EAP Success

Figure 8.2.9.1.4-1: Sending the PDN connection release to the UE

- Step 1-2a: These steps are performed as in TS 33.402 [28].

- Step 2b-2c: The TWAN adds the indication of the PDN connection release into the Diameter message within a Diameter information element. This indication shall contain an identifier of the release PDN connection to be released.

- Step 3a: The 3GPP AAA server extracts the Release Indication from the Diameter message and inserts it into the EAP message in a new information element. Note that the 3GPP AAA server does not interpret the Release Indication, it just copies it from the received Diameter message into the EAP message.

- Step 3b-3c: The UE receives the Release Indication within the EAP message.

- Step 4-8: These steps are performed as in TS 33.402 [28]. After the successful EAP procedure the UE shall consider the PDN connection released.

In the procedures described below the principles presented in this clause are used to carry session management information within EAP signalling, but for the sake of simplicity the details are not presented within the procedures.

8.2.9.2 Procedures

Editor's note: The call flows are described in this clause.

8.2.9.2.1 Initial Attach in WLAN on S2a

The initial attach procedure is the same as (or similar to) the initial attach procedure described in clause 8.2.1.2 with the following addition:

In step 2 of Figure 8.2.1.2.1.1-1 during the EAP authentication within the capability indication the TWAN shall also indicate if it supports the creation of additional PDN connections or a simultaneous NSWO connection. This additional capability indication is only needed if the support of additional PDN connections or simultaneous NSWO connection creation is optional.

8.2.9.2.2 UE-Initiated Connectivity to Additional PDN in WLAN on S2a

8.2.9.2.2.1 UE-Initiated Connectivity to Additional PDN in WLAN on GTP S2a

This procedure is used to create additional PDN connections or when the UE is authenticated to the network (via EAP-AKA') and has a NSWO session.

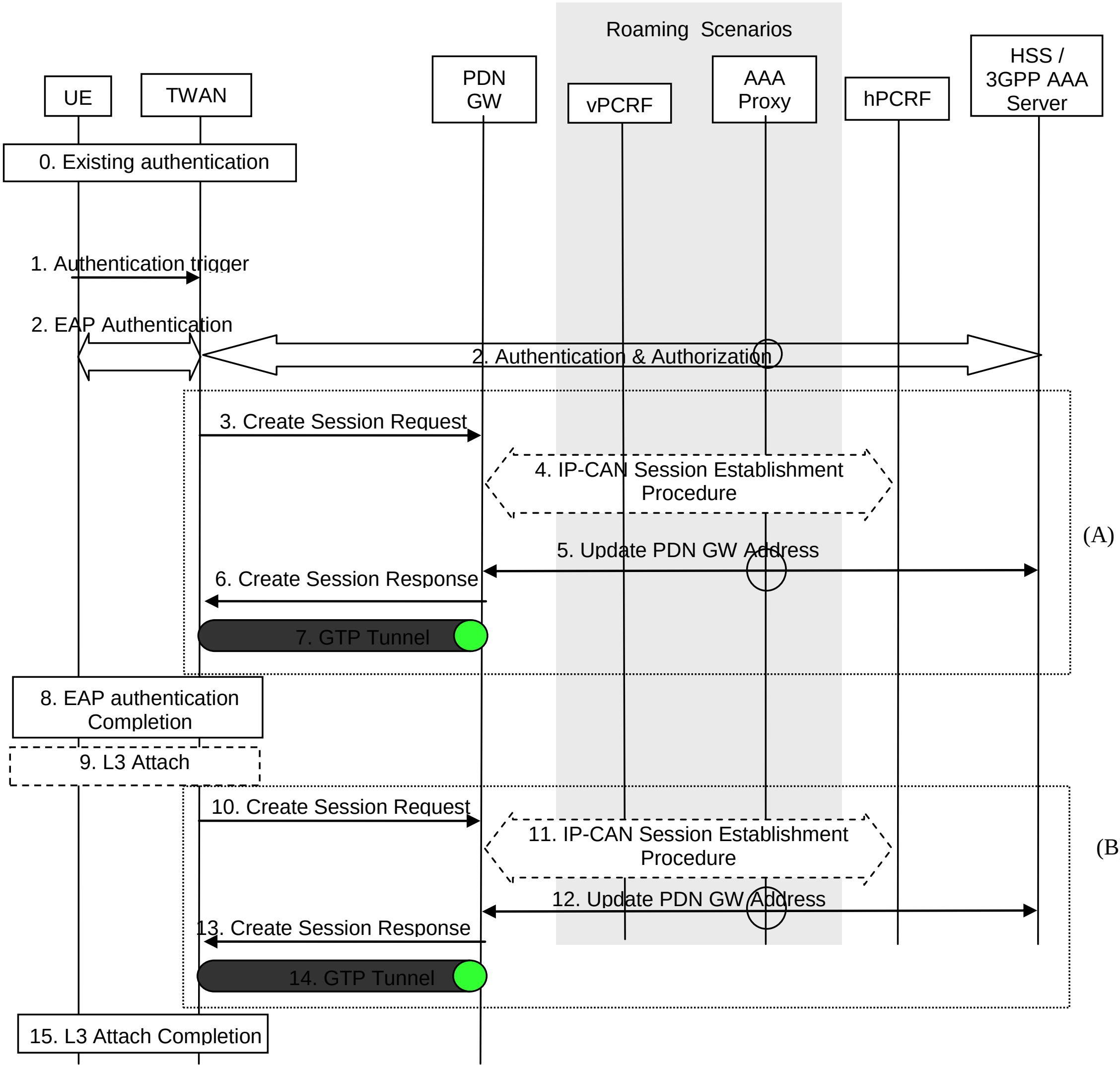

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS / 3GPP AAA Server
0. Existing authentication
1. Authentication trigger
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Create Session Response
7. GTP Tunnel
(A)
8. EAP authentication Completion
9. L3 Attach
10. Create Session Request
11. IP-CAN Session Establishment Procedure
12. Update PDN GW Address
13. Create Session Response
14. GTP Tunnel
(B)
15. L3 Attach Completion

Figure 8.2.9.2.2.1-1: UE-Initiated Connectivity to Additional PDN in WLAN on GTP S2a

The procedure is as in clause 8.2.1.2.1.1 (Initial Attach in WLAN on GTP S2a for solution 1) with the following additions:

- Step 0: The precondition of this procedure is that the UE has valid authentication with the TWAN. The UE might have an existing PDN connection or might use NSWO capability of the TWAN.

- Step 1. The UE triggers a new EAP authentication by sending an IEEE 802.1X EAPoL Start message to the authenticator.

- Step 2. An EAP authentication using Fast Reauthentication is performed if possible, otherwise a full authentication is performed. The UE indicates the APN and other 3GPP specific parameters within the EAP-

Response/AKA'-Reauthentication and EAP-Response/AKA'-Challenge messages in a new EAP attribute in a similar way as it is indicated during initial attach.

- Step 8: After the successful PDN connection establishment the EAP procedure is completed. Within this step the TWAN sends back information about the established PDN connection (e.g. success indication, necessary user plane parameters, such as VLAN tag).
- During the procedure a new virtual point-to-point between the UE and the TWAG is created for the new PDN connection (on NSWO session). When and how this is performed depends on the mechanism used for point-to-point link creation.

8.2.9.2.2.2 UE-Initiated Connectivity to Additional PDN in WLAN on PMIP S2a

The required additions to the procedure are the same as the ones described for GTP S2a (see previous clause) as the proposed additions to the EAP procedures do not depend on the protocol used over S2a.

8.2.9.2.3 Handover procedure between 3GPP access and WLAN on S2a

8.2.9.2.3.1 Handover from 3GPP access to WLAN on GTP S2a

This procedure is used to hand over a PDN connection from 3GPP access to WLAN on GTP S2a. If multiple PDN connections are handed over then this procedure is invoked for each PDN connections separately.

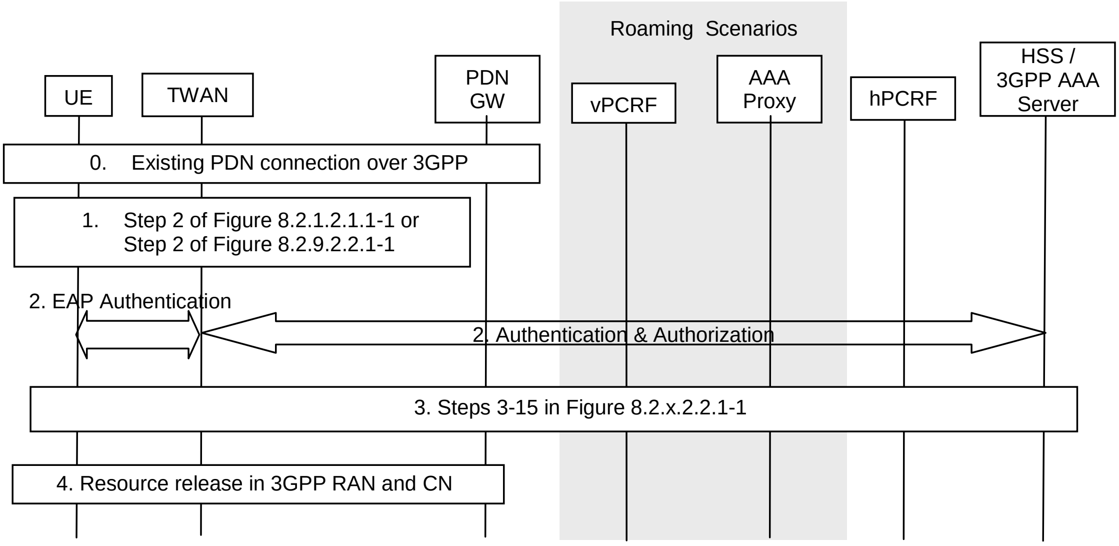

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS / 3GPP AAA Server
0. Existing PDN connection over 3GPP
1. Step 2 of Figure 8.2.1.2.1.1-1 or Step 2 of Figure 8.2.9.2.2.1-1
2. EAP Authentication
2. Authentication & Authorization
3. Steps 3-15 in Figure 8.2.x.2.2.1-1
4. Resource release in 3GPP RAN and CN

Figure 8.2.9.2.3.1-1: Handover from 3GPP access to WLAN on GTP S2a

During the steps of Figure 8.2.9.2.3.1-1 the following should be taken into account:

- Step 0: The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.
- Step 1: If the UE has no valid authentication with the TWAN, i.e. the UE has neither a PDN connection nor a NSWO connection then this step is the same as step 2 of 8.2.1.2.1.1-1. If the UE has a valid authentication with the TWAN either due to the UE having an existing PDN connection or using NSWO capability of the TWAN, then this step is the same as step 2 of 8.2.9.2.2.1-1.
- Step 2: As step 2 in 8.2.9.2.2.1-1with the following addition: the UE indicates handover via EAP to the 3GPP AAA Server.
- Step 3: The same as step 3-15 in 8.2.9.2.2.1-1 with the addition that handover is performed: the handover indication is set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF.

- Step 4: The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.9.2.3.2 Handover from 3GPP access to WLAN on PMIP S2a

The required additions to the procedure are the same as the ones described for GTP S2a (see previous clause) as the proposed additions to the EAP procedures do not depend on the protocol used over S2a.

8.2.9.2.3.3 Handover from TWAN to 3GPP access

This procedure can be performed as specified in TS 23.402 [3]. Solution specific changes are needed when after the handover the PGW initiates the removal of the resources in the TWAN. These changes can be found in clause 8.2.9.2.4.

8.2.9.2.4 PDN GW initiated Resource Allocation Deactivation

8.2.9.2.4.1 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

This procedure applies when the PDN GW would like to release a PDN connection.

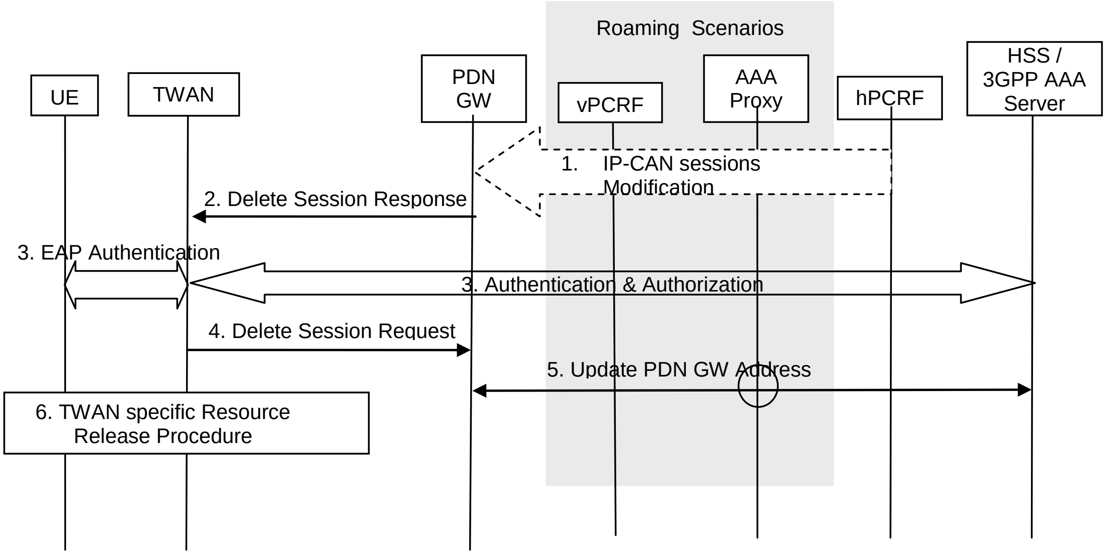

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS / 3GPP AAA Server
1. IP-CAN sessions Modification
2. Delete Session Response
3. EAP Authentication
3. Authentication & Authorization
4. Delete Session Request
5. Update PDN GW Address
6. TWAN specific Resource Release Procedure

Figure 8.2.9.2.4.1-1: PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

During the steps of Figure 8.2.9.2.4.1-1 the following should be taken into account:

- Step 3: An EAP authentication is triggered by the TWAN. Preferably a Fast Reauthentication is performed, but if it is not possible due to any reason then a full authentication is performed. The TWAN indicates that it requests a release of an existing PDN connection within the EAP-Request/AKA'-Reauthentication and EAP-Request/AKA'-Challenge messages in a new EAP attribute.

NOTE: Step 3 and steps 4 and 5 can be performed simultaneously.

8.2.9.2.4.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a

The required additions to the procedure are the same as the ones described for GTP S2a (see previous clause) as the proposed additions to the EAP procedures do not depend on the protocol used over S2a.

8.2.9.2.5 TWAN requested PDN Disconnection Procedures

8.2.9.2.5.1 TWAN requested PDN Disconnection Procedure in WLAN on GTP S2a

This procedure applies when multiple PDN connections have been established or when the UE has at least one PDN connection and simultaneously uses NSWO.

