ETSI TS 123 234 V12.0.0 (2014-09)

Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP system to Wireless Local Area Network (WLAN) interworking;
System description
(3GPP TS 23.234 version 12.0.0 Release 12)

Reference
RTS/TSGS-0223234vc00

Keywords
LTE,UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

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

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

This document specifies system description for interworking between 3GPP systems and Wireless Local Area Networks (WLANs). This specification is not limited to WLAN technologies. It is also valid for other IP based Access Networks that support the same capabilities towards the interworking system as WLAN does. The intent of 3GPP–WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. The 3GPP–WLAN Interworking System provides bearer services allowing a 3GPP subscriber to use a WLAN to access 3GPP PS based services.

This specification defines a 3GPP system architecture and procedures to do the following:

- Provide Access, Authentication and Authorisation (AAA) services to the 3GPP-WLAN Interworking System based on subscription.
- Provide access to the locally connected IP network (e.g. the Internet) if allowed by subscription.
- Provide WLAN UEs with IP bearer capability to the operator's network and PS Services, if allowed by subscription.
- Provide WLAN UEs with IP bearer capability to access IMS Emergency calls for both UICC and UICC-less cases.

The interworking between 3GPP systems and Wireless Local Area Networks (WLANs) functionality in this specification is replaced by the functionality in 3GPP TS 23.402 [40].

No further changes to this specification are intended. If any future evolution of the procedures in this specification is necessary, it should be documented in other specifications.

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] void.

[2] void.

[3] void.

[4] void.

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.040: "Technical Realisation of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "GPRS; Service description".

[8] void.

[9] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[10] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[11] void.

[12] void.

[13] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[14] 3GPP TS 33.234: "WLAN Interworking Security".

[15] 3GPP TS 23.125: "Overall High Level Functionality and Architecture Impacts of Flow Based Charging".

[16] void.

[17] IETF RFC 4282: "The Network Access Identifier".

[18] void.

[19] IEEE Std 802.1X-2001: "IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control".

[20] IETF RFC 4284: "Identity Selection Hints for the Extensible Authentication Protocol (EAP)".

[21] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.

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

[23] IETF RFC 4186: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)".

[24] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".

[25] 3GPP TS 22.234: "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[26] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".

[27] 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces".

[28] 3GPP TS 29.060: "GPRS; GTP across the Gn and Gp interface".

[29] 3GPP TS 23.008: "Organization of subscriber data".

[30] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[31] 3GPP TS 23.002: "Network architecture".

[32] IETF RFC 4739: " Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[33] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture ".

[34] IEEE 802.1D, 1998 Edition (ISO/IEC 15802-3:1998): "IEEE Standard for Information technology--Telecommunications and information exchange between systems--IEEE standard for local and metropolitan area networks--Common specifications--Media access control (MAC) Bridges".

[35] IEEE 802.11e: "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 - Amendment: Medium Access Method (MAC) Quality of Service Enhancements".

[36] 3GPP TS 23.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture".

[37] IETF RFC 2475: "An Architecture for Differentiated Services".

[38] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[39] 3GPP TS 23.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Support of SMS and MMS over generic 3GPP IP access".

[40] 3GPP TS 23.402: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP access".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions defined in TR 21.905 [30] and the following apply:

Available SSID: An SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

3GPP WLAN QoS profile: 3GPP defined QoS profile for I-WLAN access.

Differentiated Services Field (DS Field): The IPv4 header TOS octet or the IPv6 Traffic Class octet when interpreted in conformance with the definition given in IETF RFC 2474 [38].

External AAA Server: The AAA Server is located in the external packet data networks. The PDG interworks with the External AAA Server via the Wi reference point.

External IP Network/External Packet Data Network: An IP or Packet Data network with access provided by the 3GPP – WLAN Interworking, rather than directly from the WLAN AN.

Home WLAN: A WLAN which interworks with the HPLMN without using a VPLMN.

Interworking WLAN (I-WLAN): A WLAN that interworks with a 3GPP system.

I-WLAN selection: Procedure to select a specific I-WLAN from the available I-WLANs.

Local Service Identifier: An identifier used within the 3GPP system for a service available directly from the I-WLAN, for example Internet access or access to a specific corporate network.

Offline charging: Mechanism for collecting and forwarding charging information concerning I-WLAN and core network resource usage without affecting the service rendered in real-time.

Online charging: Mechanism for collecting and forwarding charging information concerning I-WLAN and core network resource usage where the service may be affected in real-time.

Policy Enforcement: Functionality implemented in a WAG to ensure packets coming from or going to the WLAN AN are allowed based on unencrypted data within the packets. (e.g. source and destination IP address and port number).

Private network access from WLAN 3GPP IP Access: UE access to an external IP network via a PLMN via a tunnel. This is one of the WLAN 3GPP IP access. While the WLAN 3GPP IP access only performs user authentication and authorization with 3GPP AAA server, this access performs authentication and authorization with external server via PDG in addition to the authentication and authorization with 3GPP AAA server.

PS based services: General term to refer to the services provided by a PLMN using the IP bearer capability between a WLAN UEs and the PLMN when WLAN 3GPP IP Access is used. Examples include bearer services such as Internet access, and Corporate IP network access and higher level services such as SMS and LCS.

Requested W-APN: The W-APN requested by the user.

Routing Enforcement: Routing Enforcement ensures **all** packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the WLAN -UE subscriber request.

Service Authorization: Authorization allowing a subscriber to access the requested service based on subscription.

Tunnel Identifier: Identifier of a tunnel between a WLAN UE and a PDG. It is contained in the unencrypted part of a packet.

User Identifier: Identifier of a user which may be used, for example, in charging functionality.

WLAN Access Point Name (W-APN): Is used to identify a specific IP network and a point of interconnection to that network (Packet Data Gateway).

WLAN 3GPP IP Access: Access to an IP network via a PLMN via a tunnel. A related term is WLAN Direct IP Access.

WLAN coverage: The area where a WLAN UE can connect to a WLAN.

WLAN Direct IP Access: Access to an IP network directly from a WLAN AN without passing data to a PLMN via a tunnel. A related term is WLAN 3GPP IP Access.

WLAN UE's local IP address: The address used to deliver a packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. The WLAN UE's local IP address may be translated by a Network Address Translation prior to being received by any other IP network, including a PLMN.

WLAN UE's remote IP address: The address used by the data packet encapsulated inside the WLAN UE to PDG tunnel. It represents the address of the WLAN UE in the network which the WLAN UE is accessing via the PDG.

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Dw	Reference point between a 3GPP AAA Server and an SLF
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between an Offline Charging System and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Server/Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server or 3GPP AAA proxy
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Ww	Reference point between a WLAN UE and a WLAN Access Network
Wx	Reference point between an HSS and a 3GPP AAA Server
Wy	Reference point between a PDG and an OCS
Wz	Reference point between a PDG and an Offline Charging System

3.3 Abbreviations

AAA	Authentication, Authorisation and Accounting
ACL	Access Control List
AKA	Authentication and Key Agreement

AP	Access Point
APN	Access Point Name
CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	DiffServ Code Point
EAP	Extensible Authentication Protocol
FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IP-SM-GW	IP Short Message Gateway
ISP	Internet Service Provider
I-WLAN	Interworking WLAN
NAI	Network Access Identifier
NAT	Network Address Translation
OCS	Online Charging System
PDA	Personal Digital Assistant
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
SIM	Subscriber Identity Module
SSID	Service Set IDentifier
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	UMTS SIM
SSID	Service Set IDentifier
VLAN	Virtual Local Area Network
VPLMN	Visited PLMN
WAG	WLAN Access Gateway
W-APN	WLAN APN
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WLAN UE	WLAN User Equipment
WMM	Wi-Fi™ Multimedia

4 WLAN Radio networks interworking with 3GPP

This specification defines two new procedures in the 3GPP System:

- WLAN Access, Authentication and Authorisation, which provides for access to the WLAN and the locally connected IP network (e.g. Internet) to be authenticated and authorised through the 3GPP System. Access to a locally connected IP network from the WLAN, is referred to as WLAN Direct IP Access.

- WLAN 3GPP IP Access, which allows WLAN UEs to establish connectivity with External IP networks, such as 3G operator networks, corporate Intranets or the Internet via the 3GPP system.

WLAN 3GPP IP Access should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, WLAN 3GPP IP Access to External IP Networks from 3GPP–WLAN Interworking Systems shall be possible only if WLAN Access Authentication/Authorisation has been completed first.

NOTE: The independence requirement does not preclude the possibility that the procedure WLAN GPP IP Access may rely on information derived in the procedure for WLAN Access Authorization.

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking.

The Packet Data Gateway supports WLAN 3GPP IP Access to External IP networks. The WLAN includes WLAN access points and intermediate AAA elements. It may additionally include other devices such as routers. The WLAN

User Equipment (WLAN UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.

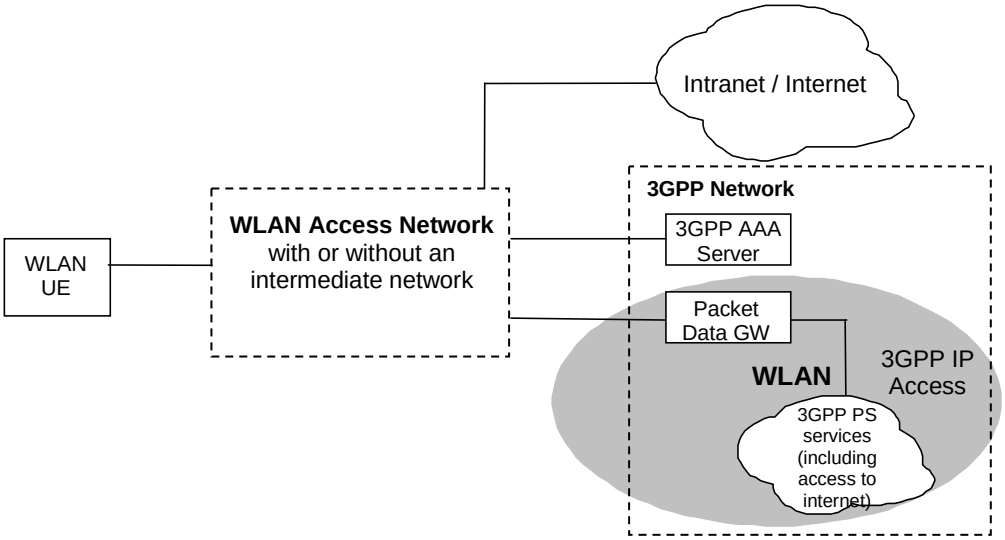


Figure 4.1: Simplified WLAN Network Model. The shaded area refers to WLAN 3GPP IP Access functionality

As 3GPP-WLAN interworking concentrates on the interfaces between 3GPP elements and the interface between the 3GPP system and the WLAN, the internal operation of the WLAN is only considered in order to assess the impact of architecture options/requirements on the WLAN.

3GPP-WLAN interworking shall be independent of the underlying WLAN Radio Technology.

5 High-level Requirements and Principles

5.1 Access Control

Access Control is the capability to permit or deny a subscriber the use of a resource, in this case the WLAN and/or the interworking to the 3GPP system. The following functional requirements and principles have guided the development of this standard with regard to Access Control.

5.1.1 WLAN Impacts

The following requirements should be satisfied by the WLAN 3GPP Interworking function with regard to the WLAN itself:

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. to access a (U)SIM.
- Existing client hardware and software should be used where ever possible
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain WLAN UE software shall be minimized.
- Methods for key distribution to the WLAN access network to allow secure tunnels to be established shall be supported. Note: This does not mean Wireless Equivalent Privacy (WEP) keys in the case of a 802.11 network.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It may take into account the user's subscription profile and optionally information about the WLAN AN, such as WLAN AN operator name, WLAN AN location information (e.g., country, telephone area code, city), WLAN AN throughput (e.g., maximum and minimum bandwidth guarantees for both ingress and egress traffic).

- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- It shall be possible to indicate to the user of the results of authorization requests.
- The WLAN Access Authorization mechanism shall be able change service provisioning dynamically, and inform the user and WLAN of any change.
- **Transporting Authentication signalling over WLAN Radio Interface:** WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.
- **Transporting Authentication signalling between WLAN AN and 3GPP network**: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network.
- Changes to the WLAN required to support IMS Emergency Calls should be supported, although these changes are to be minimized.

5.1.2 Existing 3GPP Element Impacts

The following requirements should be satisfied by the 3GPP-WLAN Interworking System function with regard to existing 3GPP network elements:

- Existing SIM and USIM shall be supported. Authentication shall rely on (U)SIM based authentication mechanisms. R6 USIM may include new functionality if necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- The Service Location Function (SLF) node shall be used in the same way as defined in TS 23.228 [24] to find the address of a subscriber's HSS, if necessary.
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber. (e.g. the HLRSS shall not deregister a PS subscriber when the UE registers on a WLAN)
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.
- IMS Emergency Calls over I-WLAN shall be supported in this release. This includes also the case of UICC-less UE.

5.1.3 Requirements for WLAN Direct IP Access

The following requirements should be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to allowing direct access to the IP network to which the WLAN is connected (e.g. the Internet):

- A WLAN supporting both WLAN Direct IP Access and WLAN 3GPP IP Access shall be able to support a WLAN UE operating in the WLAN Direct IP Access mode only, e.g. according to subscription.

5.1.4 Requirements for WLAN 3GPP IP Access

The following requirements should be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to allowing access to a WLAN 3GPP IP network (e.g. the operator's intranet which allows IMS access):

- Service Authorization for 3GPP services shall occur after successful Authentication.
- It shall be possible to use Service Based Policy Control.

- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall provide IP connectivity to be able to support all 3GPP PS based services. 3GPP PS based services which use more than IP connectivity (e.g. SMS, MMS, MBMS) could require additional entities and interfaces not specified in this document. Depending on operator's policy, it shall also be possible to access 3GPP PS based services via the Internet (noting that the access to the Internet in this case may or may not be via WLAN Direct IP Access).

- Quality of Service shall be supported when accessing these services via WLAN, although some limitations may exist because of the WLAN AN.

- A combined access capable user with the subscription for both services should be able to choose between "WLAN Direct IP Access only" or "WLAN 3GPP IP Access".

  The WLAN UE shall be able to detect if a 3GPP–WLAN does not support access to 3GPP PS based services.

- Data flows must be able to be routed to the HPLMN or the VPLMN, e.g. according to subscription. The enforcement of this routing shall not rely on the WLAN UE client.

NOTE: This routing enforcement may require additional functionality in the WLAN AN

- **End to End Authentication:** WLAN Authentication signalling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network. Details of End-to-End Authentication is covered in TS 33.234 [14].

- **Service Selection and Authorisation:** The solution shall include means for securely delivering service selection information from the WLAN UE to the 3GPP AAA Server in the Home Network. If a user chooses to access the Internet directly using the local IP network, no service selection information is passed to the PLMN. In all other cases, where WLAN 3GPP IP Access is desired, the service selection information shall contain the name of the W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the users subscription to the indicated W-APN against the subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.

- The service request shall be indicated by a tunnel establishment request from the WLAN UE to the PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.

- The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.

- In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

5.1.4.1 Requirement for private network access from WLAN 3GPP IP Access

The following requirements should be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to allowing private network access from WLAN 3GPP IP Access:

- Confidentiality of ID and password used for authentication and authorization by PDN service provider shall be possible.

- It shall be possible that PAP and CHAP capability with existing RADIUS protocol between PDG and external RADIUS server in PDN is utilized.

- Duration of tunnelling establishment should be as short as possible.

- Impact to UE or PDG should be as less as possible.

5.1.4.2 Requirements for Support of IMS Emergency Calls

The following requirements shall be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to support for IMS Emergency Calls:

- **Service Selection and Authorisation:** The WLAN UE shall be able to ask for IMS Emergency Call Service in tunnel establishment via an IMS Emergency Call specific W-APN for this purpose. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.

No service subscription shall be necessary for the user to gain access to the IMS Emergency Call W-APN i.e. the 3GPP AAA Server in the Home network does not need to verify the users subscription to the indicated W-APN against the subscriber profile retrieved from HSS.

- **End to End Authentication**: Based on the national regulations and operator's policy, WLAN Authentication signalling between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network may be skipped. Details of End-to-End Authentication are covered in TS 33.234 [14].

  For the UICC-less case, it shall be possible to either (i) Skip authentication or (ii) use a dummy or null authentication method.

- The results of the authorisation decision shall be communicated to the VPLMN and the WLAN AN.

5.1.5 WLAN Access Authorization

WLAN Access Authorization defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the stage after access authentication, but before service authorisation and WLAN UE's local IP address allocation.

After the authentication process succeeds, there could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied. These conditions may be based on the subscriber's profile, the account status, O&M rules, local agreements or information about the WLAN AN.

The procedure for WLAN Access Authorization between the WLAN UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

Access rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and in other entities such as the WAG or the WLAN AN.

Access rules/policy may include access scope limitation, time limitation, bandwidth control values, and/or user priority.

WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules.

The access scope limitation could be, for example, only/not/may "access through WAG"; only/not/may "access intranet X".

Access scope limitation can be achieved using IP allocation scheme, VLAN allocation, Filtering, ACLs in the routers and switchers, or other methods.

Different access priority or the range of priorities may be authorized for different subscribers, and/or for one subscriber based on different access time or location, etc.

The UE should be able to indicate in the access authorization procedure that the user is connecting in order to make an IMS Emergency Call. The 3GPP AAA Server shall in that case be able to deploy access/rules and policy to restrict the user to only that service.

5.1.6 3GPP WLAN Attach

3GPP WLAN attach status indicates whether the WLAN UE is now being served by the 3GPP–WLAN Interworking System.

A WLAN UE is "WLAN-attached" after successful authentication and WLAN Access Authorization.

A WLAN UE is "WLAN-detached" in 3GPP network after its disconnection, or its authentication or WLAN Access Authorization being cancelled.

The WLAN-attach status is maintained by the 3GPP AAA Server.

The WLAN UE's WLAN attach status should be obtained from the 3GPP AAA Server directly or through the HSS, by other entities in the 3GPP or 3GPP connected network. Other entities in the 3GPP network obtain the WLAN

UE's WLAN-attach status directly from the 3GPP AAA Server or through the HSS. These entities and the corresponding reference points are not in the scope of this TS.

The description of the corresponding status in the WLAN UE is out of the scope of this TS.

5.2 Void

5.3 User Identity

5.3.1 General

The network authentication procedure is based on the use of EAP method where user identification is based on Network Access Identifier (NAI), whose format is specified in RFC 2486 [17]. A NAI is composed of a username part and a realm part. In the following, the term of 'identity' includes both the NAI username part and the realm part, while the term of 'username' only refers to the NAI username part.

5.3.2 NAI Username

The NAI username part format shall comply with IETF EAP-SIM [23] and EAP-AKA [22]. Three types of usernames are:

1. a Permanent username;
2. a Pseudonym username;
3. a Fast re-authentication username.

Both of the Pseudonym and the Fast re-authentication usernames are used in temporary identities, but the purpose and usage of them are different. The first two types of usernames are only used on full authentication and the last one only on fast re-authentication.

The Permanent username, which is specified in IETF EAP-SIM [23] and EAP-AKA [22], shall be derived from IMSI, which resides in the UICC. Details of these are covered in TS 33.234 [14], TS 24.234 [9] and TS 23.003 [5]. For the case of UICC-less IMS Emergency Call, an identifier of the UE (e.g. IMEI) should be used as the permanent username.

NOTE: The permanent username is not used for authentication in case of UICC-less IMS emergency calls.

The Pseudonym username is used for user identity protection. The use of the Pseudonym username is necessary to replace the Permanent username derived from IMSI in radio transmissions, so that it protects the user against tracing from unauthorized access networks.

The Fast re-authentication username is used in fast re-authentication. It also provides user identity protection. For the fast re-authentication, a WLAN UE shall use the previously allocated Fast re-authentication identity as specified in the IETF EAP-SIM [23] and IETF EAP-AKA [22] RFCs.

Temporary identities (pseudonyms and fast re-authentication identities) are allocated by the 3GPP AAA Server. The format and the procedure for deriving the temporary identities are defined in TS 33.234 [14].

5.3.3 NAI Realm Name

The NAI realm name shall be in the form of an Internet domain name as specified in RFC 1035 and shall identify the user's HPLMN, based on its MCC and MNC. Details on NAI realm construction are specified in TS 23.003 [5].

5.3.4 NAI decoration for roaming

A roaming NAI is constructed when the WLAN UE authenticates through a VPLMN. The WLAN UE shall indicate in the NAI both the user's HPLMN and the chosen VPLMN, based on their MCC and MNC.

The details on Roaming NAI construction are specified in TS 23.003 [5].

5.3.5 NAI decoration for IMS Emergency Call Service

For IMS Emergency Calls, IMS Emergency Call Service specific realms within the PLMN shall be defined. When requesting an emergency service, realm should be decorated with this service part.

The details on IMS Emergency Call NAI construction are specified in TS 23.003 [5].

5.4 Network Advertisement and Selection

5.4.1 Description of the issue

If the WLAN radio technology allows for features enabling radio access network sharing or provider selection these shall be reused for WLAN Access Network (WLAN AN) selection in 3GPP-WLAN interworking.

In addition to WLAN Access Network selection, the WLAN UE may need to select a VPLMN through which to authenticate, if more than one is available through the chosen radio network.

A WLAN UE may need to select a PLMN within which IMS Emergency Calls are supported.

WLAN Access Network advertisement and selection depends on the particular WLAN technology.

VPLMN advertisement and selection should be independent of WLAN technology.

The generic Network Advertising and Selection scenario is illustrated in figures 5.1 and 5.2.

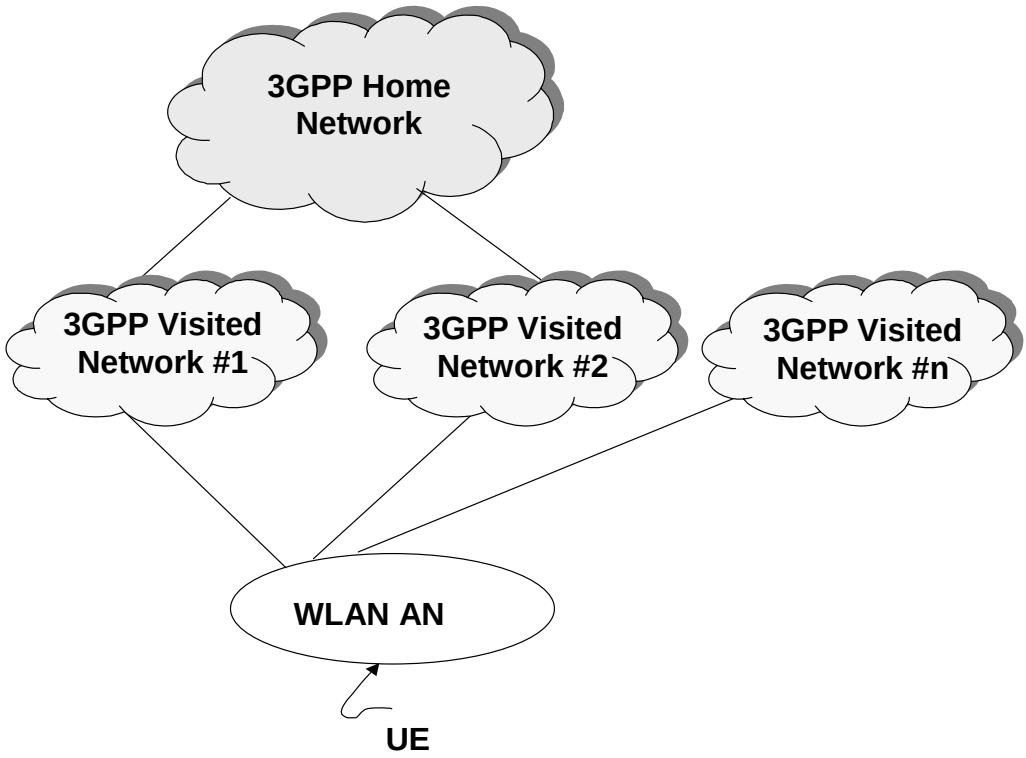


Figure 5.1: Network Advertising and Selection Scenario

An area is shown covered by a WLAN Access Networks having a set of roaming agreements with different 3G networks (3GPP Visited Network #1, #2,…, #n). A WLAN UE entering the WLAN AN wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in figure 5.1).