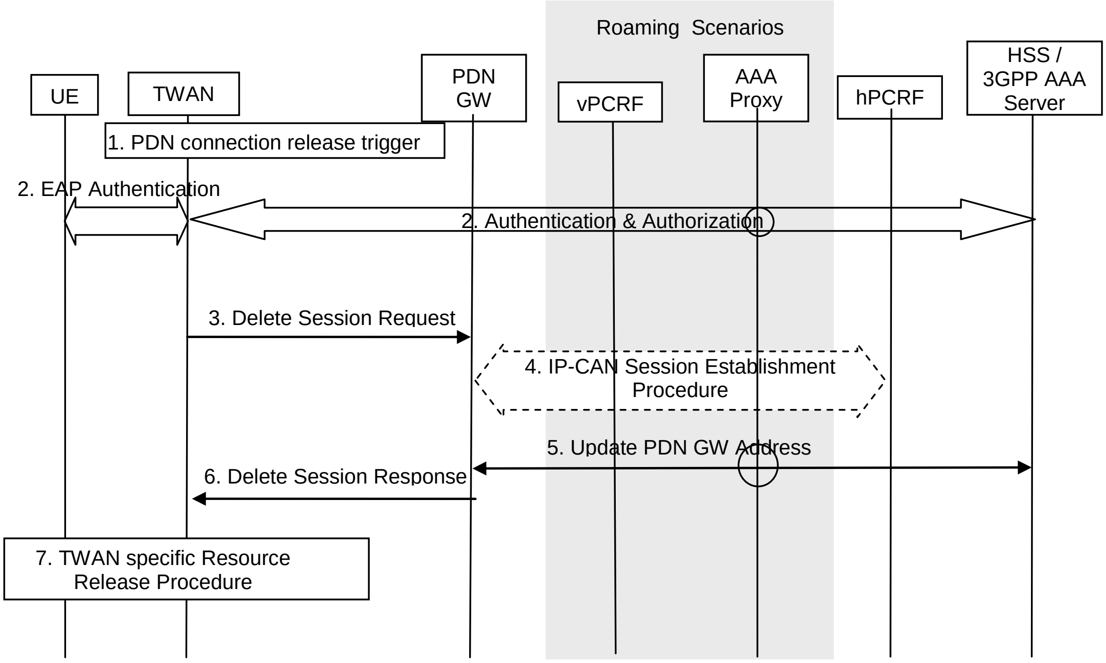

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS / 3GPP AAA Server
1. PDN connection release trigger
2. EAP Authentication
2. Authentication & Authorization
3. Delete Session Request
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Delete Session Response
7. TWAN specific Resource Release Procedure

Figure 8.2.9.2.5.1-1: TWAN initiated Resource Allocation Deactivation in WLAN on GTP S2a

During the steps of Figure 8.2.9.2.3.1-1 the following should be taken into account:

- Step 2. An EAP authentication is triggered by the TWAN. Preferably a Fast Reauthentication is performed, but if it is not possible due to any reason then a full authentication is performed. The TWAN indicates that it requests a release of an existing PDN connection within the EAP-Request/AKA'-Reauthentication and EAP-Request/AKA'-Challenge messages in a new EAP attribute.

NOTE: An NSWO session that is simultaneously used with PDN connection(s) can also be terminated in this way. If the NSWO offload session is terminated then steps 3-6 are not performed.

8.2.9.2.5.2 TWAN Initiated Detach and requested PDN Disconnection Procedure in WLAN on PMIP S2a

The required additions to the procedure are the same as the ones described for GTP S2a (see previous clause) as the proposed additions to the EAP procedures do not depend on the protocol used over S2a.

8.2.9.2.6 UE requested PDN Disconnection Procedures

8.2.9.2.6.1 UE requested PDN Disconnection Procedure in WLAN on GTP S2a

This procedure applies when multiple PDN connections have been established or when the UE has at least one PDN connection and simultaneously uses NSWO.

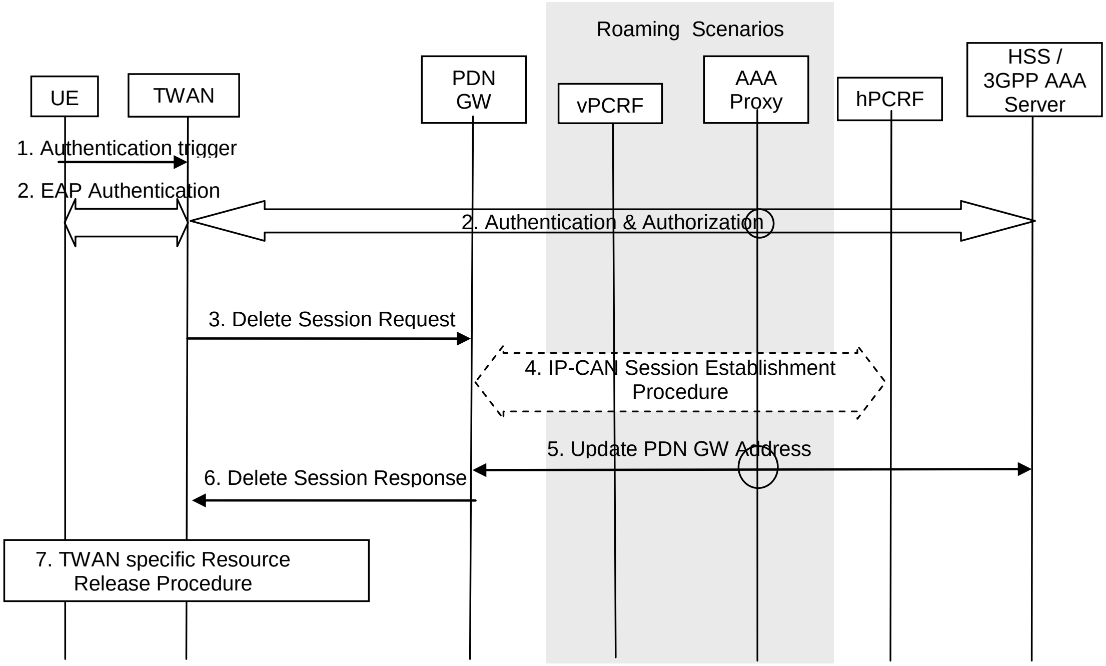

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS / 3GPP AAA Server
1. Authentication trigger
2. EAP Authentication
2. Authentication & Authorization
3. Delete Session Request
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Delete Session Response
7. TWAN specific Resource Release Procedure

Figure 8.2.9.2.6.1-1: UE requested PDN Disconnection Procedure in WLAN on GTP S2a

During the steps of Figure 8.2.9.2.3.1-1 the following should be taken into account:

- Step 1. The UE triggers a new EAP authentication.

Editor's note: It is FFS how the UE can trigger a new authentication, especially if IEEE 802.1X EAPoL Start message can trigger a new EAP authentication.

- Step 2. An EAP authentication is performed. Preferably a Fast Reauthentication is performed, but if it is not possible due to any reason then a full authentication is performed. The UE indicates that it requests a release of an existing PDN connection within the EAP-Response/AKA' Reauthentication and EAP-Response/AKA'-Challenge messages in a new EAP attribute.

NOTE: An NSWO session that is simultaneously used with PDN connection(s) can also be terminated in this way. If the NSWO offload session is terminated then steps 3-6 are not performed.

- Step 3-6: Step 3 is triggered by the PDN connection release request indication received in step 2.

8.2.9.2.6.2 UE requested PDN Disconnection Procedure in WLAN on GTP S2a on PMIP S2a

The required additions to the procedure are the same as the ones described for GTP S2a (see previous clause) as the proposed additions to the EAP procedures do not depend on the protocol used over S2a.

8.2.9.2.7 Detach Procedures

There is nothing special in the detach procedures, they are in principle the same as specified in TS 23.402 [3] for Trusted Non-3GPP Access Networks. If the detach procedure requires to perform PDN connection release procedures then the procedures described above are applicable.

8.2.9.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

The UE shall support an enhanced EAP-AKA' scheme with new attributes in EAP messages.

The 3GPP AAA server shall support:

- an enhanced EAP-AKA' scheme with new attributes in EAP messages;

- additional Diameter AVP for parameters sent from TWAN to the UE.

NOTE: The 3GPP AAA server does not process the new parameters, their values are simply ignored or copied between messages.

8.2.9.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 as well as simplicity of implementation in the UE should be evaluated.

8.2.10 Solution 10 : WCS Solution

8.2.10.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.10.1.1 Overview

This solution proposes a control plane protocol between the UE and the TWAG for mobility management PDN connections.

This solution supports simultaneous NSWO and PDN connections.

For the user plane, a virtual MAC address or VLAN is used to differentiate multiple connections (including PDN connections and NSWO connection).

UE and network capability is negotiated during EAP-AKA' procedure to decide whether the Rel-11 or the Rel-12 SaMOG procedure is performed.

8.2.10.1.2 User plane

The point-to-point link required to transport traffic for a given PDN connection, or for Non-Seamless WLAN Offload (NSWO) is realized via the TWAN reserving a distinct VLAN ID or virtual MAC address that uniquely (on a per-UE basis) corresponds to an PDN connection or NSWO.

The link model for VLAN based user plane is described in 8.2.2.1.1.1, and the link model for virtual MAC based user plane is described in 8.2.2.1.1.2.

Editor's note: Whether VLAN or Virtual MAC address is chosen is FFS.

8.2.10.1.3 Control plane

A UE-TWAG protocol is used to control (i.e. setup and teardown) the per-PDN point-to-point link. This protocol is denoted as WCS (WLAN Control Signalling) and should be defined by 3GPP. The functions that WCS supports include: Establishment of a per-UE-and-PDN point-to-point link; Tear down of a per-UE-and-PDN point-to-point link; IP address allocation for PDN connections connection. An NSWO connection is established using DHCP or IPv6 stateless autoconfiguration after authentication in the per UE p2p link.

Reliability of the WCS protocol uses RFC 3315 reliability mechanisms and depends on the reception of a reply message in response to a request message. If no response is received, re-transmission of the request message can use the DHCP re-transmission timer value. No support for fragmentation is provided and is not necessary for the control protocol.

Three alternatives for the transport of WCS are outlined below.

Editor's note: One of these alternatives for protocol transport needs to be chosen. The selection would depend on the choice of user plane.

8.2.10.1.3.1 Alternative 1: Virtual MAC-based control protocol transport

The frame format of the control plane is as shown in Figure 8.2.10.1.3-1.

A new Ethertype is used to identify the WCS protocol. If the virtual MAC address is used by TWAG to differentiate the user plane PDN connections, a dedicated virtual MAC address may also be used to differentiate the control plane.

The new Ethertype for WCS needs to be defined in IEEE.

MAC/LLC	WCS Ethertype	Payload(WCS)

Figure 8.2.10.1.3-1: Frame format for PDN for Virtual MAC-based control protocol

A dedicated p2p Link ID (i.e. (Virtual MAC address) allocated by TWAG is used for WCS signalling. The Virtual MAC address is unique per UE.

This MAC address is sent to the UE during EAP-AKA' authentication as described in clause 8.2.10.1.3.4. In this case, the p2p link ID in clause 8.2.10.1.3.4 is a Virtual MAC address of the TWAG.

8.2.10.1.3.2 Alternative 2: VLAN-based control protocol transport

The frame format of the control plane is as shown in Figure 8.2.10.1.3.2-1.

MAC/LLC	VLAN	New Ethertype	Payload (WCS)

Figure 8.2.10.1.3.2-1: Frame format for PDN for L2.5-based control protocol

The VLAN ID is used to differentiate the tunnel between the control plane and the user plane protocol. In the corresponding user plane, the VLAN ID used to distinguish PDN connections.

As in the case of Alternative 1 (clause 8.2.10.1.3.1), a new Ethertype is needed to indicate that payload is WCS.

The dedicated p2p link ID (i.e. VLAN ID) used for control plane signalling on top of per UE p2p link is negotiated during the EAP-AKA' procedure. Details of provisioning the p2p link ID (i.e. VLAN ID) are described in clause 8.2.10.1.3.4. The TWAG MAC address is also sent to the UE during EAP-AKA' authentication sequence, along with the VLAN ID.

8.2.10.1.3.3 Alternative 3: L3-based control protocol transport

In this alternative, the frame format of the control plane message is as shown in Figure 8.2.10.1.3.3-1.

MAC/LLC	UDP/IP	Payload (WCS)

Figure 8.2.10.1.3.3-1: Frame format for L3-based control protocol

The payload contains the WCS control protocol message. The UE gets a link-local address or NSWO address before using L3 based control protocol. The IP address of the TWAG is sent to the UE during the EAP-AKA' procedure in the same as how the TWAG MAC address is delivered in alternative2. A well known UDP port could be used for the WCS control protocol.

8.2.10.1.3.4 p2p link ID negotiation in EAP-AKA' procedure.

This procedure describes the p2p link ID is negotiation during EAP-AKA'. The p2p link ID is used to establish tunnel to transport the control plane protocol (WCS) when layer 2 based control protocol is used.

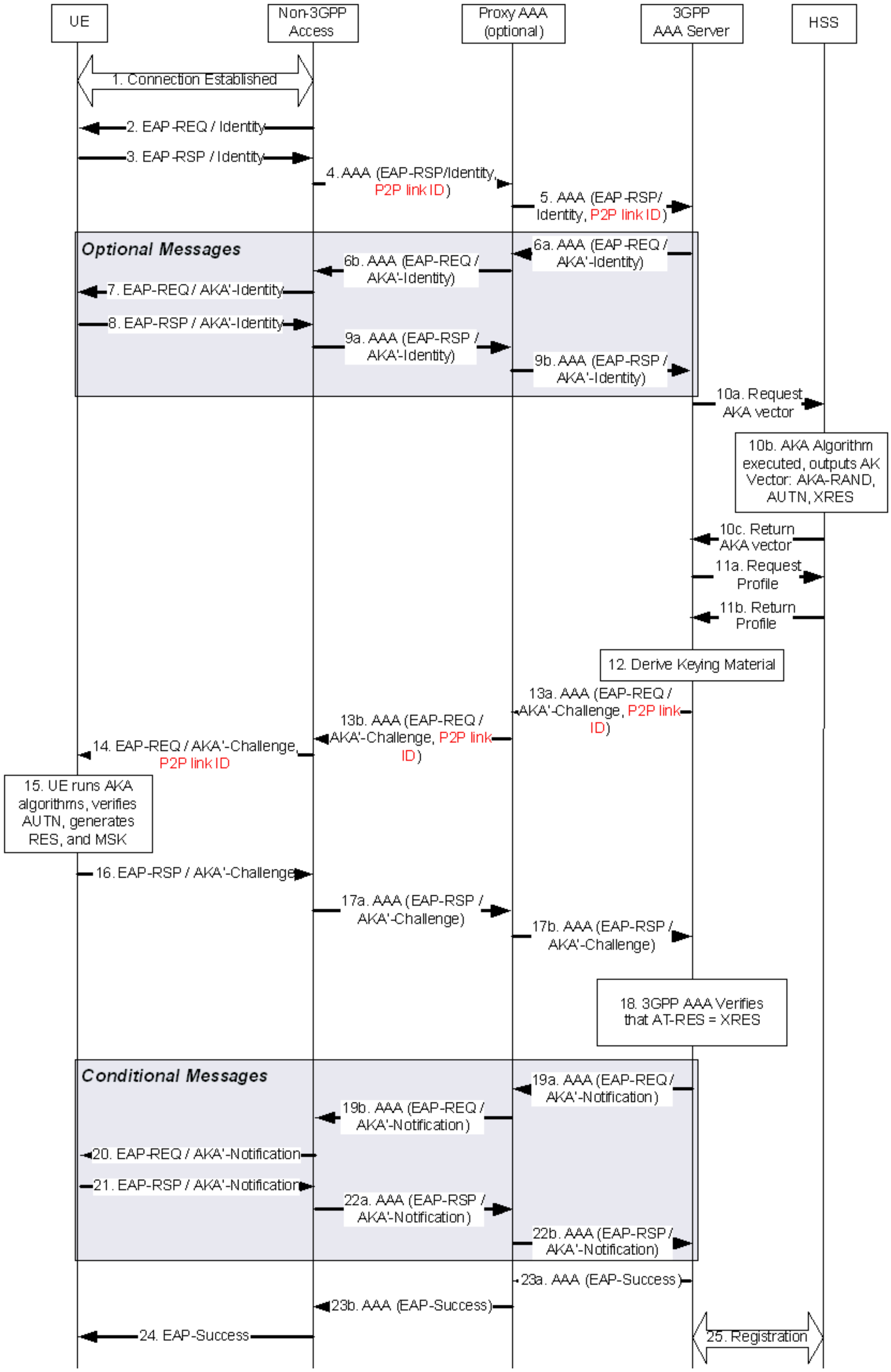

UE
Non-3GPP Access
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity, P2P link ID)
5. AAA (EAP-RSP/ Identity, P2P link ID)
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / AKA'-Identity
9a. AAA (EAP-RSP / AKA'-Identity)
9b. AAA (EAP-RSP / AKA'-Identity)
10a. Request AKA vector
10b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
10c. Return AKA vector
11a. Request Profile
11b. Return Profile
12. Derive Keying Material
13a. AAA (EAP-REQ / AKA'-Challenge, P2P link ID)
13b. AAA (EAP-REQ / AKA'-Challenge, P2P link ID)
14. EAP-REQ / AKA'-Challenge, P2P link ID
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge
17a. AAA (EAP-RSP / AKA'-Challenge)
17b. AAA (EAP-RSP / AKA'-Challenge)
18. 3GPP AAA Verifies that AT-RES = XRES
Conditional Messages
19a. AAA (EAP-REQ / AKA'-Notification)
19b. AAA (EAP-REQ / AKA'-Notification)
20. EAP-REQ / AKA'-Notification
21. EAP-RSP / AKA'-Notification
22a. AAA (EAP-RSP / AKA'-Notification)
22b. AAA (EAP-RSP / AKA'-Notification)
23a. AAA (EAP-Success)
23b. AAA (EAP-Success)
24. EAP-Success
25. Registration

Figure 8.2.10.1.3.4-1: p2p link ID negotiation

Step4-Step5 TWAG sends the p2p link ID via TWAN to the 3GPP AAA.