Referring to the figure the user subscribing to the services provided to the 3GPP Home Network can reach the associated home network in two different ways, e.g. via either of 3GPP Visited Network #1 or 3GPP Visited Network #2.

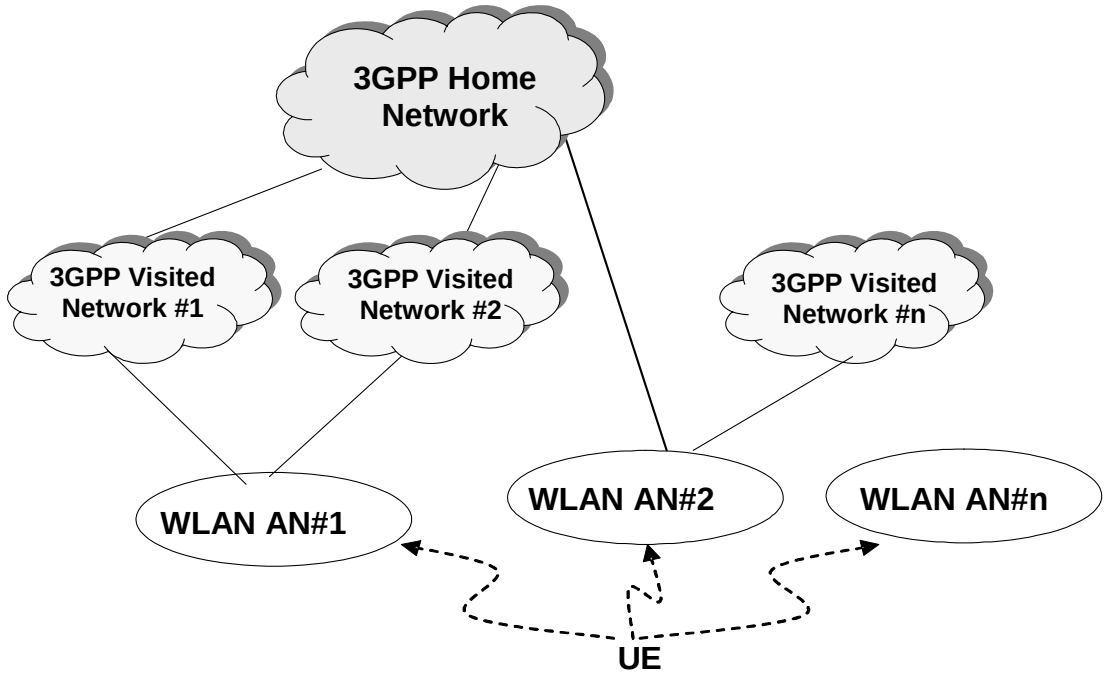


Figure 5.2: Network Advertising and Selection Scenario

Another scenario is represented by an area covered by some WLAN Access Networks (WLAN AN#1, #2, …, #n) having a set of roaming agreements with different 3G networks (3GPP Visited Network #1,#2,…,#n) and where one of the WLAN Access Network has a directly roaming agreement with the 3GPP Home network or the WLAN Access Network is directly deployed by the 3GPP Home network. A WLAN UE entering the area wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in figure 5.2).

Referring to the figure the user subscribing to the services provided to the 3GPP Home Network can reach the associated home network in three different ways, e.g. via WLAN AN#1 then through either of 3GPP Visited Network #1 or 3GPP Visited Network #2, or via WLAN AN#2.

5.4.2 I-WLAN Access Network Advertisement and Selection

5.4.2.1 Case of IEEE 802.11 WLANs

5.4.2.1.1 General

The following principles shall apply:

- Require no modifications of existing legacy APs.
- Have no impact on existing legacy clients (implies no modification of current broadcast SSIDs).
- Have low latency and overhead.
- The WLAN UE should be able to select the I-WLAN Access Network supporting the preferred PLMN.

In the case of IEEE 802.11 WLANs:

- Modification of current broadcast SSIDs shall not be required;
- Active scanning should be supported by the WLAN UE;
- Passive scanning shall be supported by the WLAN UE;

- Multiple SSIDs may be supported (i.e. only standard 802.11 capable APs are required).

5.4.2.1.2 WLAN Access Network Advertisement

A WLAN network name is provided in WLAN beacon signal in so-called SSID (Service Set ID) information element. There is also the possibility for a WLAN UE to actively solicit support for specific SSIDs by sending a probe request message and receive a reply if the access point does support the solicited SSID. Active and passing scanning are defined in IEEE 802.11 [21].

A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

The above requirement may be met through explicit EAP-based procedures or through the generic Preferred SSID list procedures - for example Preferred SSID lists could include SSID formats defined by operators for the above purposes.

For the case of EAP based procedures, WLAN should be able to indicate which PLMNs explicitly support IMS Emergency Call service (via service specific realms).

NOTE: The definition of the service specific realm for IMS emergence calls is FFS.

5.4.2.1.3 I-WLAN Access Network Selection

For purpose of selecting the preferred I-WLAN AN the WLAN UE may contain lists of I-WLAN identities' preferences. One list will contain the SSIDs preferred by the Home Network operator and one list contains the SSID's preferred by the user.

The Operator's preferred SSID list would be populated, for example, with the SSIDs commonly used by major hotspot operators with whom the Home Operator has a direct or indirect (through VPLMN in a roaming case) relationship.

There are two modes in network selection, i.e. Manual mode and automatic mode.

Manual mode

In the manual mode, the WLAN UE shall try to find all available SSIDs through passive scanning and/or active scanning (when it is supported).

Once a list of all available SSIDs has been obtained, it shall be possible for the WLAN UE to obtain a list of all available PLMNs from each SSID. When a list of PLMNs has been obtained from all SSIDs it shall present them to the user to select one. The WLAN UE shall then associate with the SSID that supports the PLMN that is selected by the user.

Automatic Mode

In the automatic mode the procedure is as follows:

0. The WLAN UE scans for all available SSID using passive scan and/or active scans. If the WLAN UE contains the I-WLAN identities' preference lists, the scan should be done in the order of these lists. It is not required to continue the scanning after the highest priority SSID is found.

1. Start association and perform Network Discovery. When there is more than one available SSID and the WLAN UE contains I-WLAN identities' preference lists, the association shall be done in the order of these lists.

   1a) If authentication to HPLMN succeeds (i.e. EAP-Success is received), then stop this procedure.

   1b) If Network Advertisement information [20] is received (i.e. EAP-Identity/Request is received), then store the list and start again step 1.

   Repeat step1 for all available SSIDs. If the scanning in step 0 was stopped due to the discovery of the highest priority SSID, but the HPLMN has not been found (e.g. because the SSID list is not updated or the selected SSID was a fake one), then the user should go back to step 0 and scan for all remaining SSIDs.

   Note that if an AP supporting HPLMN is found in the middle of the procedure, step 1a, then step 1 is stopped and association with the remaining available APs will not take place.

2. Use the lists of 'User Controlled PLMN Selector list for I-WLAN' and 'Operator Controlled PLMN Selector list for I-WLAN' and the lists from step 1b) to select the best matching PLMN. Note that the 'User Controlled PLMN Selector list for I-WLAN' has higher priority than the 'Operator Controlled PLMN Selector list for I-WLAN'. Then select the I-WLAN AN that supports the best match PLMN. If more than one I-WLAN AN supports the best matched PLMN, the I-WLAN AN having the highest priority SSID is selected, if 'I-WLAN identities' preference lists are available.

3. Associate with the AP selected in step 2 and attempt authentication with the best match PLMN. A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

If such an indication is provided by the WLAN AN and if the WLAN UE supports the indication, then the WLAN UE shall use it at SSID selection as defined in TS 24.234 [9].

The above requirement may be met through explicit EAP-based procedures or through the generic 'I-WLAN identities' preference lists procedures - for example I-WLAN identities preference lists could include SSID formats defined by operators for the above purposes.

NOTE: These selection procedures may have to be modified for the IMS Emergency Call case.

5.4.2.2 Case of other WLANs

Other Access Network Technologies are not described in this TS but not excluded.

5.4.3 PLMN Advertisement and Selection

5.4.3.1 General

The following principles shall be used in PLMN Advertisement and Selection:

- This procedure takes place after association with an AP
- The user shall be able to select the Visited Network
- Use the NAI for routing of AAA messages.
- Have low latency and overhead.
- Use existing EAP mechanisms, if possible.
- Be extensible to permit advertisement of WLAN characteristics other than the PLMNIDs of roaming partners.

5.4.3.2 Network Advertisement

Network advertisement information enumerates the roaming partners and associated NAI realms. This information shall be provided to the WLAN UE when the WLAN is unable to route an authentication request from the WLAN UE based on the initial NAI (e.g. when the WLAN AN receives a NAI with an unknown realm) and when the WLAN UE explicitly requests Network advertisement information. The network advertisement information is returned from the first hop AAA functionality. The first hop AAA functionality may be located either in the WLAN AN or in the PLMN in case no AAA functionality is in the WLAN AN. The provisioning of this AAA functionality is an implementation issue and does not put new requirements on 3GPP AAA Proxy/Server. Details on the usage and coding of Network advertisement information are included in TS 24.234 [9]. In order to support IMS Emergency Call service, this information shall contain an indicator showing those PLMNs that support IMS Emergency Call service.

5.4.3.3 Network Selection

The automatic and manual mode PLMN selection procedures are defined in TS 22.234 [25]. The detailed procedure in case of IEEE 802.11 WLAN is described in 5.4.2.

The WLAN UE shall indicate its home network through the use of an initial NAI. The realm part of this initial NAI shall be derived from the IMSI, as described in section 5.3.3. Optionally, if there is preference for a roaming network, the initial NAI then takes the form of a Roaming NAI, as described in section 5.3.4; e.g., for optimizing user access

experience in re-access case, the WLAN UE may include information of preferred roaming network from previous successful authentication while it is associated to the same AP. For IMS Emergency Call case, NAI shall be decorated as described in 5.3.5.

For the manual selection case allowed by some operator, initial NAI can include the roaming network decided by the user, e.g. using a preferred PLMN list stored in the UICC.

If the WLAN AN is able to route authentication request based on the initial NAI, then no special processing for network advertisement/selection is needed.

If the WLAN AN is unable to route authentication request from WLAN UE based on the initial NAI, the WLAN AN shall deliver the network advertisement information to the WLAN UE. The WLAN UE processes this information according to its internal roaming preference policies or prompts the user to select a VPLMN preference. It uses the result to determine how to construct a new NAI indicating the selected VPLMN, according to Section 5.4.2.

After the network advertisement information is delivered and VPLMN selection is performed, the WLAN UE attempts to authenticate with the new NAI determined in the prior step.

The WLAN AN shall use the NAI to route the AAA traffic to the appropriate VPLMN AAA Proxy.

5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [14].

5.6 Service Authorization Principles for WLAN 3GPP IP Access

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after successful authentication.
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the HPLMN.
- Service authorization information shall be protected.
- The Access Point Name (APN) concept defined in TS 23.003 [5] shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
    - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server based on the requested W-APN and subscription information retrieved from the HSS/HLR, which includes e.g. the subscribed W-APNs).
    - The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
    - The PDG selection shall be performed under control of the 3GPP Home Network by means of answers to DNS queries for the requested W-APN. The selection is based on the requested W-APN and user subscription information. The WLAN UE shall choose an IP address of the PDG, if there is more than one PDG address in the answer to the DNS queries.

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.

- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.
- For the case of IMS Emergency Calls, there shall be W-APN indicating the IMS Emergency Call service. No subscription is needed to access this service.

5.6.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- In order for the WLAN UE to be able to use W-APNs in the VPLMN, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.
- The V-PDG selection is shall be under control of the 3GPP Visited Network by means of answers to DNS query for the requested W-APN. The selection is based on the authorized W-APN and service related information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

  The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.
- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.
- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the VPLMN.

In the roaming case, IMS Emergency Calls shall be accessed in the VPLMN.

5.6.3 External IP Network selection

The WLAN UE can connect to different External IP networks, such as the Internet, an operator's IP network or a corporate IP network. The user may indicate a preferred IP network with a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN UE and a PDG. It is then forwarded to the 3GPP AAA server/proxy in the same network as the PDG.

5.7 IP Connectivity for WLAN 3GPP IP Access

5.7.1 Principles

The WLAN UE initiates the establishment of tunnels and is involved in packet encapsulation/decapsulation. The tunnel shall reside between the WLAN UE and the PDG. In the non roaming case, the PDG shall reside in the Home PLMN; in the roaming case, the PDG may reside either in the Home or in the Visited PLMN (both cases shall be supported).

The following steps are performed at tunnel establishment:

1. W-APN resolution and discovery of the tunnel endpoint (PDG) IP-address is performed using the procedures described in clause 7.9.
2. Tunnel establishment, including mutual authentication, shall occur between the WLAN UE and the PDG.

NOTE 1: Filtering attributes may be needed in order to enable the WLAN to enforce that the WLAN UE tunnels all traffic as required. Filtering attributes may be transmitted from 3GPP AAA Server to WLAN over the Wa reference point. The WLAN Access Network sets up appropriate packet filters.

NOTE 2: The PDG is described in section 6.

The tunnel establishment is not coupled to WLAN access authentication/authorisation. The WLAN UE may establish several tunnels in order to access several external IP networks simultaneously. The external IP network selection is performed as part of the establishment of each tunnel.

Editor's note: Routing towards the Home PLMN in the Visited PLMN, as well as its impacts on the WLAN AN, are for further study.

5.7.2 Tunnelling Requirements

The requirements that a WLAN UE-Initiated tunnelling protocol should meet are:

- Minimal requirements to the underlying IP connectivity network, i.e. WLAN UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks
- Minimal impacts to the WLAN Access Network
- Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible
- Tunnel IP configuration of the WLAN UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- Remote IP address (inner IP):
  - The transport of IPv4 packets shall be supported
  - The transport of IPv6 packets shall be supported (e.g. in order to support IPv6 services like IMS)
- Local IP address (outer IP):
  - The tunnel protocol shall be able to support IPv4 and IPv6 transport addresses
  - The tunnel protocol shall support private WLAN UE's local IP addresses, which are non-routable in the public Internet.
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

5.7.3 Void

5.8 Roaming requirements for WLAN 3GPP IP Access

For the delivery of 3GPP PS based services in a roaming scenario:

- The roaming architecture shall ensure that CDRs can be generated e.g. volume and time based by the visited network.
- The roaming architecture shall ensure that tunnels established are between entities that have a roaming agreement.
- The roaming architecture shall ensure that the bearer path from the WLAN to Home/Visited 3GPP network conforms to QoS and roaming agreement(s).
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. local PS services.
- The roaming architecture shall allow the home network to limit the set of 3GPP services available for a given roaming user.

- All packets of PS based services sent to/from a WLAN UE are routed via a VPLMN in a 3GPP network; however basic Internet access may be routed directly from the WLAN.

5.9 Routing Enforcement and Policy Enforcement for WLAN 3GPP IP Access

5.9.1 Purpose for routing enforcement and policy enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, WLAN 3GPP IP Access requires routing enforcement and policy enforcement to be implemented in the 3GPP–WLAN Interworking System.

5.9.2 Routing Enforcement in the WLAN AN

Routing enforcement shall be used to ensure that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent a WLAN AN from routing non 3G PS based service traffic to another network (e.g. the Internet) other than a PLMN, when provision of such services (e.g. direct Internet access from the WLAN) is agreed between the WLAN and the PLMN.

When subscription limits a WLAN UE to exclusively access only 3GPP PS based service, the PLMN can indicate to the WLAN AN routing enforcement to ensure that all packets sent to/from the WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case).

If a WLAN UE user subscription allows a WLAN Direct IP Access the WLAN AN should be capable of routing packets directly to the external packet data network.

Routing enforcement in the WLAN AN shall ensure that packets sent between a PDG and a WLAN UE are routed to the right entity in the interworking VPLMN (roaming case) or HPLMN (no roaming case).

Routing enforcement should not prevent the WLAN AN from supporting a WLAN Direct IP Access only capable WLAN UE or a WLAN 3GPP IP Access capable WLAN UE opting for a WLAN Direct IP Access, and non 3G interworking WLAN terminals. Routing enforcement should have minimal impact on the WLAN AN.

5.9.3 Routing enforcement and policy Enforcement in the HPLMN

When supporting WLAN 3GPP IP Access and access is via a tunnel endpoint (PDG) in the HPLMN, the HPLMN shall be able to provide the VPLMN with suitable policy enforcement information. The HPLMN may also provide suitable routing enforcement information to WLAN.

5.9.4 Routing enforcement and policy Enforcement in the VPLMN

When supporting WLAN 3GPP IP Access, the VPLMN shall be able to implement policy enforcement on traffic sent to/from a WLAN UE according to policy enforcement information provided by the HPLMN.

The VPLMN may also provide suitable routing enforcement information to WLAN.

5.10 IP address allocation for the WLAN UE

5.10.1 General

When using WLAN Direct IP Access, a WLAN UE needs to use its local IP address only. When using WLAN 3GPP IP Access, a WLAN UE shall use two IP addresses; its local IP address and remote IP address.

A WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In systems supporting only WLAN Direct IP Access, the WLAN UE's local IP address is assigned by the WLAN AN; in a WLAN 3GPP IP Access enabled system, it can be assigned by a WLAN or by a PLMN (a VPLMN in roaming case and a HPLMN in non-roaming case). For the WLAN-assigned local IP address, which belongs to the address space of WLAN AN, there is no additional requirement on the WLAN. WLAN UE's local IP address allocation by the PLMN is for further study.

When using WLAN 3GPP IP Access, a WLAN UE's remote IP address identifies the WLAN UE in the network that the WLAN UE is accessing for the 3G PS service. It shall be used for the inner packet of the WLAN UE-initiated tunnel. It can be assigned by HPLMN, VPLMN or an external IP network. The remote IP address can be statically or dynamically assigned. The only case where VPLMN assigns the remote IP address for the WLAN UE is when the WLAN UE-initiated tunnel terminates at the VPLMN's PDG. When the WLAN UE's remote IP address is allocated by the external IP network, the PDG is required to have an interface with an address allocation server, such as AAA or DHCP, belonging to the external IP network. For the WLAN UE's remote IP address, IPv4 addresses shall be supported. When the WLAN UE accesses 3G PS based services using an IPv6 network such as IMS services, IPv6 addresses shall be supported for the WLAN UE's remote IP address. To avoid any clashes between addresses used in WLAN AN and PLMN and to enable correct routing of packets sent out by the WLAN UE the PLMN operator should allocate public addresses to network nodes, which are addressed by WLAN UEs.

When a WLAN UE accesses several 3G PS based services with different W-APNs simultaneously, the WLAN UE can get several remote IP addresses. There may be several WLAN UE-initiated tunnels for the services.

5.10.2 Static and Dynamic Remote IP Address

Remote IP address can be allocated to a WLAN UE in four different ways:

- The HPLMN operator assigns a Remote IP address permanently to the WLAN UE (static remote IP address).
- The HPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the home network (dynamic HPLMN remote IP address).
- The VPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the visited network (dynamic VPLMN remote IP address).
- The external IP network operator assigns a permanent or dynamic Remote IP address to the WLAN UE (external Remote IP address allocation).

It is the HPLMN operator that defines in the subscription whether static IP address allocation is used.

When static IP address allocation is used, a WLAN UE either can include its static IP address in the tunnel setup request message, or indicate in the tunnel setup request message that the network should configure the static IP address of the WLAN UE or the network simply provides the static address to the WLAN UE.

5.11 Charging

The following functionality and requirements have been identified:

- The WLAN Access Network shall be able to report the WLAN access usage to the appropriate 3GPP system (i.e. VPLMN in the roaming case and HPLMN in the non-roaming case).
- It shall be possible for the 3GPP system to control a specific ongoing WLAN access session for online charging purposes.
- It shall be possible for an operator to maintain a single prepaid account for WLAN, PS, CS, and IMS for a user.
- The 3GPP system shall be able to process the WLAN access resource usage information, and convert it into the format used in 3GPP networks (e.g. CDR).
- It shall be possible to correlate charging and accounting records generated in WLAN Access related nodes and records generated in 3GPP nodes.
- It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

Additionally, for WLAN 3GPP IP Access:

- It shall be possible to generate per user charging information in the HPLMN and in the VPLMN irrespective of whether the service is provided in the HPLMN or in the VPLMN.
- WLAN Charging Information shall be collected for each WLAN UE by the WAG and the PDG that are serving the WLAN UE. The operator can control whether charging information shall be collected in the PDG on an

individual WLAN UE and/or W-APN context basis by appropriately setting the Subscribed Charging Characteristics and/or W-APN Charging Characteristics in the HSS. The Charging Characteristics on the WLAN subscription and individually subscribed W-APNs are specified in TS 32.252 [26].

5.12 AAA Protocol Requirements

- As far as possible, a common AAA protocol shall be used across all AAA interfaces. This may not be possible for the Wa and Wd interfaces when the WLAN AN is using a legacy AAA protocol.
- If protocol interworking is needed, then in the non-roaming case it shall be performed at the edge of the 3GPP network. For roaming, such interworking shall be performed either in the visited network or in the home network (dependent upon inter-operator roaming agreements).

5.13 QoS Support

5.13.1 General

The support of QoS mechanisms is an optional functionality of the 3GPP-WLAN Interworking architecture.

Figure 5.3 shows the considered QoS architecture for WLAN Direct IP Access.

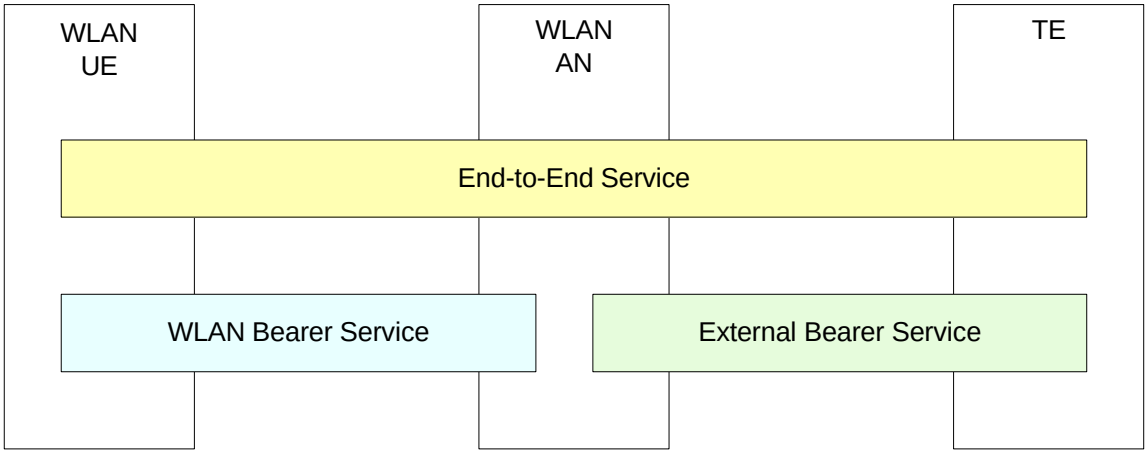


Figure 5.3: QoS Architecture for WLAN Direct IP Access

Figure 5.4 shows the considered QoS architecture for WLAN 3GPP IP Access.