Step13a,b-14, the p2p link ID is sent in EAP-REQ message to the UE.

The p2p link ID could be the virtual MAC address or VLAN ID provisioned in the TWAN.

8.2.10.1.4 Protocol Stacks

Editor's note: Impact on link model due to handover support is FFS.

8.2.10.2 Procedures

Editor's note: The call flows are described in this clause.

8.2.10.2.1 Initial Attach procedure

8.2.10.2.1.1 Initial Attach in WLAN on S2a - network capability negotiation

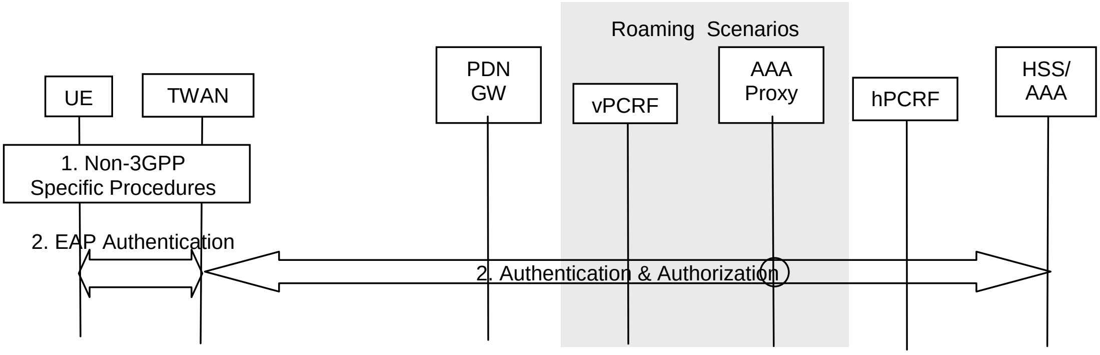


Figure 8.2.10.2.1-1: Initial attachment in WLAN on S2a for roaming and non-roaming scenarios

The procedure is as in TS 23.402 [3] clause 16.2 with the following additions:

- Step 2. As part of this step, the UE shall send an indication to the network as to whether it supports Rel-12 SaMOG. Depending on the capabilities of the network and the indication of the UE, the network informs the UE as part of step 2 whether the Rel-12 SaMOG procedures should be performed.

8.2.10.2.1.2 Initial Attach continuation for GTP based S2a

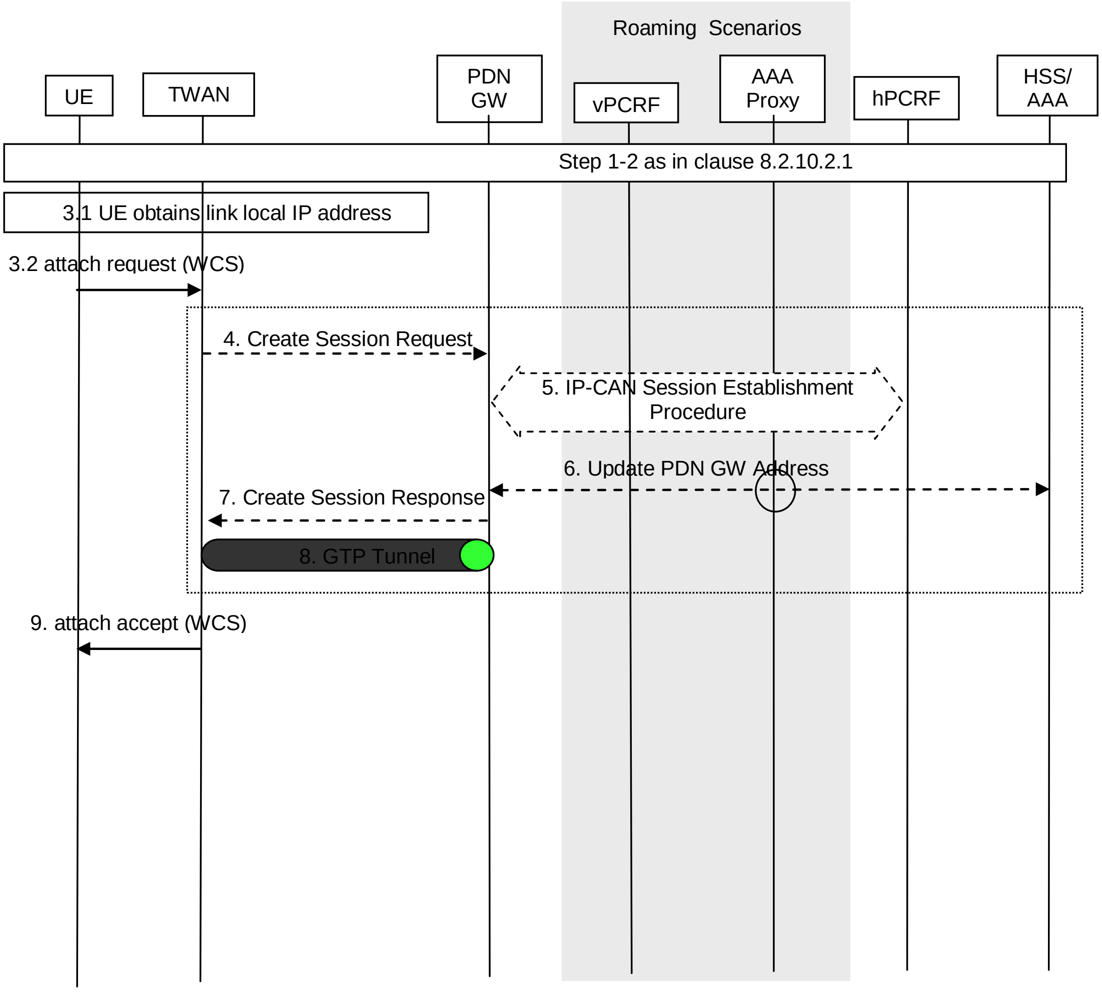

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Step 1-2 as in clause 8.2.10.2.1
3.1 UE obtains link local IP address
3.2 attach request (WCS)
4. Create Session Request
5. IP-CAN Session Establishment Procedure
6. Update PDN GW Address
7. Create Session Response
8. GTP Tunnel
9. attach accept (WCS)

Figure 8.2.10.2.1-2: Initial attachment in WLAN on S2a for roaming and non-roaming scenarios

The procedure continues from step 2 in clause 8.2.10.2.1:

- Step 2, as part of the authentication procedure, the p2p link ID for WCS signalling is negotiated between the UE and the TWAG. An NSWO indication which indicates whether NSWO is permitted or not is sent to the UE. There are following alternatives to establish the p2p link for WCS:
  - If Alternative 1 (clause 8.2.10.1.3.1) based mechanism is used for WCS, then a (virtual) MAC address of TWAG is send to the UE.
  - If Alternative 2 (clause 8.2.10.1.3.2) based mechanism is used for WCS, then the VLAN ID is negotiated between the UE and the TWAG. Also the MAC address of the TWAG should be sent to the UE.
  - If Alternative 3 (clause 8.2.10.1.3.3) based mechanism is used for WCS, the TWAG IP address is sent to the UE.
- Step3.1, The UE will get a link local address or NSWO Address from TWAN using IETF RFC 4861 [11] for IPv6, or RFC 3927 for IPv4.The UE can use this IP address for the transport of the control plane protocol to TWAG. If the UE wants to setup an NSWO connection, and if NSWO is permitted, the UE sends a DHCP Request (and optionally an IPv6 Router Solicitation Request) in this step. If NSWO is not permitted, UE should not send a DHCP Request and UE should configure a LLA as per RFC 3927.
- Step3.2: If the UE wants to set up a PDN connection, the UE sends a WCS Attach Request to the TWAN. This message includes AttachType, APN, , PDN type, PCO. The Attach Type field indicates initial attach and the APN field indicates the APN that the UE requests. The PDN type field indicates the IP address type the UE request. The PCO field may indicate that the UE wants deferred IP address allocation and if so, the UE will send DHCP/RS after the attach procedures.

There are two options for user plane p2p link ID. 1) virtual MAC address 2) VLAN ID allocated by the TWAG

- Step 4-8 refers to step-3 -step7 in clause 16.2.1 of TS 23.402 [3]. Additionally, if the PDN GW receives the PCO which indicates deferred IPv4 address allocation, then the PDN GW will not allocate IP address to the UE at this step.

- Step 9 the TWAN sends a WCS attach accept message to the UE. If the UE does not indicate an APN in the attach request, the TWAN should send the selected APN to the UE. The IP address(es) is also sent to the UE if the PDN GW has allocated the IP address to the UE (i.e., not deferred address for IPv4). . This response contains a User Plane p2p link ID to be used in further signalling associated with this PDN connection.

If the user plane p2p link is VLAN based, the VLAN ID allocated by the TWAN is included in the p2p link field of the attach accept message. Alternatively, if the user plane p2p link is virtual MAC based, the virtual MAC allocated by the TWAN is included in the p2p link field.

If the UE requests a deferred IPv4 address allocation, the UE may request for an IP address using DHCP after the attach procedure. DHCP signalling is performed over the established p2p link. In IPv6, prefix assignment takes place using IETF RFC 4861 [11] over the established p2p link.

8.2.10.2.1.2 Initial Attach in WLAN on PMIP S2a

Editor's note: The procedure is FFS.

8.2.10.2.2 UE-initiated Connectivity to Additional PDN

This procedure is used when the UE requests additional PDN connections.

This procedure is also used when the UE requests more PDN connections in the same APN.

The p2p link is established between UE and TWAG per each PDN connection.

8.2.10.2.2.1 UE-Initiated Connectivity to PDN in WLAN on GTP S2a

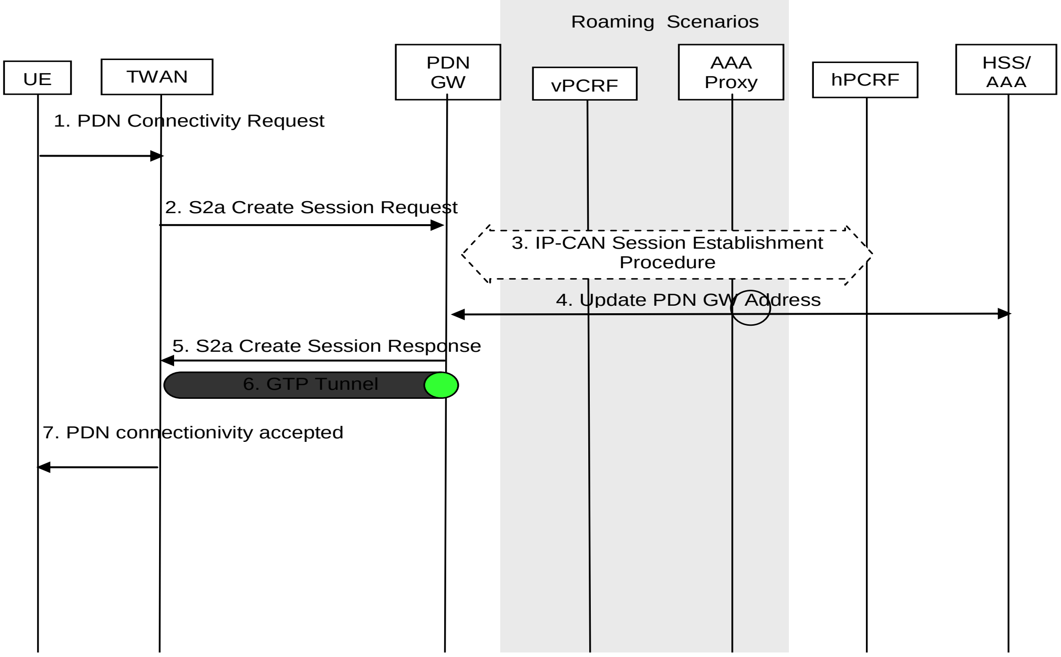

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. PDN Connectivity Request
2. S2a Create Session Request
3. IP-CAN Session Establishment Procedure
4. Update PDN GW Address
5. S2a Create Session Response
6. GTP Tunnel
7. PDN connectionivity accepted

Figure 8.2.10.2.2.1-1: UE initiated connectivity to PDN/NSWO

- Step 1. The UE triggers the establishment of a new per-UE and per-PDN point-to-point link. The UE sends WCS PDN Connectivity Request (APN, PDN Type, Protocol Configuration Options, Request Type). The Request Type indicates "initial request" if the UE requests new additional PDN connectivity over the 3GPP access network for multiple PDN connections, the Request Type indicates "handover" when the UE is performing a handover from 3GPP access and the UE has already established connectivity with the PDN over the 3GPP access.

- Step 2-6. Same as step 3-7 in clause 8.2.10.2.2.1. As part of these steps, the TWAN verifies that the APN requested by the UE is allowed by subscription. Upon handover, the TWAN selects the PDN GW handling this PDN connection; otherwise, the TWAN performs PDN GW selection as described in TS 23.402 [3]. Steps 2-6 are executed with the selected PDN GW.
- Step 7. The TWAN replies with WCS PDN connectivity accept to the UE. This response contains a p2p link id to be used in further signalling associated with this PDN connection.
- If the UE requests deferred IPV4 address allocation, it may negotiate the IPv4 address with DHCPv4 after step7.

8.2.10.2.2.2 UE-Initiated Connectivity to PDN in WLAN on PMIP S2a

Editor's note: The procedure is FFS.