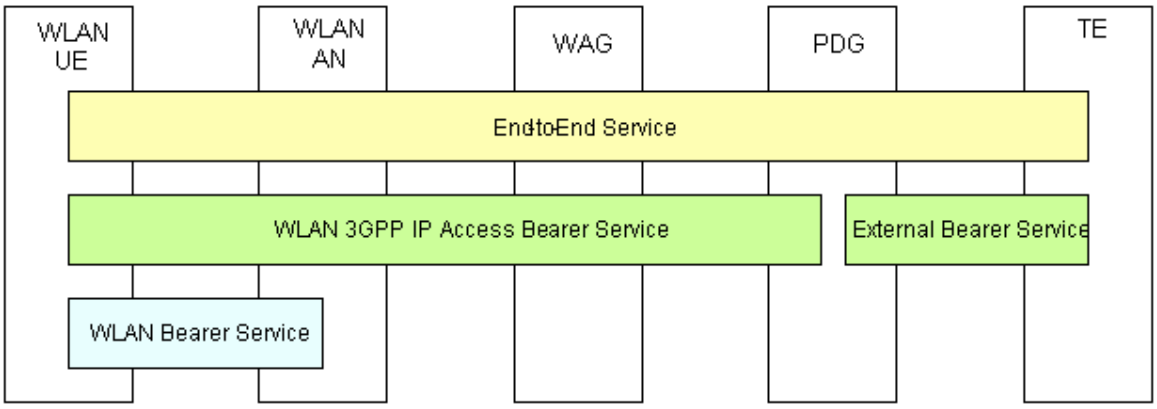


Figure 5.4: QoS Architecture for WLAN 3GPP IP Access

The End-to-End Service provides transport of the signalling and user data between the WLAN UE and another (external) TE (or correspondent node) passed over different bearer services of the network. In case of WLAN Direct IP Access, it consists of WLAN Bearer Service and External Bearer Service. In case of WLAN 3GPP IP Access, it consists of 3GPP IP Access Bearer Service and External Bearer Service.

The External Bearer Service is not further elaborated here as this bearer may be using several network services, e.g. another UMTS Bearer Service (TS 23.107 [33]). The 3GPP IP Access Bearer Service provides transport of signalling and user data between WLAN UE and PDG and supports QoS.

WLAN Bearer Service supports WLAN AN specific bearer capability between WLAN UE and WLAN AN.

5.13.2 Use of CoS based DiffServ for providing QoS over I-WLAN using WLAN 3GPP IP Access

When using 3GPP IP Access, a tunnel from UE to PDG is established for carrying PS based services traffic. This tunnel traverses over inter PLMN backbone (e.g. GRX) in the case of a roaming user. While accessing home network services, one or more tunnels will be setup that will carry traffic for all home network services that are being accessed irrespective of the level of QoS required for an individual service. It is possible that data for more than one IP flow and for different services is carried in one tunnel. Since the data within these tunnels (including the inside IP headers) is likely to be encrypted, it may not be possible to separate out individual IP flows and service traffic at intermediate nodes.

A possible way to provide QoS in such a situation is the use of DiffServ [37] by the WLAN UE and PDG to appropriately colour the DS Field in the external IP header based on the QoS required for the service that the individual packet belongs to DiffServ therefore allows to provide for different classes of traffic different levels of QoS. Such use of DiffServ mechanism works well with GSMA's specifications on GRX (IR 34).

5.13.3 QoS requirements on the architecture

The 3GPP WLAN QoS profile shall be WLAN technology independent.

The 3GPP AAA Server shall be the single point to authorize the 3GPP WLAN QoS profile for both WLAN direct IP Access and WLAN 3GPP IP Access.

The 3GPP WLAN QoS profile shall be specified within the subscriber data of the HSS (defined in TS 23.008 [29]).

Policy Control and Charging (PCC) functionality shall be used where applicable, in accordance with TS 23.203 [36].

A mechanism shall be defined, which allows that the WLAN AN's QoS capabilities (e.g. the supported 3GPP WLAN QoS profile) are provided by the WLAN AN to the 3GPP AAA Server during initial WLAN direct IP Access authorization.

The authorized 3GPP WLAN QoS profile shall be sent from the 3GPP AAA Server to the WLAN AN during WLAN 3GPP IP Access authorization and re-authorization.

A mechanism for change of authorized 3GPP WLAN QoS profile after initial authorization from 3GPP AAA Server/Proxy to WLAN AN and PDG shall be considered.

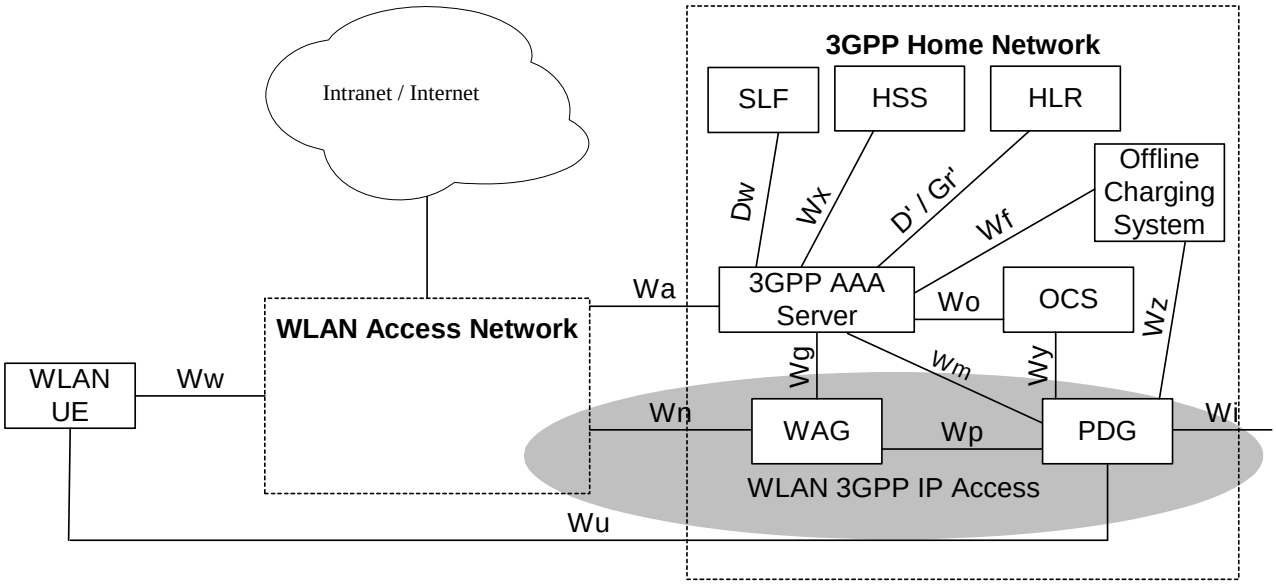
Charging signalling sent between WLAN AN and 3GPP AAA Proxy/Server shall contain information about the used 3GPP WLAN QoS profile.

6 Interworking Architecture

6.1 Reference Model

Editor's note: The term roaming is used here when referring to roaming between 3GPP networks. However, an intermediate aggregator or a chain of intermediate networks may possibly separate the user when accessing the WLAN from the 3GPP home network.

6.1.1 Non Roaming WLAN Inter-working Reference Model



NOTE: The shaded area refers to WLAN 3GPP IP Access functionality.

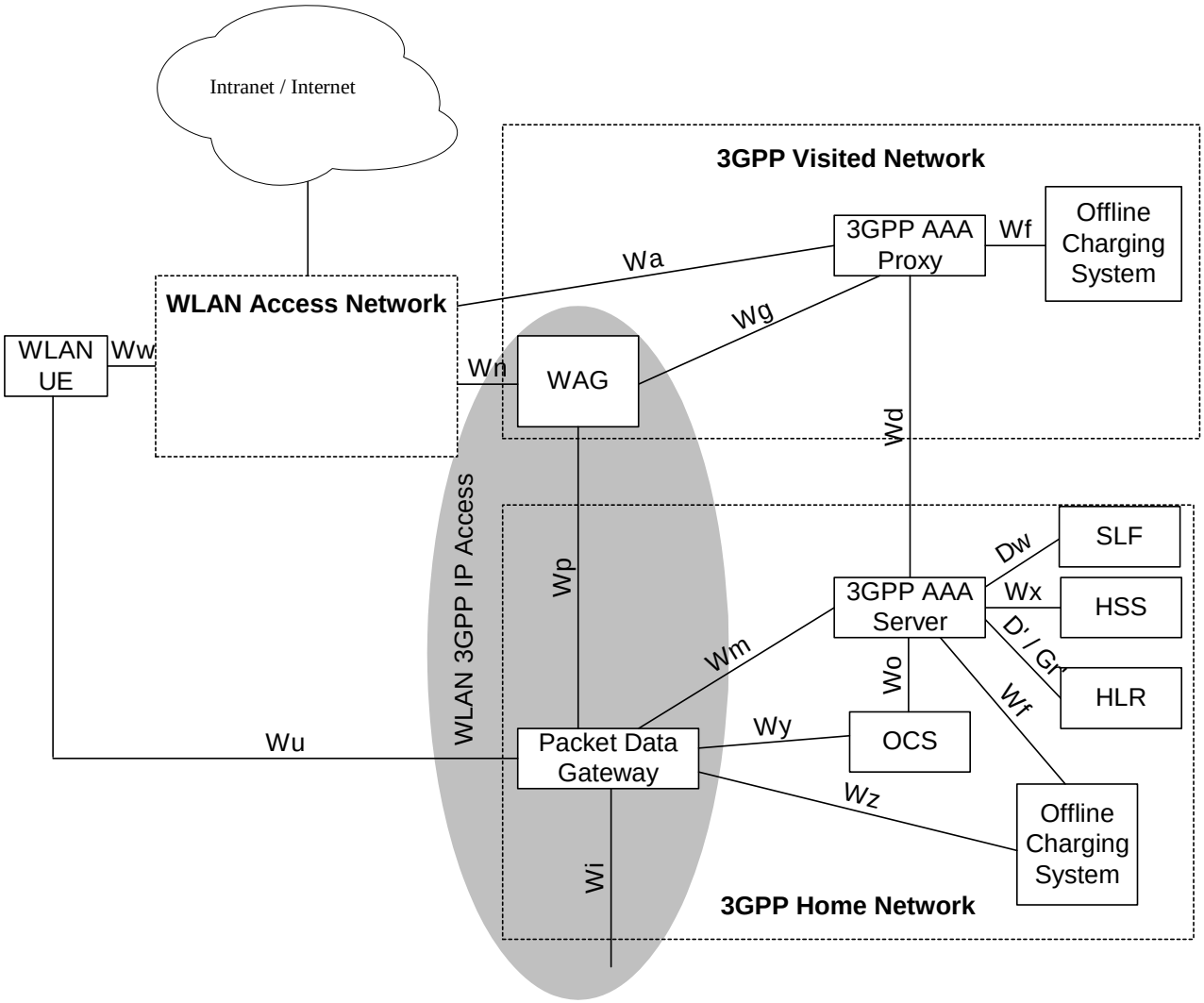
Figure 6.1: Non-roaming reference model

6.1.2 Roaming WLAN Inter-working Reference Model

The home network is responsible for access control. Charging records can be generated in the visited and/or the home 3GPP networks. The Wx and Wo reference points are intra-operator. The home 3GPP network interfaces to other 3GPP networks via the inter-operator Wd reference point.