8.2.10.2.3 Handover procedure in multi-connection scenario from 3GPP access to WLAN on S2a

8.2.10.2.3.1 Handover in multi-connection scenario from 3GPP access to WLAN on GTP S2a

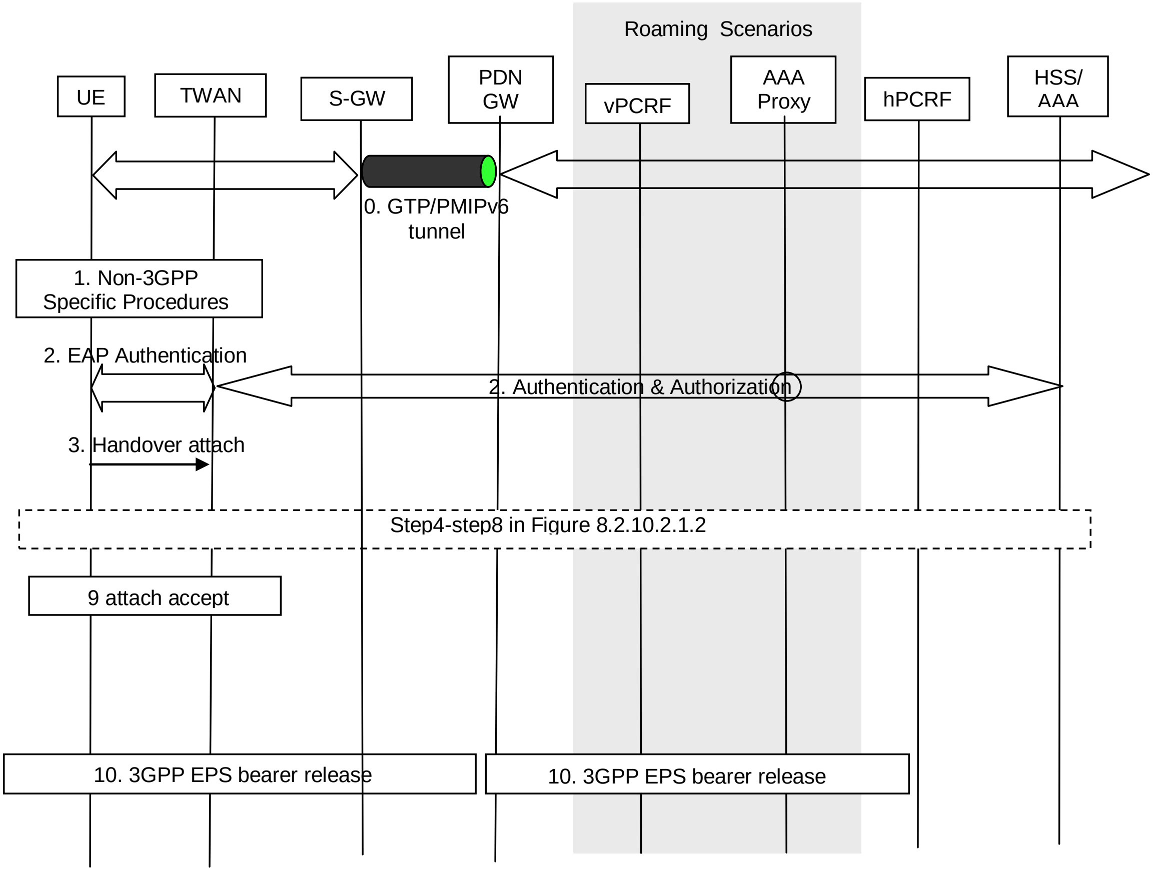

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0. GTP/PMIPv6 tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Handover attach
Step4-step8 in Figure 8.2.10.2.1.2
9 attach accept
10. 3GPP EPS bearer release
10. 3GPP EPS bearer release

Figure 8.2.10.3.1-1: Handover from 3GPP access to WLAN

- Step1- Step2, same as in clause 8.2.10.2.1-1
- Step3- Refer to Step3.2 of attach procedure in clause 8.2.10.2.1.2. Attach type indicates handover attach.

If L3 based WCS is used, then the UE should get a link local IP address or NSWO address before step3 as described in step3.1 of attach procedure in clause 8.2.10.2.1.2.

- Step4-step8: Since these steps represent handover attach, IP address preservation is handled by the PDN GW.

- Step9: same as Step9 of attach procedure in clause 8.2.10.2.1.2.

8.2.10.2.3.2 Handover in multi-connection scenario from 3GPP access to WLAN on PMIP S2a

Editor's note: The procedure is FFS.

8.2.10.2.4 Handover procedure in multi-connection scenario from WLAN on S2a to 3GPP access

Editor's note: The procedure is FFS.

8.2.10.2.5 Handover procedure from WLAN on S2a to 3GPP access

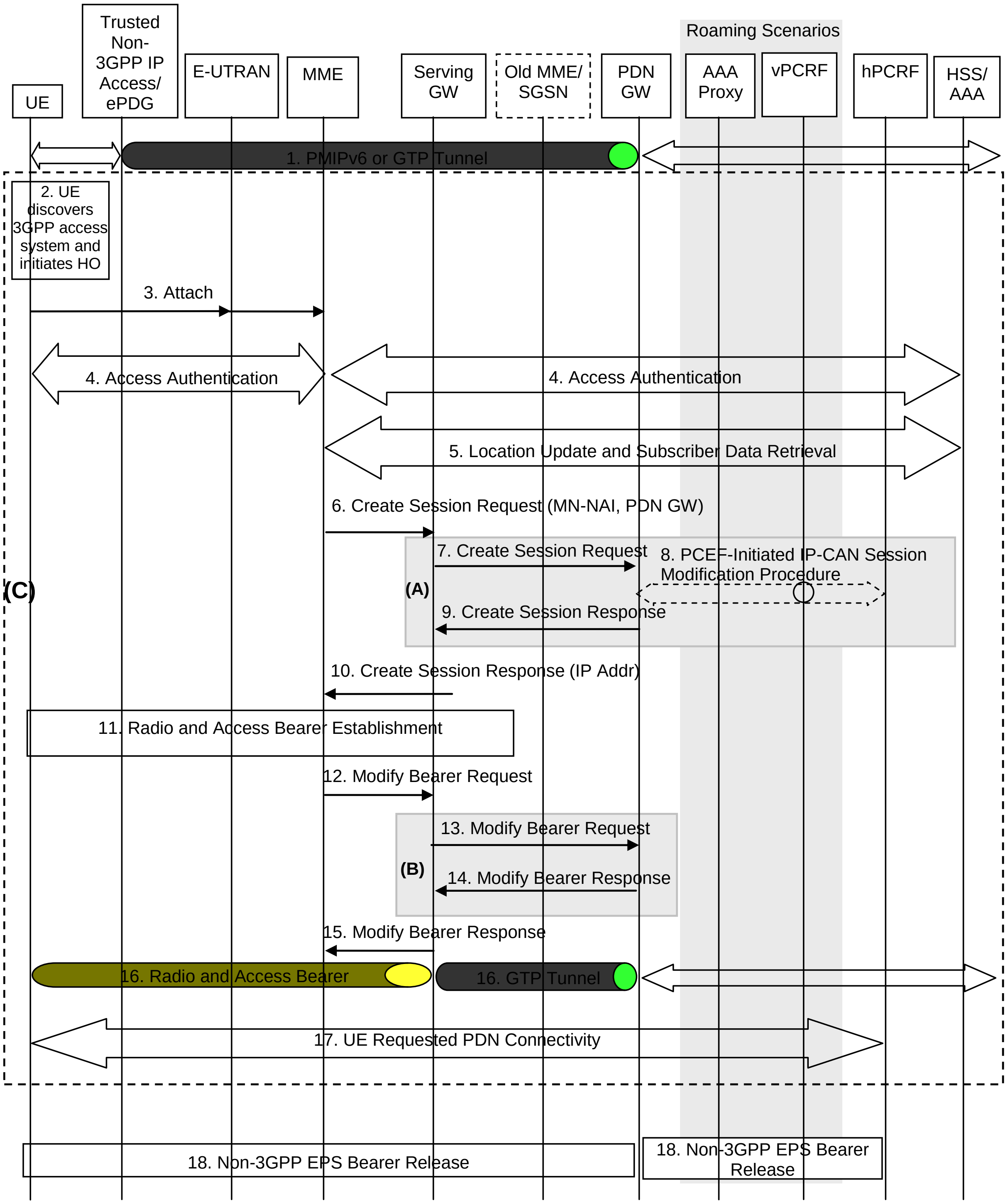

Roaming Scenarios
UE
Trusted Non-3GPP IP Access/ ePDG
E-UTRAN
MME
Serving GW
Old MME/ SGSN
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. PMIPv6 or GTP Tunnel
2. UE discovers 3GPP access system and initiates HO
3. Attach
4. Access Authentication
4. Access Authentication
5. Location Update and Subscriber Data Retrieval
6. Create Session Request (MN-NAI, PDN GW)
7. Create Session Request
8. PCEF-Initiated IP-CAN Session Modification Procedure
(A)
(C)
9. Create Session Response
10. Create Session Response (IP Addr)
11. Radio and Access Bearer Establishment
12. Modify Bearer Request
13. Modify Bearer Request
(B)
14. Modify Bearer Response
15. Modify Bearer Response
16. Radio and Access Bearer
16. GTP Tunnel
17. UE Requested PDN Connectivity
18. Non-3GPP EPS Bearer Release
18. Non-3GPP EPS Bearer Release

Figure 8.2.10.2.5-1: Handover from Trusted WLAN on S2a to 3GPP access for roaming, LBO and non-roaming scenarios

This procedure is as in TS 23.402 [3] clause 8.2.1.1/8.2.1.2 with the following differences:

- Step 1. There is a GTP or PMIP tunnel between TWAN and PGW.
- Step 18. The PDN GW shall initiate resource allocation deactivation procedure in the TWAN as defined in clause 8.2.10.2.9.

8.2.10.2.6 UE/TWAN Requested PDN disconnection in WLAN on S2a

8.2.10.2.6.1 UE/TWAN requested PDN disconnection in WLAN on GTP S2a

For multiple PDN connections, this disconnection procedure shall be repeated for each PDN connection that needs to be released.

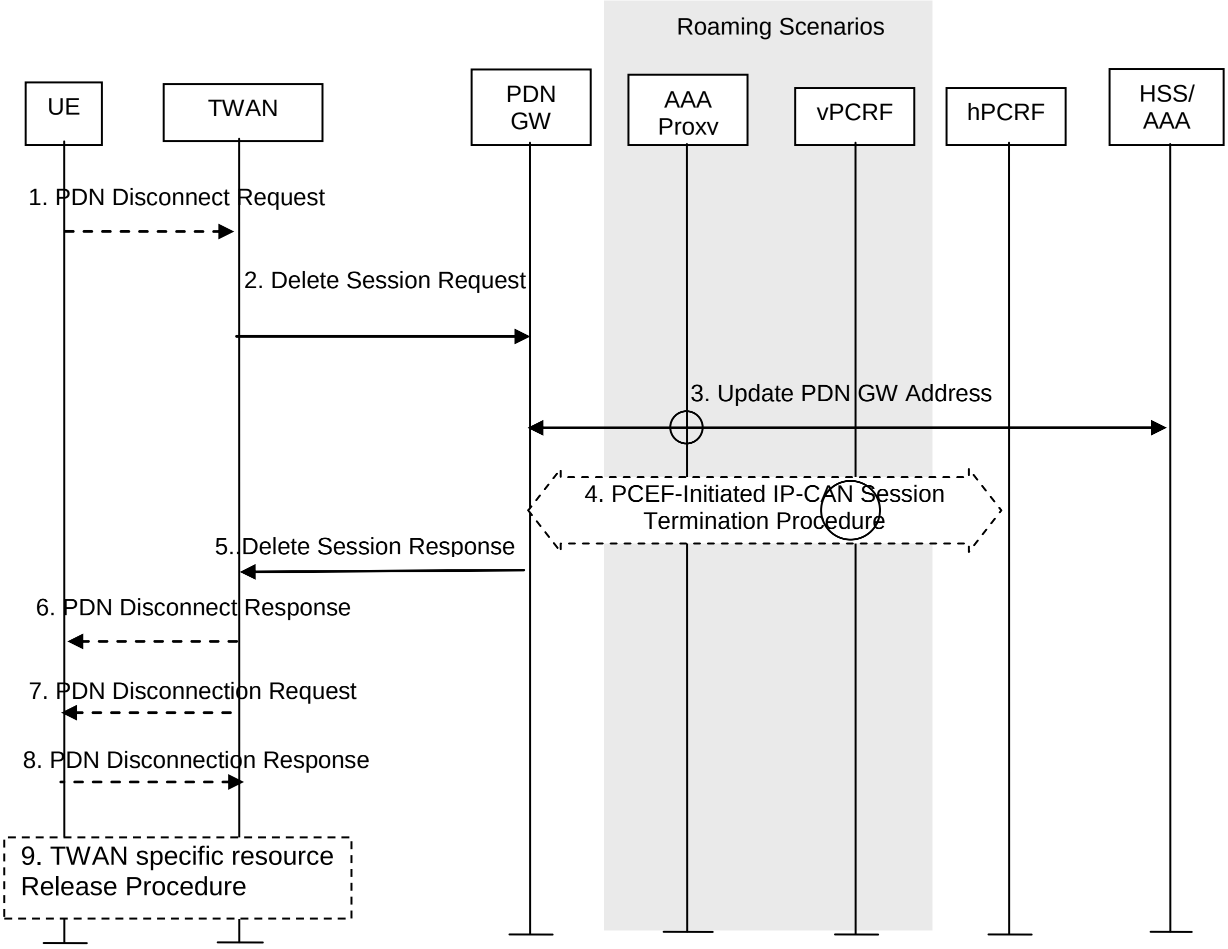

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. PDN Disconnect Request
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. PDN Disconnect Response
7. PDN Disconnection Request
8. PDN Disconnection Response
9. TWAN specific resource Release Procedure

Figure 8.2.10.2.6.1-1: UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF do not occur. Instead, the PDN GW may employ static configured policies.

- Step 1. If the PDN disconnection is initiated by the UE, the UE sends a WCS PDN Disconnection Request (p2p link ID) to the TWAG. The p2p link ID identifies a PDN connection uniquely. Step 2. The TWAN releases the PDN connection and sends a Delete Session Request (Linked EPS Bearer ID) message for this PDN connection to the PDN GW.
- Step 3. The PDN GW informs the 3GPP AAA Server of the PDN disconnection.
- Step 4. The PDN GW deletes the IP-CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [4].
- Step 5. The PDN GW acknowledges with a Delete Session Response (Cause) message.
- Step 6. TWAN sends WCS PDN disconnection response to the UE.

- Step 7. If the PDN disconnection was initiated by the TWAG, then the UE is informed of the disconnection by means of a WCS PDN Disconnection Request (User Plane Connection ID).
- Step 8. The UE acknowledges the disconnection request received in step 7.

NOTE 1: Either step 1 and 6, or step 7 and 8, are performed. Step1 and 6 is used for UE initiated disconnection procedure, step7 and 8 is for TWAN initiated disconnection procedure.

NOTE 2: If NSWO disconnection is performed steps from 2 to 5 are skipped.

8.2.10.2.6.2 UE TWAN requested PDN disconnection in WLAN on PMIP S2a

Editor's note: The procedure is FFS.

8.2.10.2.7 UE initiated Detach in WLAN on S2a

8.2.10.2.7.1 UE initiated Detach in WLAN on GTP S2a

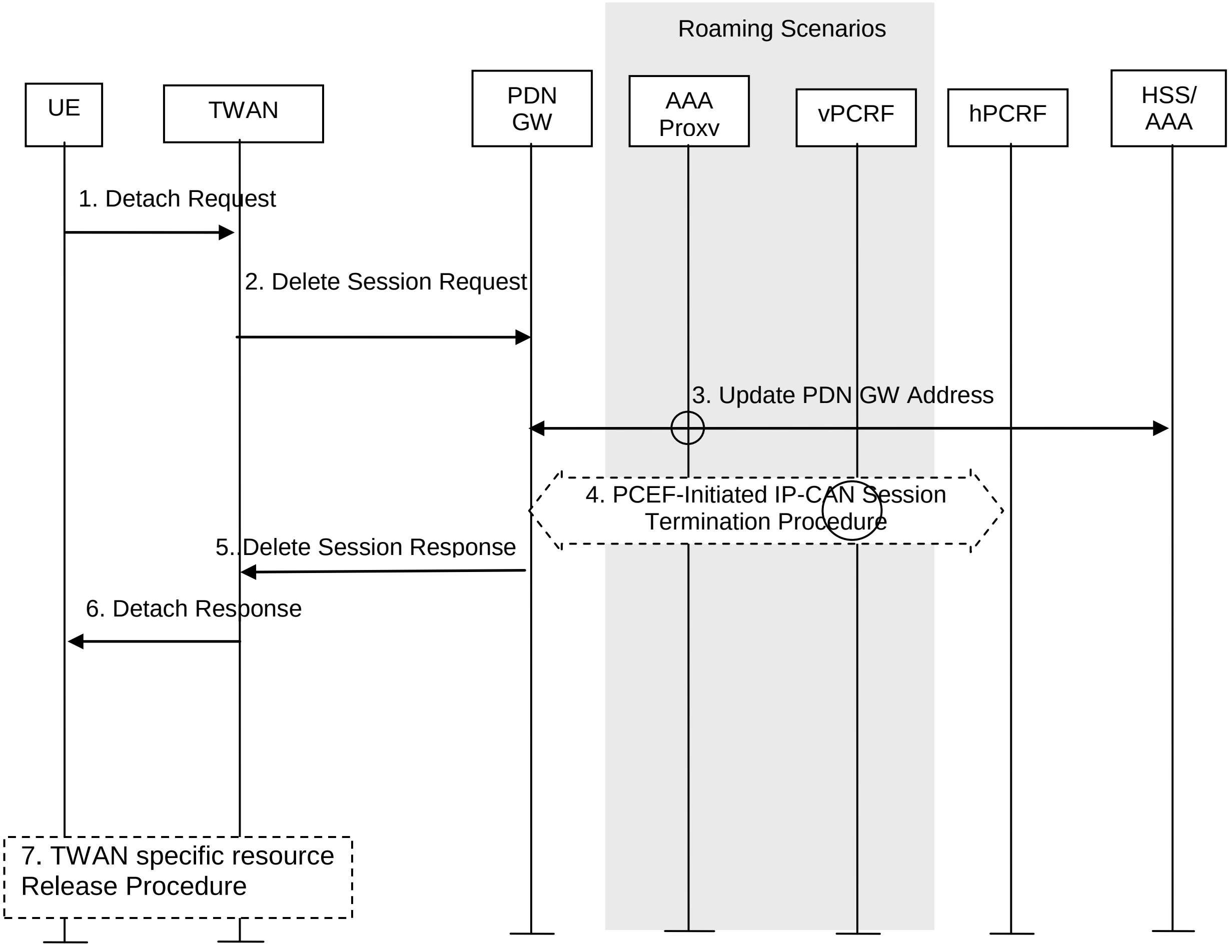

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. Detach Request
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. Detach Response
7. TWAN specific resource Release Procedure

Figure 8.2.10.2.7.1-1: UE -initiated Detach procedure with GTP S2a in WLAN

- Step1 The UE sends a WCS Detach Request to the TWAN.
- Step2 - Step5. Same as step 2-5 in clause 8.2.10.2.6.1 The TWAN deleted all the S2a bearers. - Step6. TWAN send Detach Response to the UE.