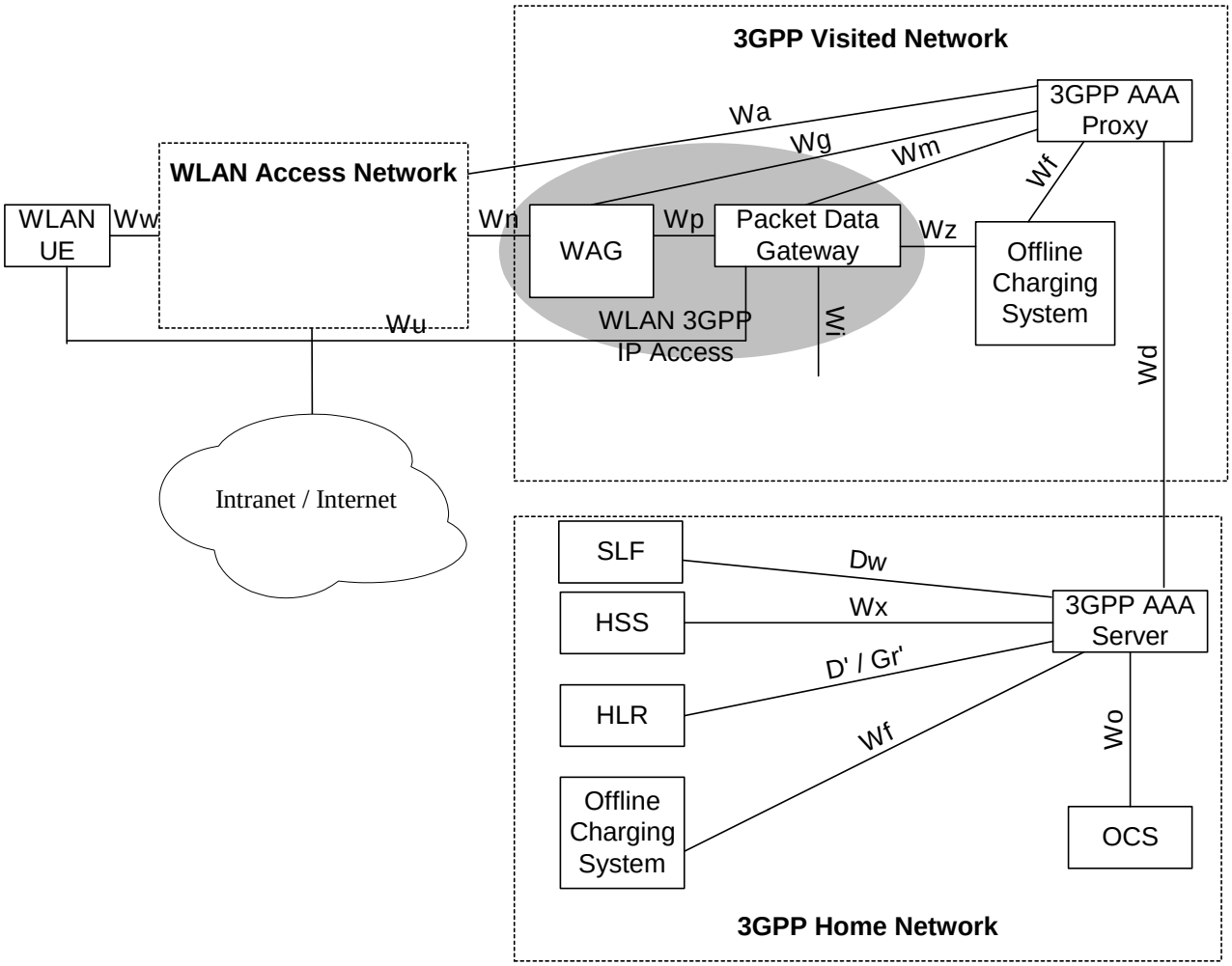
The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Wd reference point.

It can also issue charging records to the visited network Offline Charging System when required. The 3GPP network interfaces to WLAN Access Networks via the Wa reference point.



NOTE: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure 6.2a: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network



NOTE: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure 6.2b: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network

6.2 Network elements

6.2.1 WLAN UE

A WLAN UE is the User Equipment using a UICC card utilized by a 3GPP subscriber to access the WLAN AN for 3GPP interworking purpose. The WLAN UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP radio access. Some WLAN UE's may be capable of simultaneous access to both WLAN and 3GPP radio access. A WLAN UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

The WLAN UE functions include:

- Associating to an I-WLAN.
- WLAN access authentication based on EAP methods.
- Selection of a suitable VPLMN in the roaming case.
- Building an appropriate NAI.
- Obtain a local IP address. If the WLAN UE is intended for use with WLAN ANs supporting IPv4 only as well as with WLAN ANs supporting IPv6 only, it shall be equipped with a dual IP stack.

- If QoS mechanisms are applied: the UE applies DiffServ mechanisms by marking the DS field of IP packets according to the application QoS requirements (as recommended in Annex H);
- If QoS mechanisms are applied, the UE maps the DS field of IP packets into WLAN technology specific QoS parameters.

For WLAN 3GPP IP Access enabled WLAN UE:

- Building an appropriate W-APN to be used for External IP network selection.
- Request the resolution of a W-APN to a PDG address.
- If IPv4 and IPv6 addresses are returned during the resolution process, the WLAN UE shall select the address that has the same format as its own local IP address (IPv4 or IPv6).
- Establish a secure tunnel to a PDG.
- Obtain a remote IP address.
- Accessing services provided in the operators PS domain.
- Allowing users to select the type of network access, i.e. WLAN 3GPP IP Access or WLAN Direct IP Access.
- Ability to indicate whether multiple authentication is needed or not in the tunnel establishment procedure. This function is only required in case that the specified W-APN requires the authentication and authorization with the External AAA Server. Details on the multiple authentications are specified in RFC 4739 [32].

6.2.1.1 Void

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Providing access scope limitation information to the WLAN based on authorization information from the Home network
- Reporting per-user charging/accounting information to the VPLMN Offline Charging System for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For WLAN 3GPP IP Access only:

- Receiving per-tunnel charging information based on the tunnel identifier from the WAG and mapping of a user identifier and a tunnel identifier from the PDG; generating per user charging records for roaming users.
- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy
- Receiving the suitable policy enforcement information from AAA-Server and provides it to the WAG in VPLMN.
- May provide suitable routing enforcement information to WLAN AN.

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

6.2.3 3GPP AAA Server

The 3GPP AAA server is located within the 3GPP network. There should be only one 3GPP AAA Server for a WLAN attached subscriber. The 3GPP AAA Server:

- Retrieves authentication information and subscriber profile (including subscriber's authorization information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network.
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.
- Updates the WLAN access authorisation information when user's service subscription is modified when requested by HSS/HLR.
- Communicates (including updates) authorization information to the WLAN AN potentially via AAA proxies.
- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorized 3GPP subscriber.
- Initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.
- May act also as a AAA proxy (see above).
- Maintains the WLAN UE's WLAN-attach status.
- Provides the WLAN UE's WLAN-attach status to other entities (which are out of the scope of this TS).
- Generates and reports per-user charging/accounting information about WLAN Direct IP Access to the HPLMN Offline Charging System.
- Transfer a subscriber's authentication to a 3GPP AAA Server when it is requested by HSS/HLR.
- If QoS mechanisms are applied: the 3GPP AAA server authorizes and stores the 3GPP WLAN QoS profile. The authorized QoS profile is based on the closest match of subscriber's WLAN QoS profile with the WLAN AN capabilities/policies.

For WLAN 3GPP IP Access:

- Communicates (including updates) service authorization information (e.g. authorized W-APN, necessary keying material for tunnel establishment and user data traffics) to the PDG. AAA proxies if the PDG is located in VPLMN.
- Provides the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
- Provides the AAA-Proxy with suitable policy enforcement information.
- Provides suitable policy enforcement information to WAG in HPLMN.
- May provide suitable routing enforcement information to WLAN AN.
- If QoS mechanisms are applied: the 3GPP AAA server authorizes the 3GPP WLAN QoS profile for tunnels. The authorized QoS profile is based on the subscriber's WLAN QoS profile in the subscription information and stored 3GPP WLAN QoS profile for the WLAN Direct IP Access if WLAN Access Authentication and Authorization procedure has been performed.

6.2.4 HLR/HSS

The HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service. Besides other information, the HSS contains 3GPP WLAN QoS profiles' authentication and subscription data for the 3GPP subscriber.

The HSS also provides access to the WLAN UE's WLAN-attach status for other entities, e.g. answers or relays the WLAN-attach status query from other entities. To this end, the HSS shall store the IP address of the 3GPP AAA server to which the WLAN UE is registered.

When a 3GPP AAA Server other than the registered 3GPP AAA Server of a subscriber, requests authentication information or the profile of the subscriber, the HSS should request it transfer the authentication to the registered 3GPP AAA Server by providing the registered 3GPP AAA Server address to it.

6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to a WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway is a gateway via which the data to/from the WLAN Access Network shall be routed via a PLMN to provide a WLAN UE with 3G PS based services in a WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway shall reside in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case.

The WLAN Access Gateway:

- Allows VPLMN to generate charging information for users accessing via the WLAN AN in the roaming case.
- Enforces routing of packets through the PDG.
- Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements in case of the roaming scenario when the Wu reference point is between the WLAN UE and a PDG in the home network (figure 6.2a). The charging information is forwarded to the 3GPP AAA proxy in the visited network via the Wg reference point.
- Filters out packets based on unencrypted information in the packets. Packets should only be forwarded if they:
  1. are part of an existing tunnel or
  2. are expected messages from the WLAN UEs. This includes service requests, and tunnel establishment messages.
- If QoS mechanisms are applied: supports DiffServ mechanism for uplink/downlink IP packets.

Since the WAG does not have a full trust relationship with the WLAN UE, it is not able to stop all messages. However, messages from an unknown IP address can easily be discarded. Other approaches may be used as well. Additional types of message screening are left to the operators' control. Furthermore, Network Address Translators within the WLAN may modify the source address of IP packets from the WLAN UEs. The modified source address can be reliably associated to a WLAN UE by the PDG during tunnel establishment and provided to the WAG via the 3GPP AAA Server/Proxy. Before this point, all tunnel establishment packets shall be routed by the WAG except those which are possibly discarded due to certain Firewall rules implemented on the WAG.

NOTE: Per tunnel accounting generation in the WAG is not required when the WAG and PDG are in the same network, i.e. the non-roaming case.

The WAG may implement policy enforcement before tunnel establishment to enhance the firewall against unwanted packets go through the PLMN, for example, to forbid the roaming WLAN UE from sending tunnel establishment to PLMN other than its HPLMN; to forbid packets from unauthorized WLAN UE.

The WAG shall implement policy enforcement after tunnel establishment.

After tunnel establishment, the following procedures apply at the WAG:

- If service is provided through a PDG in the HPLMN the WAG:
  - Ensures that all packets from the WLAN UE are routed to the HPLMN.
  - Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the HPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.
- If service is provided through a PDG in the VPLMN the WAG:

- Ensures that all packets from the WLAN UE are routed to the VPLMN.
- Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the VPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.

6.2.5.1 Policy Enforcement

Information regarding the selected PDG, including whether the PDG is in the HPLMN or the VPLMN is provided by the HPLMN to the VPLMN.

In the roaming case, the PDG information is delivered from the 3GPP AAA Server to the 3GPP AAA Proxy.

Within the VPLMN, policy enforcement information is delivered to the WAG.

NOTE: Whether information regarding one or all PDGs is provided will likely impact the signalling which supports the activation of a further W-APN. Delivering information of all valid PDGs may limit impacts on signalling for further W-APN establishment.

The policy enforcement delivered during initial authentication (before the tunnel establishment) will be bound to a user's AAA signalling. The WAG requires functionality to be able to associate this information to a user's traffic. As an implementation option, this functionality can be achieved by allocating the local IP Address by VPLMN.

The binding of the policy to a user's traffic allows the WAG to drop un-authorized packets sent to/from a user.

6.2.5.2 Void

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to a WLAN 3GPP IP Access enabled system.

3GPP PS based services are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- Allows allocation of the WLAN UE's remote IP address;
- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.

- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging (TS 32.251 [13], TS 23.125 [15]), e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.
- In case the PDG has the interface with the PDN which requires the authentication and authorization with the External AAA Server, then the PDG shall negotiate with the WLAN UE whether "Multiple authentication Exchanges in IKEv2" is supported or not. If both WLAN UE and PDG support this function and WLAN UE requests multiple authentications with the External AAA Server, then next authentication and authorization with the External AAA Server is performed after the successful authentication and authorisation with the 3GPP AAA Server. Details on the multiple authentications are specified in RFC 4739 [32]. Whether or not multiple authentications and authorizations are required is configured on a W-APN basis in the PDG.
- If QoS mechanisms are applied: it operates as a QoS edge router between 3GPP/WLAN Interworking system and external network, by supporting DiffServ edge function. When applying receiver control DiffServ edge functions the authorized 3GPP WLAN QoS profile (as received from the 3GPP AAA server) shall be enforced according to operator policy. This may result in re-classification (re-marking the DSCP) or discarding of IP packets.
- If QoS mechanisms are applied: enforces policy control (e.g. service based QoS control or gating) according to TS 23.203 [36].

Annex F describes how PDG functionality can be provided by re-using existing unmodified GGSN functionality.

6.2.7 Subscription Locator Function (SLF)

The SLF is located within the 3GPP subscriber's home network and enables the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS's. The SLF should be used in the same way for WLAN as for IMS, which is specified in TS 23.228 [24].

6.2.8 Offline Charging System

The Offline Charging System is within the 3GPP network. The mapping of the Offline Charging System in the Release 6 charging architecture is specified in TS 32.252 [26].

6.2.9 Online Charging System

The Online Charging System (OCS) is located within the 3GPP network. The OCS is described in TS 32.296 [27].

6.3 Reference Points

6.3.1 Wa reference point

6.3.1.1 General description

The Wa reference point connects the WLAN Access Network, possibly via intermediate networks, to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN Access Networks.

Legacy logical nodes outside of 3GPP scope that terminate or proxy the Wa reference point signalling and do not support 3GPP AAA protocol shall require signalling conversion between the legacy AAA protocol and the 3GPP AAA protocol.

EAP authentication shall be transported over the Wa reference point.

6.3.1.2 Functionality

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

- Carrying data for authentication signalling between WLAN UE and 3GPP Network;
- Carrying data for authorization (including the authorization information update) signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN;
- Carrying charging signalling per WLAN user to enable offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN;
- Enabling the identification of the operator networks amongst which the roaming occurs;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately;
- Purging a user from the WLAN access for immediate service termination;
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters);
- If QoS mechanisms are applied: carrying data for WLAN AN QoS capabilities/policies (e.g. the supported 3GPP WLAN QoS profiles) within authentication request from WLAN AN to 3GPP AAA Proxy and 3GPP AAA Server.

6.3.2 Wx reference point

This reference point is located between 3GPP AAA Server and HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HSS.

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HSS.
- Retrieval of WLAN access-related subscriber information (profile) from HSS
- Registration of the 3GPP AAA Server of an authorised (for WLAN Access) WLAN user in the HSS.
- Indication of change of subscriber profile within HSS (e.g. indication for the purpose of service termination).
- Purge procedure between the 3GPP AAA server and the HSS.

- Retrieval of online charging / offline charging function addresses from HSS.
- Fault recovery procedure between the HSS and the 3GPP AAA Server.
- Retrieval of service related information (e.g. W-APNs that may be selected by the WLAN UE and the data defined for the W-APNs in the WLAN UE's profile) including an indication of whether the VPLMN is allowed to provide this service.

6.3.3 D'/Gr' reference point

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HLR. The protocol crossing this reference point is based upon the D/Gr reference points defined in TS 23.002 [31]. Support of the D'/Gr' reference points requires no modifications to the MAP protocol at the HLR.

When the HLR makes it possible the functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.
- Registration of the 3GPP AAA Server of an authorised WLAN user in the HLR.
- Indication of change of subscriber profile within HLR (e.g. indication for the purpose of service termination).
- Purge procedure between the 3GPP AAA server and the HLR.
- Fault recovery procedure between the HLR and the 3GPP AAA server.
- Retrieval of service related information (e.g. APNs that may be selected by the WLAN UE) including indications of whether the service is to be supported by the HPLMN or by an identified VPLMN.
- Retrieval of online/offline charging function address from HLR.

The functions provided on the D'/Gr' reference points are a subset of the functions provided on the D/Gr reference points described in TS 23.002 [31].

If a 3GPP AAA Server supports the D' reference point, it will appear to the HLR/HSS as a VLR and shall behave according to the description of the behaviour of a VLR supporting the D reference point as described in TS 23.002 [31].

If a 3GPP AAA Server supports the Gr' reference point, it will appear to the HLR/HSS as an SGSN and shall behave according to the description of the behaviour of an SGSN supporting the Gr reference point as described in TS 23.002 [31].

6.3.4 Wo reference point

The Wo reference point is used by a 3GPP AAA Server to communicate with 3GPP Online Charging System (OCS). The prime purpose of the protocol(s) crossing this reference point is to transport online charging related information so as to perform credit control for the online charged subscriber.

The functionality of the reference point is to transport:

- Online charging data.

Wo reference point should be similar to Ro interface currently used in 3GPP OCS.

6.3.5 Wf reference point

The Wf reference point is located between 3GPP AAA Server/Proxy and 3GPP Offline Charging System. The prime purpose of the protocols crossing this reference point is to transport/forward offline charging information towards 3GPP operator's Offline Charging System located in the visited network or home network where the subscriber is residing.

The information forwarded to the Offline Charging System is typically used for:

- Generating bills for offline charged subscribers by the subscribers' home operator.

- Calculation of inter-operator accounting from all roaming users. This inter operator accounting is used to settle the payments between visited and home network operator and/or between home/visited network and WLAN.

The functionality of the reference point is to transport:

- WLAN access-related charging data per WLAN user.

6.3.6 Wg reference point

The Wg reference point applies to WLAN 3GPP IP Access.

This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to:

- provide information needed by the WAG to perform policy enforcement functions for authorised users.
- transport per-tunnel based charging information from the WAG to the AAA Proxy, only for roaming scenario.

6.3.7 Wn reference point

The Wn reference point applies to WLAN 3GPP IP Access.

This is the reference point between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. There can be several different ways to implement this interface as shown in Annex C. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN and is out of the scope of this Release of 3GPP specifications.

6.3.8 Wp reference point

The Wp reference point applies to WLAN 3GPP IP Access.

This is the reference point between the WAG and PDG.

6.3.9 Wi reference point

The Wi reference point applies to WLAN 3GPP IP Access.

This is the reference point between the Packet Data Gateway and a packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. the entry point of IMS, RADIUS Accounting or Authentication, DHCP.

Wi reference point is similar to the *Gi* reference point provided by the PS domain. Interworking with packet data networks is provided via the Wi reference point based on IP. Mobile terminals offered services via the Wi reference point may be globally addressable through the operator's public addressing scheme or through the use of a private addressing scheme.

6.3.10 Wm reference point

The Wm reference point applies to WLAN 3GPP IP Access.

This reference point is located between 3GPP AAA Server and Packet Data Gateway respectively between 3GPP AAA Proxy and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server/Proxy to retrieve tunnelling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- The 3GPP AAA Server to provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
- The 3GPP AAA Server to provide the PDG with charging data (subscribed Charging Characteristics or W-APN Charging Characteristics) for 3GPP PS based services charging

- Carrying messages between PDG and AAA Server in support of the user authentication exchange which takes place between WLAN UE and 3GPP AAA server/proxy.
- Carrying messages for user authorization (including authorization information update) between PDG and 3GPP AAA server/proxy. These messages transport e.g. the requested W-APN from PDG to 3GPP AAA server/proxy and eventually the authorized W-APN from 3GPP AAA server/proxy to PDG.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.

6.3.11 Wd reference point

6.3.11.1 General description

The Wd reference point connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner.

EAP authentication shall be transported over the Wd reference point.

6.3.11.2 Functionality

The functionality of the reference point is to transport AAA messages including:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying charging signalling per WLAN user;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the PDG is in the VPLMN;
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server;
- Used for purging a user from the WLAN access for immediate service termination;
- Enabling the identification of the operator networks amongst which the roaming occurs;
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters);
- If QoS mechanisms are applied: carrying data for WLAN AN QoS capabilities/policies (e.g. the supported 3GPP WLAN QoS profiles) within authentication request from 3GPP AAA Proxy to 3GPP AAA Server.

6.3.12 Wu reference point

The Wu reference point applies to WLAN 3GPP IP Access.

The Wu reference point is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. Transport for the Wu reference point protocol is provided by the Ww, Wn and Wp reference points, which ensure that the data are routed via the WLAN Access Gateway where routing enforcement is applied.

The functionality of the Wu reference point is to enable:

- WLAN UE-initiated tunnel establishment
- User data packet transmission within the WLAN UE-initiated tunnel

- Tear down of the WLAN UE initiated tunnel

6.3.13 Ww reference point

6.3.13.1 General Description

The reference point Ww connects the WLAN UE to the WLAN Access Network per IEEE 802.1x [19] specifications or for other access systems, by mechanisms providing equivalent security. The definition of IEEE Physical and Medium Access Control layers protocols (e.g. Layer 1 and Layer 2 defined by IEEE 802.11 standards) is out of the scope of 3GPP.

6.3.13.2 Functionality

The functionality of the reference point is based on IEEE 802.1x specifications [19] or, for non-WLAN access systems, specifications with equivalent functionality and it is intended to transport signalling messages including:

- parameters 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).

6.3.14 Dw reference point

This reference point is between the 3GPP AAA Server and the SLF. The prime purpose of the protocol(s) crossing this reference point is to enable the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS's.

6.3.15 Wy reference point

The Wy reference point is used by a PDG to communicate with an Online Charging System (OCS). The purpose of the protocol(s) crossing this reference point is to transport online charging related information about WLAN 3GPP IP Access so as to perform credit control for the online charged subscriber.

6.3.16 Wz reference point

The Wz reference point is used by a PDG to communicate with an Offline Charging System. The purpose of the protocol(s) crossing this reference point is to transport offline charging related information about WLAN 3GPP IP Access.

6.4 Protocols

The protocol stack between the WLAN UE and the PDG is shown in figure 6.3

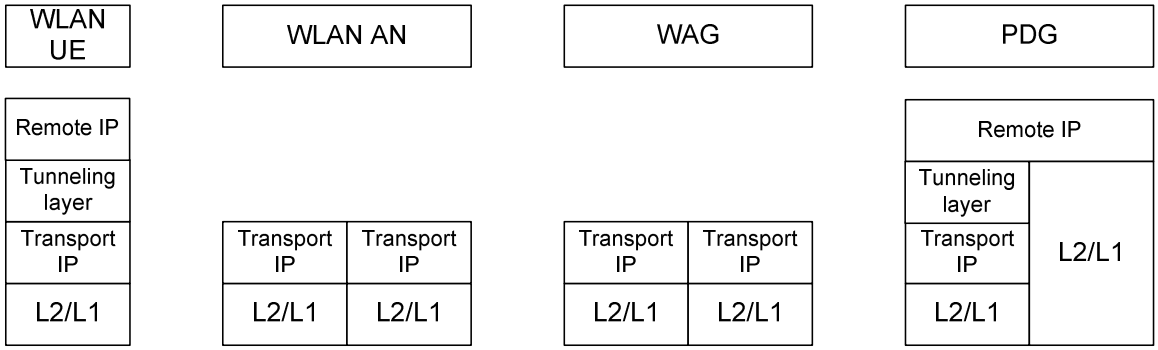


Figure 6.3: Protocol stack between the WLAN UE and the Packet Data Gateway

6.4.1 Remote IP Layer

The remote IP layer is used by the WLAN UE to be addressed in the external packet data networks (i.e. on the Wi reference point).

On this layer, the WLAN UE is addressed by its remote IP address and the packets are exchanged between the WLAN UE and an external entity. The PDG routes the remote IP packets without modifying them.