For NSWO connection, the release procedure is the same as TS 23.402 [3] clause 16.3.1.1.

8.2.10.2.7.2 UE initiated Detach in WLAN on PMIP S2a

Editor's note: This procedure is FFS.

8.2.10.2.8 HSS/AAA Initiated Detach Procedure in WLAN

8.2.10.2.8.1 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a

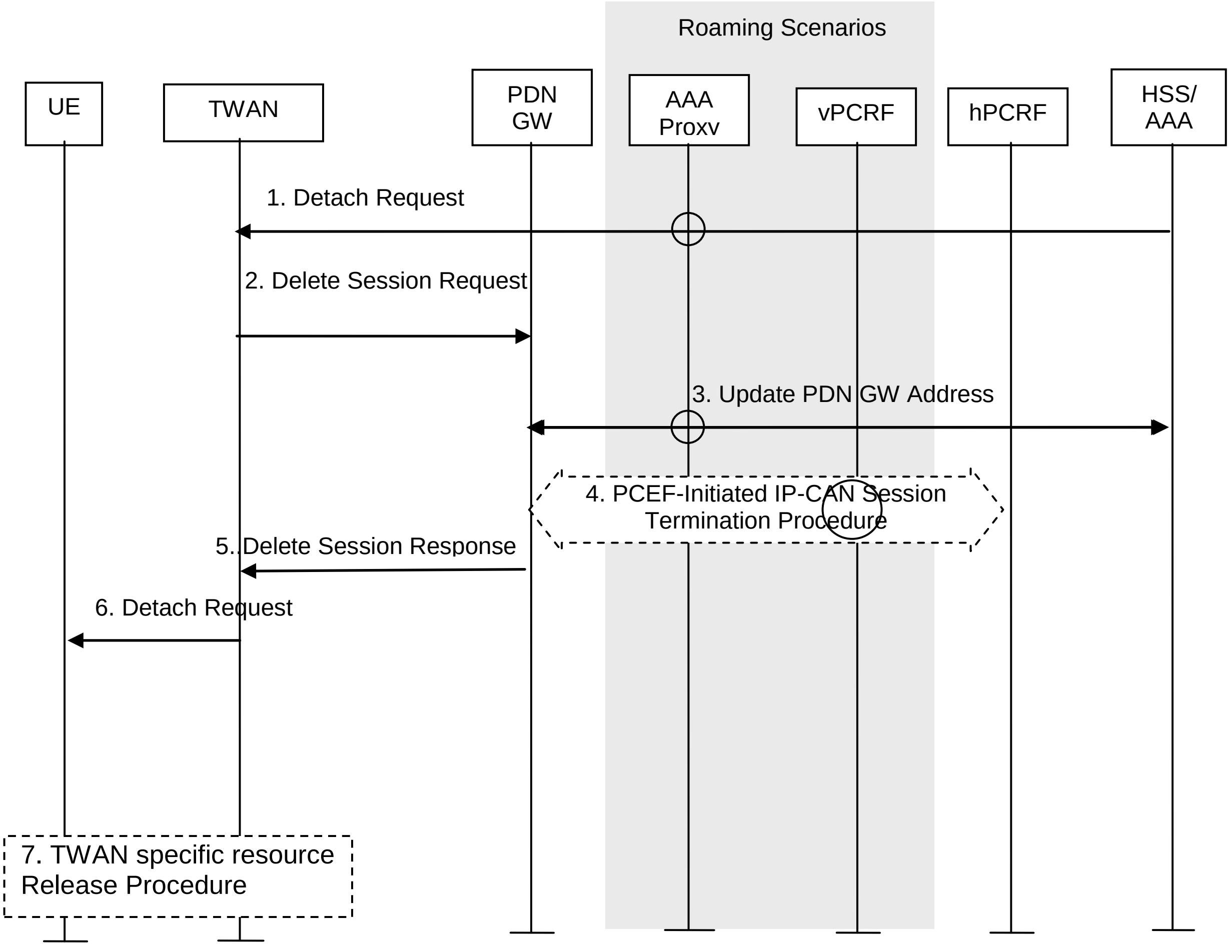

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. Detach Request
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. Detach Request
7. TWAN specific resource Release Procedure

Figure 8.2.10.2.8.1-1: HSS/AAA Initiated Detach Procedure with GTP S2a

- Step-1 HSS/AAA send Detach Request to the TWAN
- Step-2-step5 is same as procedure in 8.2.10.2.6.1.

For NSWO connection, the release procedure is the same as TS 23.402 [3] clause 16.3.1.1.

8.2.10.2.8.2 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a

Editor's note: This procedure is still to be added.

8.2.10.2.9 PDN GW initiated Resource Allocation Deactivation

8.2.10.2.9.1 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

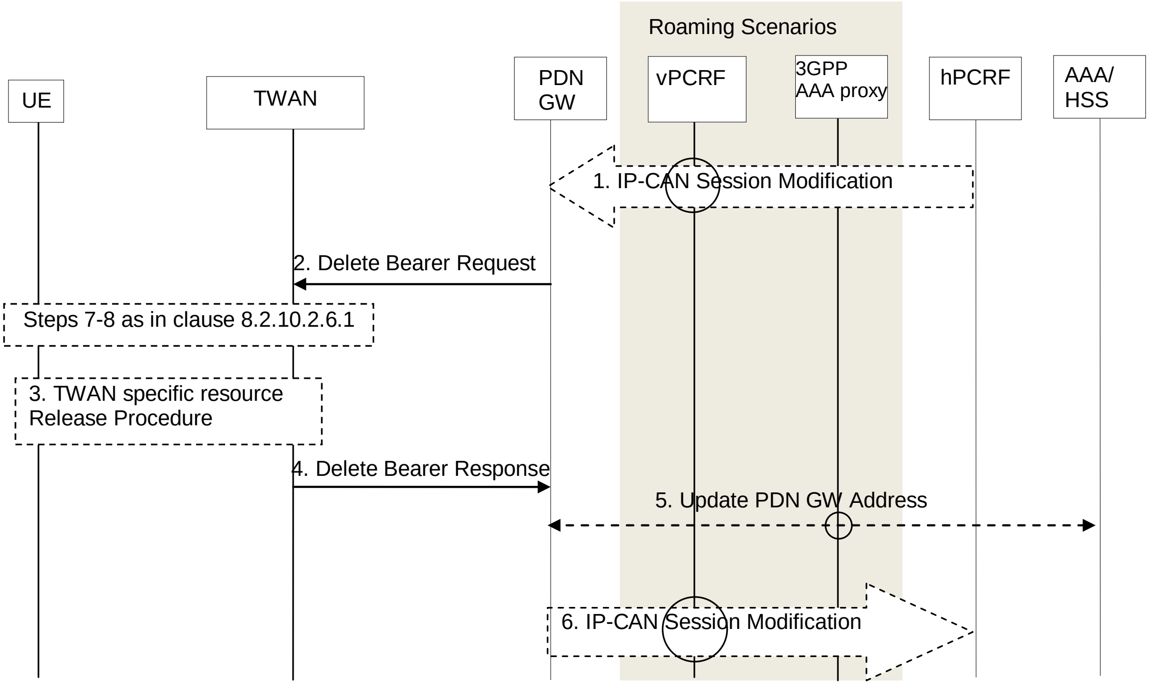

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
3GPP AAA proxy
hPCRF
AAA/ HSS
1. IP-CAN Session Modification
2. Delete Bearer Request
Steps 7-8 as in clause 8.2.10.2.6.1
3. TWAN specific resource Release Procedure
4. Delete Bearer Response
5. Update PDN GW Address
6. IP-CAN Session Modification

Figure 8.2.10.2.9.1-1: PDN GW Initiated Bearer Deactivation with GTP on S2a

The step1,-6 is same as step1,2,4,5,6 in Clause 16.4.1 in TS 23.402 [3].

If all TWAN resources related to a PDN connection are released, then step 7 and 8 of Figure 8.2.10.2.6.1-1: (UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN) are carried out to inform the UE of the PDN connection release.

8.2.10.2.9.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a

Editor's note: This procedure is FFS.

8.2.10.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

8.2.10.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 as well as simplicity of implementation in the UE should be evaluated.

The following aspects are considered and evaluated for the solution:

i) Impacts to existing network deployment:

a) There is no additional requirement for WLAN APs compared to Rel-11.

b) For TWAG, it shall support EAP enhancement for UE and network capability negotiation, and support the new control plane protocol, support p2p link for each PDN connections.

ii) Impacts to UE:

The UE should be capable of supporting enhanced EAP procedures.

It should support the new control plane protocol and user plane p2p link using virtual MAC or VLAN.

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA'):

The following protocols are extended:

a) UE network capability negotiation is enhanced for EAP protocol.

b) Defining a new control plane protocol for mobility management (e.g. APN, PDN type, user plane p2p link delivery etc).

iv) Impacts to protocols defined by other SDOs (e.g. DHCP):

For VLAN based/Virtual MAC based control plane protocol, we need to define a new Ethertype in IEEE.

v) Control plane

a) The latency/load can be affected by the messages in the following procedures:

b) A new control plane protocol is used for all the PDN connections/ NSWO connection.

c) For L3 based control plane protocol, the NSWO connection may also established by DHCP/RS/RA after authentication procedure.

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements:

a) Co-existence with Rel-11 SaMOG

b) Support for IP address preservation during handover

c) Simultaneous support for S2a EPC-routed and NSWO; support of simultaneous multiple PDN connections

vii) Other functional limitations:

There is no other functional limitation.

8.2.11 Solution 11 - Two scenario approach using DHCPv4 and Stateless DHCPv6 and a VMAC u-plane

8.2.11.1 Functional Description

Editor's note: It should be described whether and how the solution fulfils the requirements in clause 8.1.

8.2.11.1.1 Overview

Similar to Solution 1, this solution uses a two scenario approach to support handover, PDN connections to the non-default APN and multiple PDN connections:

1. Single-PDN connection scenario: This is a simple extension on top of the Rel-11 SaMOG architecture, where UE and/or NW only support a single PDN connection or a NSWO connection. EAP authentication signalling will be enhanced to enable the UE to indicate the requested connection type (PDN connection/NSWO) and whether a handover is requested.

2. Multiple-PDN-connection scenario: In this scenario, UE and network support multiple PDN connections via WLAN. A UE supporting multiple PDN connections indicates this in addition to the parameters for the single PDN connection as part of the initial EAP authentication. If the network also supports multiple PDN connections, the network indicates this back to the UE in the EAP authentication signalling. If the network indicates multiple PDN connection support, then the multiple-PDN-connection scenario is selected and the UE can request establishment/handover of PDN connections/NSWO connection. To achieve this, DHCPv4 [9] and Stateless DHCPv6 [19] are extended to carry the required control plane signalling.

8.2.11.1.2 User plane

In the single PDN connection scenario, the per-UE point-to-point link as defined for Rel-11 SaMOG is TS 23.402 [3] is used. Thus, the IP packets of the single PDN connection or the NSWO connection are carried directly on top of IEEE 802.11.

In the multiple-PDN-connection scenario the TWAG virtual MAC (VMAC) as described in 8.2.2.1.1.2 is used for PDN connections and the NSWO connection.

NOTE: At most one NSWO connection is supported per UE. NSWO connection can be established during the initial Attach, or after the initial PDN connection set up is complete.

8.2.11.1.3 Control plane

EAP authentication signalling is extended to signal

- in UE to NW direction:
  - the requested connectivity type (NSWO or PDN connection),
  - the requested APN (not to be included for NSWO; optional for connectivity type PDN connection for new PDN connections; mandatory for connectivity type PDN connection if hand-over is requested),
  - a hand-over indicator (optional; indicates that a hand-over is requested for the requested APN), and
  - the multiple PDN connection supported indicator (optional; indicates that the UE supports multiple PDN connections over Trusted WLAN).
- in NW to UE direction:
  - Selected APN,
  - the multiple PDN connection supported indicator (optional; included if UE has indicated support for multiple PDN connections and if NW also supports multiple PDN connections).

DHCPv4 [9] and Stateless DHCPv6 [19] are extended to signal

- In UE to NW direction:
  - UE-initiated connectivity request with the following parameters:
    - connectivity type (PDN connection or NSWO access),
    - PDN type (IPv4, IPv6, IPv4v6),
    - the requested APN (not to be included for connectivity type NSWO; mandatory if connectivity type is PDN connection),

NOTE: Whether the connectivity type NSWO is signalled as a pre-defined APN is up to Stage 3 to decide.

    - hand-over indicator (optional; indicates that a hand-over is requested for the requested APN).
  - PDN/NSWO disconnection request.
- In NW to UE direction:
  - Selected APN,
  - PDN type (IPv4, IPv6, IPv4v6),
  - TWAG VMAC address,
  - Cause codes (as needed).

8.2.11.2 Procedures

Editor's note: The call flows are described in this clause.

8.2.11.2.1 Initial Attach in WLAN on S2a

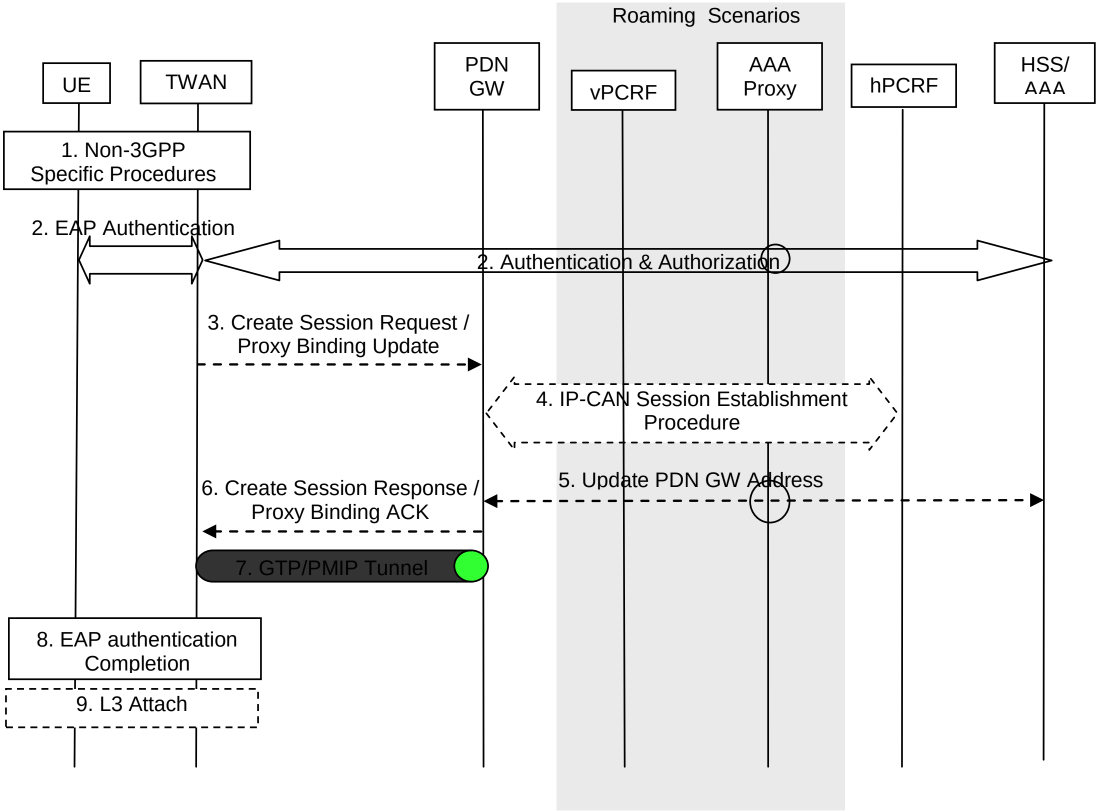

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request / Proxy Binding Update
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Create Session Response / Proxy Binding ACK
7. GTP/PMIP Tunnel
8. EAP authentication Completion
9. L3 Attach

Figure 8.2.11.2.1-1: Initial attachment in WLAN on S2a for roaming and non-roaming scenarios

1. This step is the same as step 1 in TS 23.402 [3] clause 16.2.1

2. As part of the EAP authentication, the UE shall send an indication to the network whether it supports multiple PDN connections. In addition the UE indicates whether it requests a PDN connection or an NSWO connection. In case the UE requests a PDN connection, the UE may indicate an APN.

   These indicators are sent in EAP-AKA' to the 3GPP AAA. The 3GPP AAA sends these indicators to the TWAN.

   If the UE has indicated support for multiple PDN connections and if the network also supports multiple PDN connections, the multiple PDN connection scenario is selected. In this case the network indicates support for multiple PDN connections to the UE and steps 3-7 and step 9 are skipped.

   Otherwise, the network indicates to the UE whether the Rel-12 SaMOG single PDN connection features are supported and if the requested connectivity type (PDN connection or NSWO) is accepted. If the UE requested EPC access and indicated an APN, then the network verifies that it is allowed by subscription. If the UE requested EPC access without indicating APN, then the network indicates the selected (default) APN. If the UE requested NSWO and it was accepted by the network, steps 3-7 are skipped.

   If the requested connectivity feature is not supported or not permitted, the request is rejected with an appropriate cause code.

   If the network does not support Rel-12 SaMOG, then the Rel-11 SaMOG behaviour as defined for the network according to TS 23.402 [3] applies (i.e. the network establishes the PDN connection to the default APN).

3. The TWAN determines the APN based on the UE request and on the subscription data received from the AAA server. Also, the TWAN determines the PDN type according to requested PDN type and subscribed PDN type from HSS, and sets the Dual Address Bearer Flag when the PDN type is set to IPv4v6. The TWAN selects the PDN GW for the selected APN and sends a Create Session Request message (for GTP) or Proxy Binding Update message (for PMIP) to the PDN GW, including APN, PDN type, Dual Address Bearer Flag.

4. The step is same as step 10 in TS 23.402 [3] clause 16.2.1.

5. The 3GPP AAA Server updates PDN GW identity towards the HSS.

6-7. These steps are the same as steps 6-7 in TS 23.402 [3] clause 16.2.1 (for GTP) or clause 16.2.2 (for PMIP). If Dual Address Bearer Flag is set, the PDN GW shall return an IPv4 address and an IPv6 address to the TWAN.

8. TWAN sends EAP success to the UE including either:

   - if the single PDN connection scenario was selected,

   - the selected connectivity type (PDN connection or NSWO), selected APN (if a PDN connection was established), or

   - if the multiple PDN connection scenario was selected, an indication that the multiple PDN connection scenario was selected.

9. The UE may send a DHCPv4 request as per IETF RFC 2131 [28] and/or an IPv6 Router Solicitation. A DHCPv4 message with the allocated IPv4 address and/or Router Advertisement with the allocated IPv6 prefix is sent to the UE. The UE may perform additional IP layer configuration with the TWAN as per standard IETF procedures, e.g. IPv6 Stateless Address Autoconfiguration as per IETF RFC 4862 [58], and Stateless DHCPv6 as per IETF RFC 3736 [30].

NOTE: In the single-connection scenario, if a UE using NSWO wants to establish a PDN Connection, or if the UE has a PDN Connection but wants to use NSWO, the UE needs to detach from TWAN and make a new Initial Attach.

8.2.11.2.2 Initial Attach in WLAN on S2a with hand-over

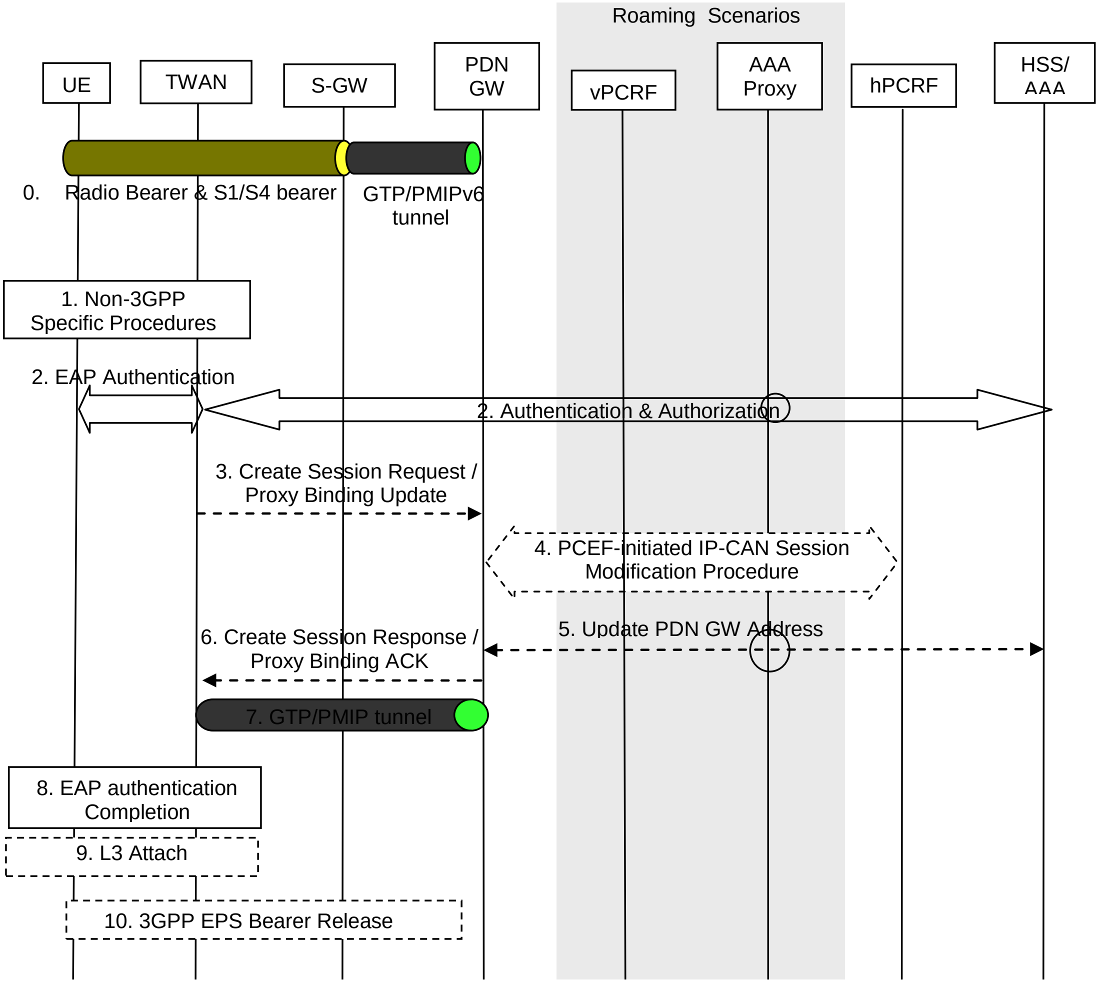

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0. Radio Bearer & S1/S4 bearer
GTP/PMIPv6 tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request / Proxy Binding Update
4. PCEF-initiated IP-CAN Session Modification Procedure
5. Update PDN GW Address
6. Create Session Response / Proxy Binding ACK
7. GTP/PMIP tunnel
8. EAP authentication Completion
9. L3 Attach
10. 3GPP EPS Bearer Release

Figure 8.2.11.2.2-1: Initial attachment in WLAN on S2a for roaming and non-roaming scenarios

The procedure works as the procedure in 8.2.11.2.1 with the following differences:

- Step 0: The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.
- Step 2: This is the same as step 2 in clause 8.2.11.2.1 with the difference that the UE includes a handover indication in EAP-AKA'.
- Step 3: This is the same as step 3 in clause 8.2.11.2.1 with the difference that the handover indication is set in the Create Session Request/Proxy Binding Update to the PDN GW.
- Step 4: The PDN GW performs an IP-CAN session modification procedure as specified in TS 23.203 [4].
- Step 6: This is the same as step 6 in clause 8.2.11.2.1 with the difference that the PDN GW returns the same IP address and/or prefix as previously assigned to the UE on the 3GPP access. Also, the Charging ID provided by the PDN GW is the Charging ID previously assigned to the default bearer of the PDN connection in the 3GPP access.
- Step 10: The PDN GW initiates the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.11.2.3 UE-Initiated Connectivity to PDN / NSWO in WLAN on S2a

This procedure applies if the network has indicated to the UE that the multiple PDN connection scenario is selected as part of the Initial Attach signalling over WLAN.

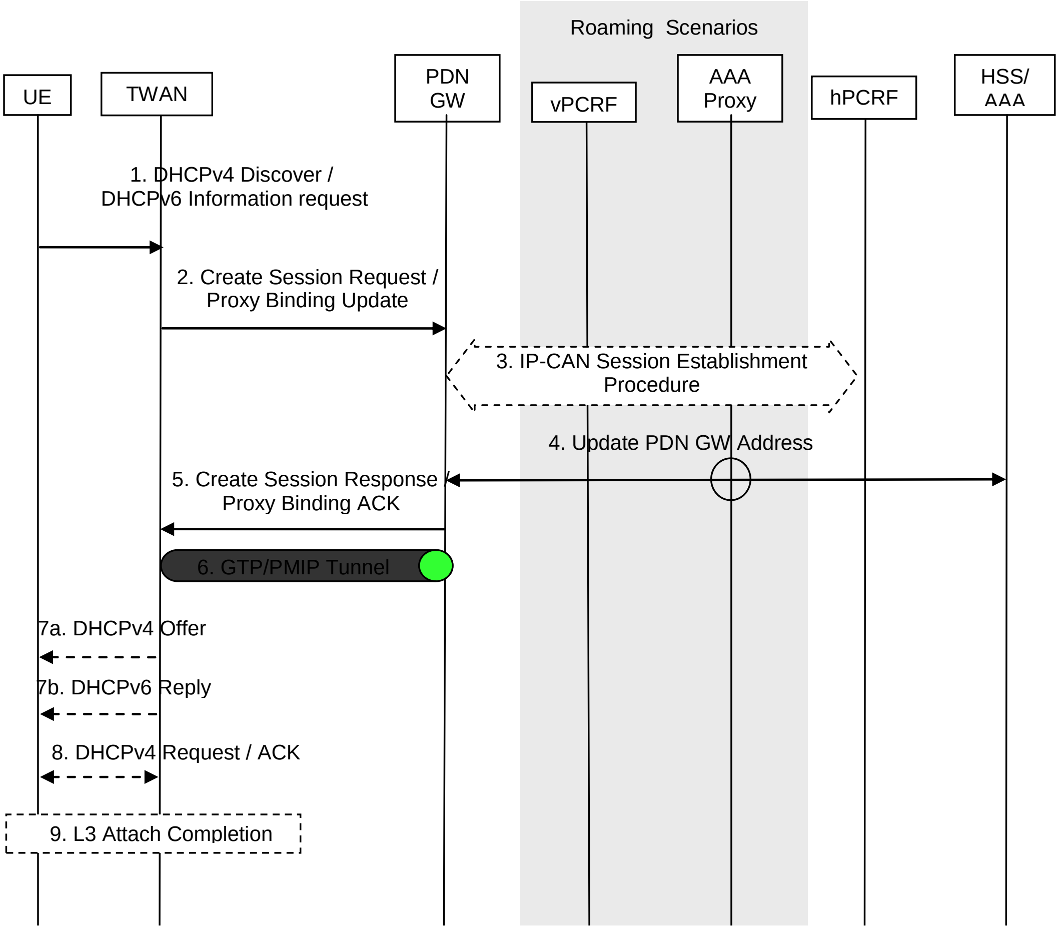

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. DHCPv4 Discover / DHCPv6 Information request
2. Create Session Request / Proxy Binding Update
3. IP-CAN Session Establishment Procedure
4. Update PDN GW Address
5. Create Session Response / Proxy Binding ACK
6. GTP/PMIP Tunnel
7a. DHCPv4 Offer
7b. DHCPv6 Reply
8. DHCPv4 Request / ACK
9. L3 Attach Completion

Figure 8.2.11.2.3-1: UE-initiated connectivity to additional PDN via Trusted WLAN Access

The UE can request additional PDN connectivity or NSWO access by sending a DHCPv4 request or a Stateless DHCPv6 request including the required parameters.

For PDN type IPv4 DHCPv4 shall be used. For PDN type IPv6 and PDN type IPv4v6 Stateless DHCPv6 shall be used.

For DHCPv4 messaging and security handling, RFC 6704 shall be applied.

1. The UE shall send a DHCPv4 discover request as per IETF RFC 2131 [9] or a Stateless DHCPv6 Information request as per IETF RFC3736 [19]), including requested connectivity type (PDN connection or NSWO access), requested APN, requested PDN type. If the UE requests a PDN connection, it shall include an APN.

   - If UE provides its requested APN to TWAN, and the TWAN determines that S2a shall be established, the TWAN continues in step 2.

   - If the UE requested NSWO access and the UE does not have an active NSWO connection, the procedure continues in step 7. If the UE requests NSWO access but already has an NSWO connection, the request is rejected.

2. TWAN decides PDN type according to requested PDN type and subscribed PDN type from HSS, and sets the Dual Address Bearer Flag when the PDN type is set to IPv4v6. The TWAN sends a Create Session Request message (for GTP) or Proxy Binding Update (for PMIP) to the PDN GW, including APN, PDN type, Dual Address Bearer Flag.

3. The step is same as step 10 in TS 23.402 [3] clause 16.2.1 (for GTP) or clause 16.2. (for PMIP).

4. The 3GPP AAA Server updates the PDN GW identity towards the HSS.

5-6. These steps are the same as steps 6-7 in TS 23.402 [3] clause 16.2.1 (for GTP) or clause 16.2.2 (for PMIP). If Dual Address Bearer Flag is set, the PDN GW shall return both IPv4 address and IPv6 address to TWAN.

7a. For DHCPv4, the TWAN returns DHCP offer message to the UE, selected APN (if a PDN connection was established) and the TWAG virtual MAC address to be used with that PDN or NSWO connection is included.

7b. For Stateless DHCPv6, the TWAN returns the Stateless DHCPv6 Reply message to the UE including the selected connectivity type, APN, PDN type and the TWAG VMAC address.

8. UE sends DHCP Request (for DHCPv4) to TWAN, and TWAN returns DHCP Ack message to the UE, including the selected connectivity type, APN, and the UE's IPv4 address allocated by its serving PDN GW.

NOTE: DHCP Request and ACK messages between UE and TWAG are using TWAG's MAC address.

9. The UE may send an IPv6 Router Solicitation. A Router Advertisement with IPv6 prefix is sent to the UE. The UE may perform additional IP layer configuration with the TWAN as per standard IETF procedures, e.g. IPv6 Stateless Address Autoconfiguration as per IETF RFC 4862 [58], and Stateless DHCPv6 as per IETF RFC 3736 [30].

NOTE: The related signalling is using the assigned TWAG VMAC address.

8.2.11.2.4 Handover procedure for additional PDN connections from 3GPP access to WLAN on S2a

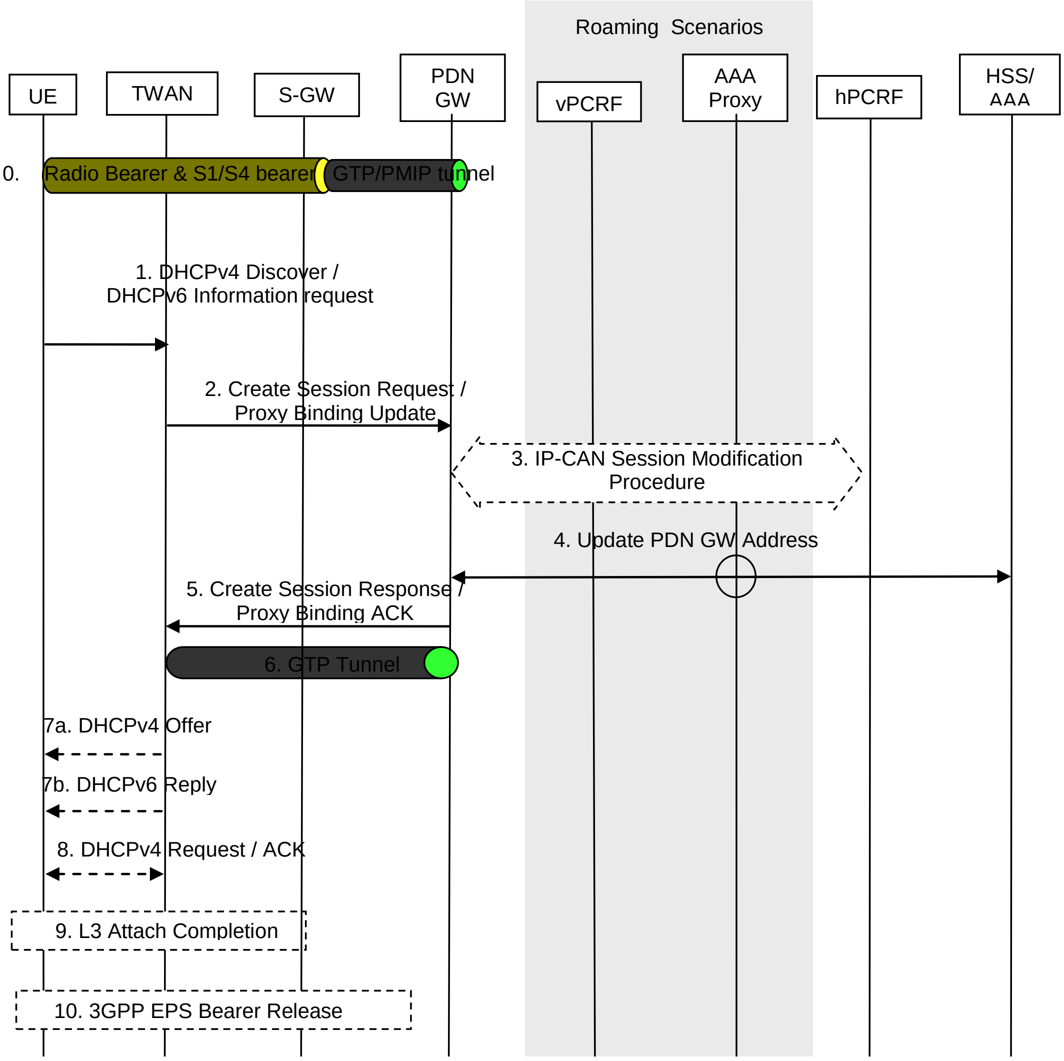

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0.
Radio Bearer & S1/S4 bearer
GTP/PMIP tunnel
1. DHCPv4 Discover / DHCPv6 Information request
2. Create Session Request / Proxy Binding Update
3. IP-CAN Session Modification Procedure
4. Update PDN GW Address
5. Create Session Response / Proxy Binding ACK
6. GTP Tunnel
7a. DHCPv4 Offer
7b. DHCPv6 Reply
8. DHCPv4 Request / ACK
9. L3 Attach Completion
10. 3GPP EPS Bearer Release

Figure 8.2.11.2.4-1: Handover procedure for additional PDN connections from 3GPP access to WLAN on S2a

This procedure works as the procedure defined in clause 8.2.11.2.3 with the following differences:

- Step 0: The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.
- Step 1: This is the same as step in clause 8.2.11.2.3 with the difference that the UE indicates that it requests a PDN connection, includes an APN and includes a handover indicator.
- Step 2: This is the same as step 2 in clause 8.2.11.2.1 with the difference that the UE includes a handover indicator in the Create Session Request or the Proxy Binding Update.
- Step 3: The PDN GW initiates the IP-CAN Session Modification Procedure as specified in TS 23.203 [4].
- Step 5: This is the same as step 5 in clause 8.2.11.2.1 with the difference that the PDN GW includes the IP address and/or prefix previously assigned to the UE for the same PDN connection on the 3GPP access.
- Step 10: The PDN GW initiates the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 [3] clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1.

8.2.11.2.5 Handover procedure from WLAN on S2a to 3GPP access

This procedure is the same as described in TS 23.402 [3] clauses 8.2.1.1/8.2.1.2/8.2.1.3 with the following differences:

- Step 0: There is either a PMIP or GTP tunnel between TWAN and PDN GW.

For GTP-based S5/S8 for EUTRAN as defined in TS 23.402 [3] clause 8.2.1.1

- Step 18: PDN GW shall initiate the PDN GW initiated Resource Allocation Deactivation in WLAN procedure as defined in TS 23.402 [3] clause 16.2.1 (for GTP-based S2a) or clause 16.2.2 (for PMIP-based S2a).

For PMIP-based S5/S8 for EUTRAN as defined in TS 23.402 [3] clause 8.2.1.2

- Step 19: PDN GW shall initiate the PDN GW initiated Resource Allocation Deactivation in WLAN procedure as defined in TS 23.402 [3] clause 16.2.1 (for GTP-based S2a) or clause 16.2.2 (for PMIP-based S2a).

For GTP-based S5/S8 for EUTRAN/GERAN as defined in TS 23.402 [3] clause 8.2.1.3.

- Step 17: PDN GW shall initiate the PDN GW initiated Resource Allocation Deactivation in WLAN procedure as defined in TS 23.402 [3] clause 16.2.1 (for GTP-based S2a) or clause 16.2.2 (for PMIP-based S2a).

8.2.11.2.6 Detach and PDN disconnection in WLAN on S2a

8.2.11.2.6.1 UE/TWAN Initiated Detach Procedure in WLAN on S2a

If the single PDN connection scenario was selected, this procedure is the same as TS 23.402 [3] clause 16.3.1.1 (for GTP) or clause 16.3.2.1 (for PMIP).

If the multiple PDN connection scenario was selected, this procedure is the same as TS 23.402 [3] clause 16.3.1.1 (for GTP) or clause 16.3.2.1 (for PMIP) with the difference that the TWAN releases all PDN connections of the UE that are active on S2a. In addition, the resources for an active NSWO connection of the UE are locally released by the TWAN.

8.2.11.2.6.2 HSS/AAA Initiated Detach Procedure in WLAN on S2a

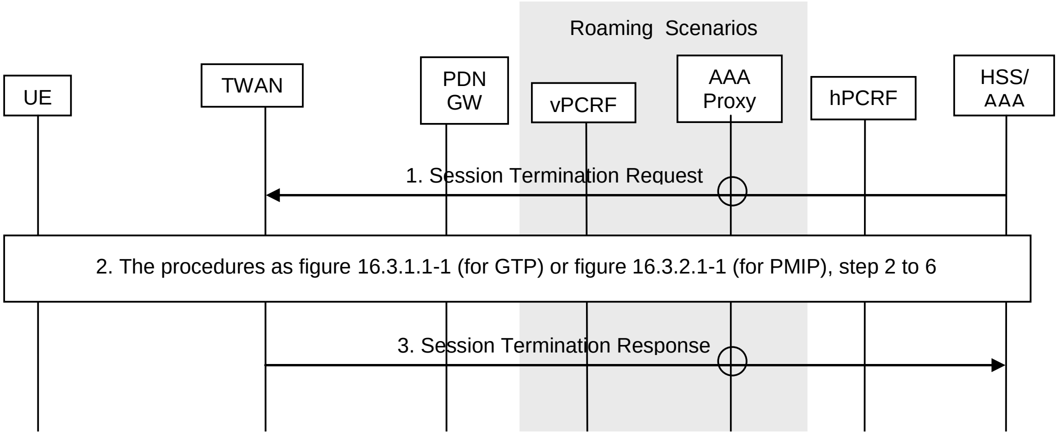

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Session Termination Request
2. The procedures as figure 16.3.1.1-1 (for GTP) or figure 16.3.2.1-1 (for PMIP), step 2 to 6
3. Session Termination Response

Figure 8.2.11.2.6.2-1: HSS/AAA Initiated Detach Procedure in WLAN on S2a

This procedure is the same as specified in TS 23.402 [3], clause 16.3.1.2 (for GTP) and clause 16.3.2.2 (for PMIP) with the different that in the multiple PDN connection scenario in step 2 all active PDN connections of the UE over S2a are deactivated.

8.2.11.2.6.3 UE requested PDN/NSWO Disconnection Procedure in WLAN on S2a

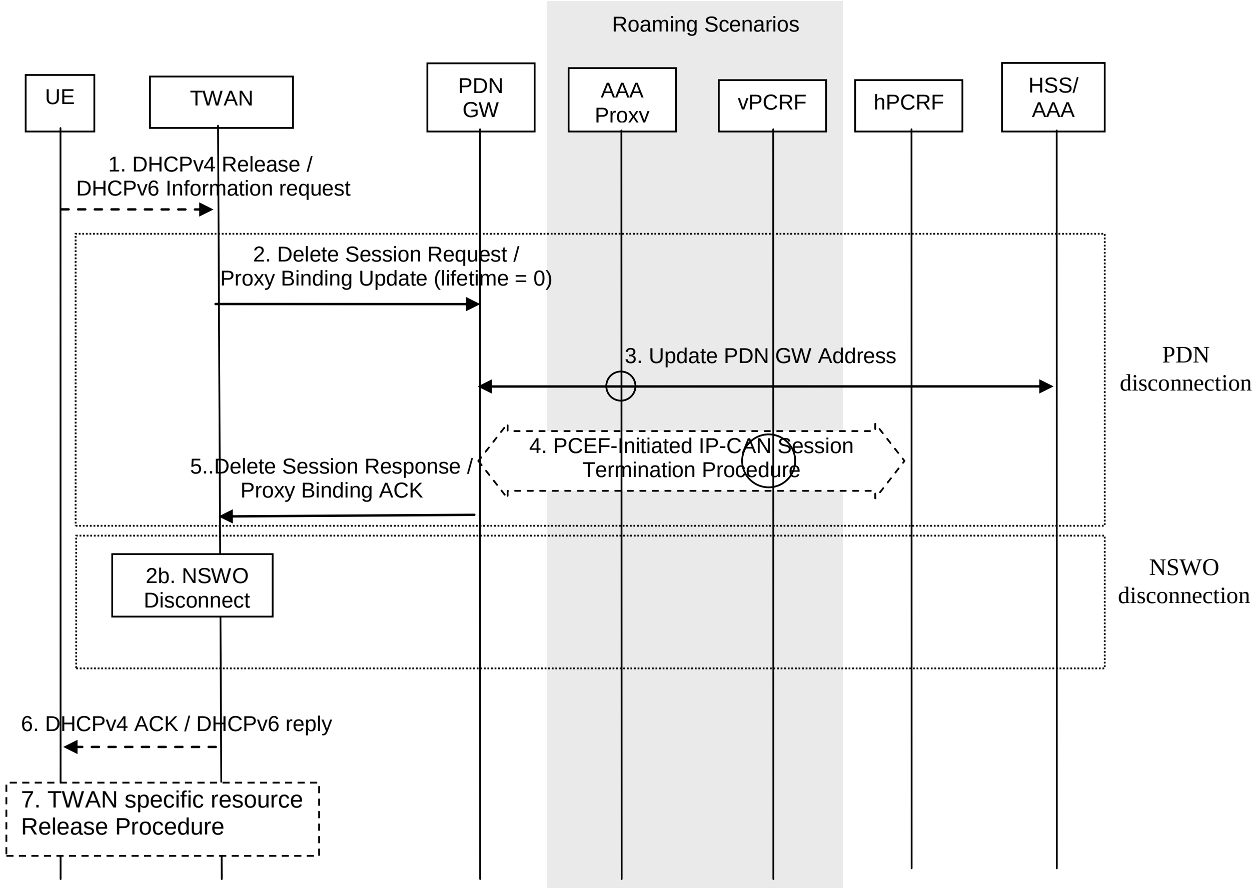

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. DHCPv4 Release / DHCPv6 Information request
2. Delete Session Request / Proxy Binding Update (lifetime = 0)
3. Update PDN GW Address
PDN disconnection
4. PCEF-Initiated IP-CAN Session Termination Procedure
5..Delete Session Response / Proxy Binding ACK
2b. NSWO Disconnect
NSWO disconnection
6. DHCPv4 ACK / DHCPv6 reply
7. TWAN specific resource Release Procedure

Figure 8.2.11.2.6.3-1: UE-initiated PDN disconnection procedure

This procedure applies only to the multiple PDN connection scenario and enables the UE to request disconnection of a PDN or NSWO connection.

For PDN type IPv4 DHCPv4 shall be used. For PDN type IPv6 Stateless DHCPv6 shall be used. For IPv4v6 the UE may use DHCPv4 or Stateless DHCPv6.

For DHCPv4 messaging and security handling, RFC 6704 shall be applied.

1. The UE shall send a DHCPv4 release request as per IETF RFC 2131 [9] or a Stateless DHCPv6 Information request as per IETF RFC3736 [19]), including the TWAG VMAC address of the PDN or NSWO connection to deactivate.

2. If the VMAC address provided by the UE relates to a PDN connection, then steps 2 to 5 are applied, which are the same as steps 2-5 in TS 23.402 [3] clause 16.3.1.1 (for GTP) or clause 16.3.2.1 (for PMIP).

   2b. If the VMAC address provided by the UE relates to an NSWO connection, then the TWAN locally deactivates the NSWO connection.

6 The TWAN sends a DHCPv4 Acknowledgement message or a Stateless DHCPv6 reply to the UE to acknowledge the release of the connection.

8.2.11.2.6.4 TWAN requested PDN/NSWO Disconnection Procedure in WLAN on S2a

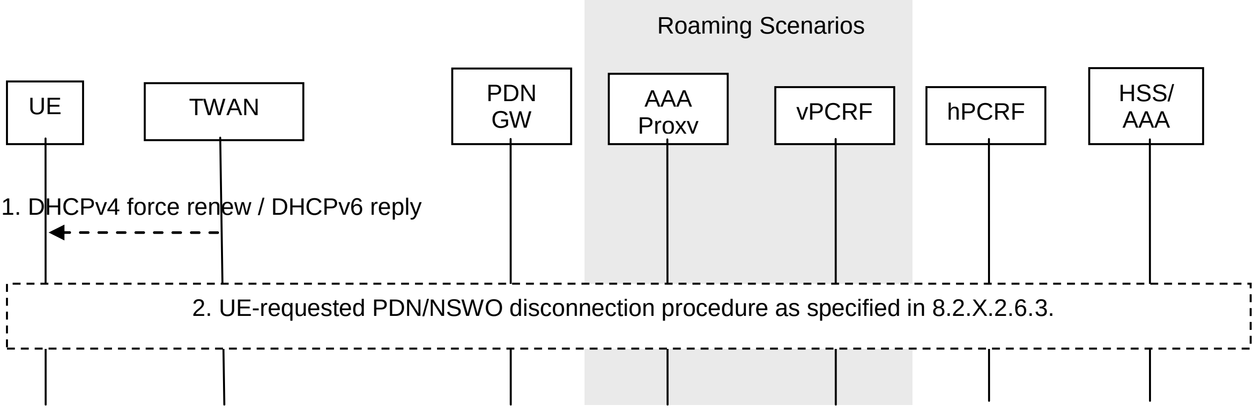

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxv
vPCRF
hPCRF
HSS/ AAA
1. DHCPv4 force renew / DHCPv6 reply
2. UE-requested PDN/NSWO disconnection procedure as specified in 8.2.X.2.6.3.

Figure 8.2.11.2.6.4-1: TWAN requested PDN/NSWO Disconnection Procedure in WLAN on S2a

This procedure applies only the multiple PDN connection scenario and enables the TWAN to request disconnection of a PDN or NSWO connection.

1. The TWAN sends a DHCPv4 FORCE RENEW message or a Stateless DHCPv6 reply including the TWAG VMAC address of the PDN or NSWO connection to deactivate.

NOTE: Whether the DHCPv6 reply message is used to trigger the UE-requested disconnection procedure or whether the DHCPv6 reconfigure message is used instead is up to Stage 3.

2. The UE-requested PDN/NSWO disconnection procedure (clause 8.2.11.2.6.2) is applied for the VMAC address as indicated by the TWAN.

8.2.11.3 Impacts on existing nodes or functionality

Editor's note: Impacts to UE and network elements within TWAN as well as EPC to support backward compatibility and co-existence with Rel-11 in this clause.

8.2.11.3.1 Single PDN connection scenario

The UE shall support:

- EAP-AKA' extensions for negotiation of SaMOG capabilities and parameters for the initial PDN/NSWO connection.

The TWAN shall support:

- Additional AVP on STa for negotiation of SaMOG capabilities and parameters for the initial PDN/NSWO connection.

The AAA server shall support:

- Additional AVP on STa for negotiation of SaMOG capabilities and parameters for the initial PDN/NSWO connection.
- EAP-AKA' extensions for negotiation of SaMOG capabilities and parameters for the initial PDN/NSWO connection.

8.2.11.3.2 Multiple PDN connection scenario

In addition to the requirements for the single PDN connection scenario the UE shall support:

- TWAG VMAC-based virtual interfaces for PDN/NSWO connections.
- For IPv4 PDN connections: DHCPv4 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

- For IPv4v6 PDN connections: Stateless DHCPv6 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

- For IPv6 PDN connections: Stateless DHCPv6 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

In addition to the requirements for the single PDN connection scenario the TWAN shall support:

- Support of TWAG VMAC.

- For IPv4 PDN connections: DHCPv4 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

- For IPv4v6 PDN connections: Stateless DHCPv6 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

- For IPv6 PDN connections: Stateless DHCPv6 including the required extensions/modifications to support PDN/NSWO connection establishment/tear-down, etc.

8.2.11.4 Evaluation

Editor's note: The fulfilment to the requirements in clause 8.1 as well as simplicity of implementation in the UE should be evaluated.

i) Impacts to existing network deployment:

a) No additional requirements for WLAN APs compared to Rel-11.

b) The TWAN needs to additionally support (on top of Rel-11):

- For the single PDN connection scenario: the EAP-AKA' enhancements.

- For the multiple PDN connection scenario: the EAP-AKA' enhancements, extended DHCPv4/Stateless DHCPv6, VMAC, extension to STa.

ii) Impacts to UE:

a) for the single PDN connection scenario the UE needs to support: EAP-AKA' extensions.

for the multiple PDN connection scenario the UE needs to support: EAP-AKA' extensions, extended DHCPv4/extended Stateless DHCPv6, TWAG VMAC-based user plane.

iii) Impacts to 3GPP protocols/extensions (e.g. EAP AKA'):

The following protocols are extended:

a) EAP-AKA' needs to be extended with capability negotiation (Rel-12 SaMOG and multiple PDN connection support), connectivity type (PDN connection or NSWO), PDN type, APN, handover indication.

b) STa protocol needs to be extended accordingly.

iv) Impacts to protocols defined by other SDOs (e.g. DHCP):

Extensions to DHCPv4 and Stateless DHCPv6 to carry the signalling exchange required for setting up / releasing a PDN/NSWO connection over TWAN. This includes support of new information elements indicating connectivity type (PDN connection or NSWO), PDN type, APN, handover indication, TWAG VMAC address and new cause codes.

v) Control plane

a) For the PDN/NSWO connection in the single PDN connection scenario the signalling latency and amount of signalling is the same as for SaMOG Rel-11.

For connections in the multiple PDN connection scenario the latency/amount of signalling is as follows: for PDN type IPv4 four messages are needed between UE and TWAG (since control plane signalling is part of the DHCPv4 address assignment). For PDN type IPv6 three messages are needed (two for Stateless DHCPv6 to establish the connection and one for the Router Advertisement sent by the TWAG). For PDN type IPv4v6 two messages are needed to establish the connection; one additional message is needed for the Router Advertisement to configure the IPv6 address; four messages are needed to configure the IPv4 address.

vi) Compliance to clause 8.1 SaMOG phase-2 system requirements:

The solution can coexist with Rel-11 SaMOG. It supports IP address preservation during handovers. It also supports multiple simultaneous PDN connections via S2a with NSWO in parallel (in case of the multiple PDN connection scenario).

vii)Other functional limitations:

none.

8.3 Evaluation

Editor's note: This clause will include all solution(s) assessment.

8.3.1 List of SaMOG Phase 2 Solutions

The following table captures- the list of potential solutions to be evaluated for SaMOG Phase 2:

Table 8.3.1-1: List of SaMOG Phase 2 Solutions and their considerations status for SaMOG Phase 2

Solution#	Solution Title	Potential Candidate (Y/N)
1	Tunnelled approach with dedicated UE-TWAG control protocol	Y
2	Layer 2 solution based on Stateful Address Configuration of Per-PDN	Y
3	Stateful DHCP-based Solution	N
4		N
5	Associating APN/PDN with Virtual IP Interface	N
6	X	N
7	PPP over Ethernet (PPPoE)	Y
8	Solution using new 3GPP specific LLC/SNAP header settings	User plane only
9	EAP based signalling solution	N
10	WCS Solution	Y
11	Two scenario approach using DHCPv4 and Stateless DHCPv6 as control-plane and a TWAG VMAC user-plane	Y

9 Conclusion

Editor's note: This clause will provide conclusions with respect to what further specification work is required in order to provide the feature of S2a mobility based on GTP and WLAN access to EPC.

9.1 Conclusion on SaMOG Phase 1

For the support of SaMOG without UE impact, it has been concluded that Solution 2 (described in clause 7.1.2) is selected as the basis for normative specifications:

- The style of the reference model and call flows of Solution 1 (described in clause 7.1.1.1, 7.1.1.2 and 7.1.1.3) will be used for documentation of the normative specification, i.e., the internal structure of the WLAN Access Network will not be exposed.

- The L2 attach/detach triggers for solution 2 (described in clause 7.1.2.4) will be used in the work of normative specifications. Only L2 attach triggers are used for PDN type IPv6 and IPv4v6; L2 or L3 attach triggers may be used for PDN type IPv4 as described in clause 9.1.1.

- Enhancements on STa reference point in clause 7.1.1.1 will be used in the work of normative specifications.

- Simultaneous access for a UE to EPC through S2a and non-seamless offload using a single SSID is not supported. For a network deployment, behaviour described in clause 7.1.1.4 will be used in the work of normative specifications.
- Whether multiple TNAN functions are mapped to a single non-3GPP access entity, or a single TNAN function is distributed among multiple non-3GPP access entities is out-of-scope of 3GPP.

9.1.1 Conclusion on attach trigger solution

Two solutions are proposed in chapter 7.1. The main difference between the two solutions is how the TNSP/TWAG is triggered to setup the S2a tunnel towards the PGW. For the support of SaMOG without UE impact, it has been concluded that:

After the successful authentication, the AAA in the TNAN (TNAP/TWAP) knows from the UE profile the PDN type for the default APN. There are two possibilities:

1. PDN type = IPv6 or IPv4v6. In that case, TNAP/TWAP shall send a trigger signal to the TNSP/TWAG. TNSP/TWAG establishes the S2a tunnel.
2. PDN type = IPv4. In that case, S2a tunnel setup by the TNSP/TWAG is triggered either by a signal from the TNAP/TWAP, or by a L3 trigger from the UE. A trigger from the TNAP/TWAP is the recommended way.

In all cases, there shall be no difference on Sta and S2a signalling.

NOTE: That this conclusion applies even though the call flows in clause 7.1 have not been updated to reflect this conclusion.

9.2 Conclusion on SaMOG Phase 2

9.2.1 Partial conclusions

It has been agreed that the usage of SNAP/LLC for the user plane and the usage of DHCP (as described in solution 2) for the control plane are excluded from the evaluation phase and will not be further progressed.

9.2.2 Final conclusions

9.2.2.1 Support of single-PDN and multi-PDN UEs

The SaMOG phase-2 solution shall support *single-PDN* and *multi-PDN* UEs. The *single-PDN* UEs support only NSWO or a single PDN connection (with IP address preservation) over a trusted WLAN and the *multi-PDN* UEs support multiple simultaneous PDN connections over a trusted WLAN, in parallel to NSWO.

The *single-PDN* UEs trigger NSWO or PDN connection establishment (for handover or initial attach) during the authentication procedure. Such UEs do not require additional protocols for NSWO or PDN connection establishment and therefore are expected to require minimum development effort.

The *multi-PDN* UEs use a specific protocol (specified in clause 9.2.3) after the authentication procedure to trigger PDN connection establishment, over a multi-PDN capable network. Therefore, such UEs are required to support additional protocols for PDN connection establishment over trusted WLANs.

A *multi-PDN* UE may or may not be able to operate as a *single-PDN* UE.

When a *multi-PDN* UE connects to a *single-PDN* capable network, then:

- The UE operates as a *single*-PDN UE, if the single-PDN functionality is supported by the UE; otherwise
- The operation is based on the SaMOG phase-1 solution.

Multi-PDN UEs and *single-PDN* UEs shall both be supported in Rel-12.

9.2.2.2 User-plane conclusion

Both *single-PDN* and *multi-PDN* UEs shall use the virtual MAC (VMAC) solution on the user plane, as specified in clause 8.2.2.1.1.2.

9.2.2.3 Control-plane conclusion

Multi-PDN UEs shall use the WLAN Control Protocol (WLCP) on the control plane, as specified in clause 8.2.1.1.3.2 (Solution 1) with the following clarifications:

- Whether WLCP messages are transported directly over IEEE 802.11/802.3 frames or UDP datagrams will be specified during the normative phase of the work.
- WLCP protocol is expected to be defined as a new 3GPP protocol described in stage 3 specification, using some TS 24.008 Session Management messages for establishing and releasing PDN Connections as a baseline.

Single-PDN UEs do not use the WLAN Control Protocol (WLCP) or any other control plane protocol. These UEs trigger NSWO or PDN connection establishment during the EAP-AKA/EAP-AKA' authentication.

Annex A:
Example of WLAN integrated with Femto

For the Femto, the network will perform authentication and integrity checking through AAA before the femto can be connect to the EPC. In addition, the IPSec function in Femto can be used to build a secure transmission tunnel through the backhaul to the EPC. Therefore, the WLAN module integrated with the Femto box can leverage the authentication, integrity checking and the IPSec function to build a trusted WLAN access for connectivity to the EPC.

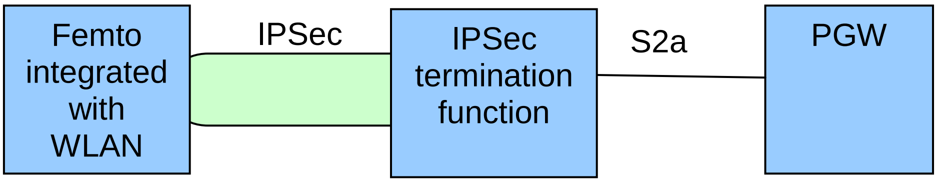


Figure A-1: WLAN integrated with Femto accessing EPC through S2a

Editor's note: Figure A-1 is illustrative and does not imply the location of the non-3GPP GTP peer.

Annex B:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2011-04	SA2#84				Initial draft		0.0.0
2011-04	SA2#84				Inclusion of P-CRs approved during SA2#84: S2-111940, S2-111941, S2-112138, S2-111943	0.0.0	0.1.0
2011-05					Add the TR number (Rapporteur)	0.1.0	0.1.1
2011-05	SA2#85				Inclusion of P-CRs approved during SA2#85: S2-112731, S2-112733, S2-112836, S2-112837, S2-112905, S2-112906, S2-112907, S2-112908	0.1.1	0.2.0
2011-07	SA2#86				Inclusion of P-CRs approved during SA2#86: S2-113828, S2-113829, S2-113779	0.2.0	0.3.0
2011-10	SA2#87				Inclusion of P-CRs approved during SA2#87: S2-114542, S2-114543, S2-114697, S2-114648, S2-114681, S2-114682, S2-114683, S2-114626	0.3.0	0.4.0
2011-11	SA2#88				Inclusion of P-CRs approved during SA2#88: S2-114800, S2-114857, S2-114987, S2-115319, S2-115332, S2-115361, S2-115364, S2-115433, S2-115434, S2-115456	0.4.0	0.5.0
2011-12	SP#54	SP-110758	-	-	MCC Update to version 1.0.0 for presentation to TSG SA for information	0.5.0	1.0.0
2012-05	SA2#91				Inclusion of P-CRs approved during SA2#91: S2-122490, S2-122491	1.0.0	1.1.0
2012-07	SA2#92				Inclusion of P-CRs approved during SA2#92: S2-123190, S2-123191, S2-123193, S2-123194, S2-123195, S2-123196, S2-123365,	1.1.0	1.2.0
2012-12	SA2#94				Inclusion of P-CRs approved during SA2#94: S2-124845, S2-124768, S2-124846, S2-124770, S2-124771, S2-124772, S2-124847	1.2.0	1.3.0
2013-02	SA2#95				Inclusion of P-CRs approved during SA2#95: S2-130562, S2-130675, S2-130565, S2-130677, S2-130566, S2-130625, S2-130624	1.3.0	1.4.0
2013-04	SA2#96				Inclusion of P-CRs approved during SA2#96: S2-131316, S2-131317, S2-131446, S2-131254, S2-131319, S2-131447, S2-131448	1.4.0	1.5.0
2013-06	SA2#97				Inclusion of P-CRs approved during SA2#96: S2-131752, S2-132042, S2-132280 including the partial conclusion thatwas capturedfor Rel12 SaMOG study phase	1.5.0	1.6.0
2013-07	-	-			MCC clean-up	1.6.0	1.6.1
2013-07	SA2#98				Inclusion of P-CR approved during SA2#98: S2-132951 that captures the "final" conclusion for Rel12 SaMOG study phase	1.6.1	1.7.0
2013-08	SA2#98				Clean up the TR to prepare for SA#61 approval (including Adrian's comments)	1.7.0	1.7.1
2013-09	SP#61	SP-130388	-	-	MCC Update to version 2.0.0 for presentation to TSG SA for approval	1.7.1	2.0.0