6.4.2 Tunnelling layer

The tunnelling layer consists of a tunnelling header, which allows end-to-end tunnelling between a WLAN UE and a PDG. It is used to encapsulate IP packets with the remote IP layer.

When encapsulated IP packets are encrypted, the tunnelling header contains a field which is used to identify the peer and decrypt the packets.

6.4.3 Transport IP Layer

The transport IP layer is used by the intermediate entities/networks and WLAN AN in order to transport the remote IP layer packets.

Between the WLAN UE and the WAG, the transport IP layer is used by the WLAN UE to be addressed within the WLAN AN, the intermediate networks (if any) and 3G networks.

On this layer, the WLAN UE is addressed by its local IP address.

For example this local IP address can be:

- a private IPv4 address allocated by the WLAN AN; in this case a NAT is required in the WLAN AN and used to make the WLAN UE's local IP address routable in the intermediate networks (if any), the VPLMN and the HPLMN;
- a public (either IPv4 or IPv6) address allocated by the WLAN AN; in this case no NAT is needed;
- an IP address allocated by the WAG in an address space that is routable in the WLAN AN as well as in the intermediate networks (if any) and the 3G network; in this case no NAT is needed.

6.5 WLAN user profile

The WLAN user profile shall reside in HSS (if the operator is using a legacy HLR, the WLAN user profile may reside in the 3GPP AAA Server) and be retrieved by 3GPP AAA server via Wx reference point. The parameters stored in the network elements for I-WLAN, which includes the parameters of the WLAN user profile, are defined in clause 3B of TS 23.008 [29].

7 Procedures

7.1 I-WLAN and VPLMN Selection Procedure

7.1.1 Initial network selection

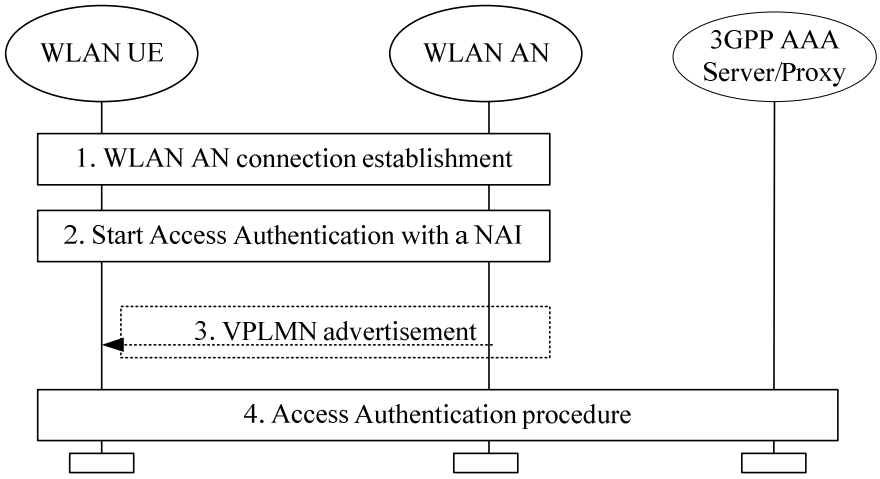


Figure 7.1: I-WLAN and VPLMN selection procedure

1. The WLAN UE selects a WLAN AN and establishes the WLAN connection with a WLAN technology specific procedure (e.g. in IEEE 802.11 it starts an association procedure). The details of the selection of the WLAN AN are specified in TS 24.234 [9].

2. The Authentication procedure is initiated in a WLAN technology specific way and as a part of this process, the WLAN UE sends a NAI to the WLAN AN. The NAI shall be constructed as it is specified in TS 23.003 [5].

3. If the WLAN AN is not able to route the authentication request (e.g. in the case where the WLAN AN receives an initial NAI with an unknown realm), the WLAN AN sends a response to the WLAN UE that provides information about the 3GPP networks to which the WLAN AN is able to route authentication requests. If IMS Emergency Calls are supported in a given 3GPP network, this shall be indicated to the WLAN UE via an IMS Emergency Call specific realm.

   From this point the WLAN UE may continue the access authentication with the selected WLAN AN using a different NAI (step 2) or may start access authentication with another available WLAN AN (step 1) or may stop. The details of the WLAN UE behaviour are specified in TS 24.234 [9]. If the WLAN UE continues the access authentication with the selected WLAN AN, it shall select a VPLMN among the 3GPP networks indicated in the response received from the WLAN AN and build the new NAI as a roaming NAI indicating this VPLMN.

4. The WLAN AN routes the AAA message to the 3GPP AAA Server or 3GPP AAA Proxy based on the NAI and the access authentication is performed as it is specified in TS 24.234 [9].

7.1.2 Network re-selection

When the WLAN UE changes from the current serving PLMN to another PLMN with or without change of the WLAN AN, it needs to use a new NAI corresponding to the new PLMN in a new authentication initiated by the WLAN UE or the WLAN AN.

The 3GPP AAA Server may then receive a new authentication with PLMN selection different from the current active connection. For example, the WLAN UE lost radio in the first WLAN AN, then it changed to another WLAN AN with a different PLMN selection before the previous WLAN AN detected that the user is lost, or the WLAN UE started the new authentication before the disconnection of the previous connection. In this case, the 3GPP AAA Server shall initiate a disconnection to the currently active connection after the success of the new authentication and authorization process.

7.2 WLAN Access Authentication and Authorisation

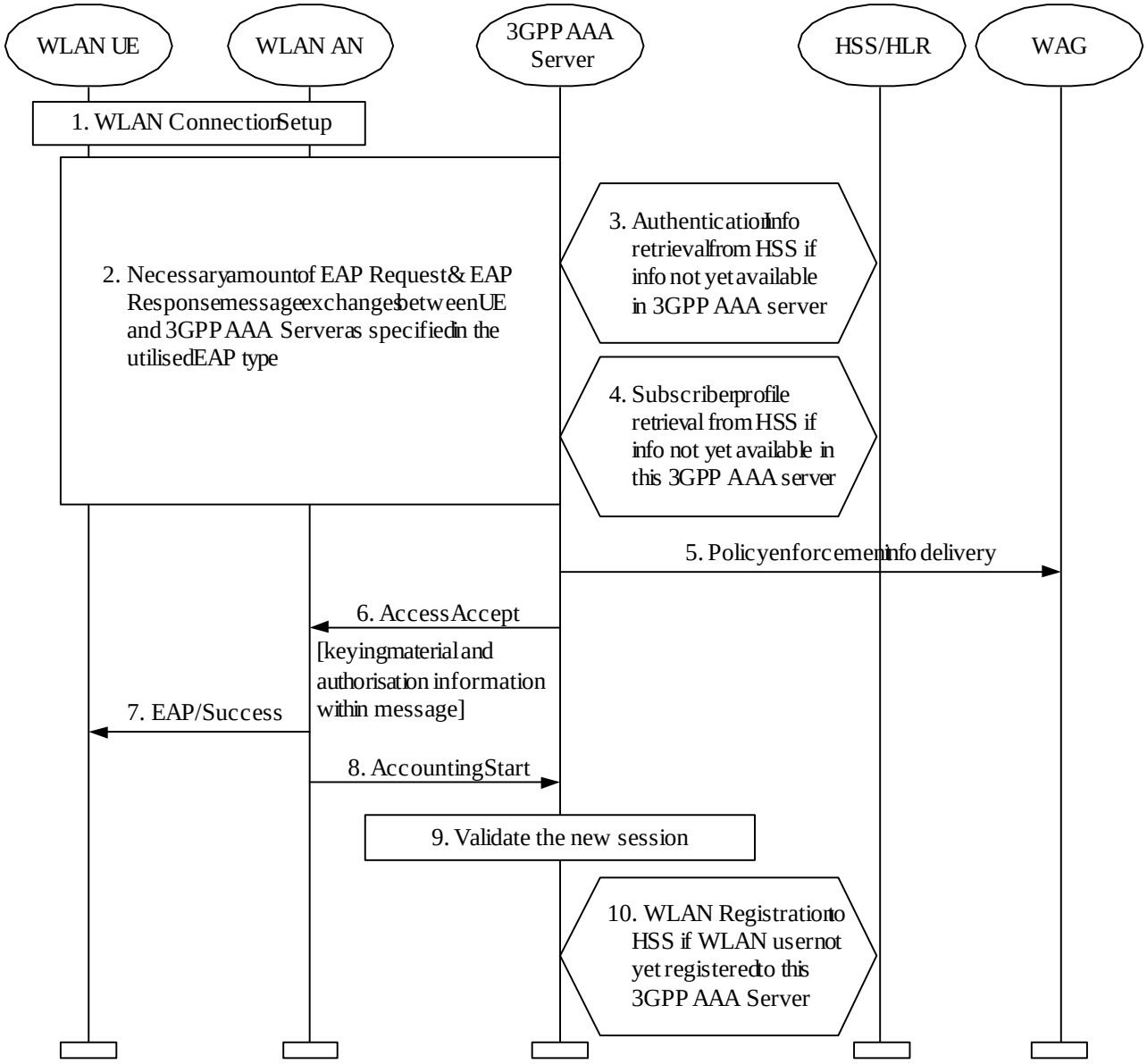


Figure 7.2: Authentication and authorisation procedure

1. WLAN connection is established with a WLAN technology specific procedure (out of scope for 3GPP).

2. The EAP authentication procedure is initiated in WLAN technology specific way.
   All EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.
   All EAP packets are transported over the Wa reference point.
   A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

   For IMS Emergency Calls, the used EAP method shall accommodate the emergency request.

   The WLAN AN may send its QoS capabilities/policies (e.g. the supported 3GPP WLAN QoS profiles) to the 3GPP AAA Server within above authentication procedure signalling. Standardized techniques for capabilities exchange are to be determined in stage 3.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in

3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised. During the information retrieval the HSS/HLR checks if there is a 3GPP AAA Server already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA Server has already registered for this user, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signalling is then routed to the previously registered 3GPP AAA Server.

NOTE 1: For IMS Emergency Calls, authentication may be skipped entirely depending on the national regulations or the operator's preference.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

NOTE 2: In case of IMS Emergency Calls it is possible that no subscription information is available, therefore no data retrieval from the HSS is possible, e.g. in case of UICC-less IMS Emergency Calls.

5. Optionally, the 3GPP AAA Server (or the 3GPP AAA Proxy in roaming case) may send the policy enforcement information to the WAG in the PLMN that the WLAN UE selected in case VPLMN is to allocate the local IP Address for the WLAN UE.

NOTE 3: Additional process, such as allocating the IP address, may be necessary during or before this step to be performed.

6 If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) to the WLAN. When QoS mechanism is applied the authorized 3GPP WLAN QoS profile shall be included in this message, and 3GPP AAA Server shall store authorized 3GPP WLAN QoS Profile and/or WLAN QoS capabilities/policies if available.
WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

NOTE 4: In the roaming case, authorisation information is passed from 3GPP AAA Server to 3GPP AAA Proxy in the form of Local service identifiers (see section 6.5).

NOTE 5: Depending on national regulations and operator preferences, in the case of IMS Emergency Calls, the 3GPP AAA server may still send Accept (i.e. indicating success of authentication and authorization) even though authentication or authorization fails. In case the WLAN UE has indicated IMS Emergency Call within the procedure, the routing policy sent to the WLAN shall include only those policies necessary to set up an IMS Emergency Call (e.g. allow tunnel set up but no Direct IP Access permitted).

7 WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.

8 The 3GPP AAA server receives an accounting start message from the WLAN AN.

9 At this point the 3GPP AAA server considers that a new authenticated session is started and it checks its validity. If there is a different previously established authentication session of the WLAN user, e.g., a session that uses a different WLAN UE or roaming in a different WLAN AN or in a different VPLMN, the 3GPP AAA Server shall close the previously established session ("Session abort procedure" over Wa) to avoid multiple WLAN direct IP access sessions.

10 3GPP AAA Server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

7.3 Subscriber Profile Update

7.3.0 WLAN Direct Access Authorization information update procedure

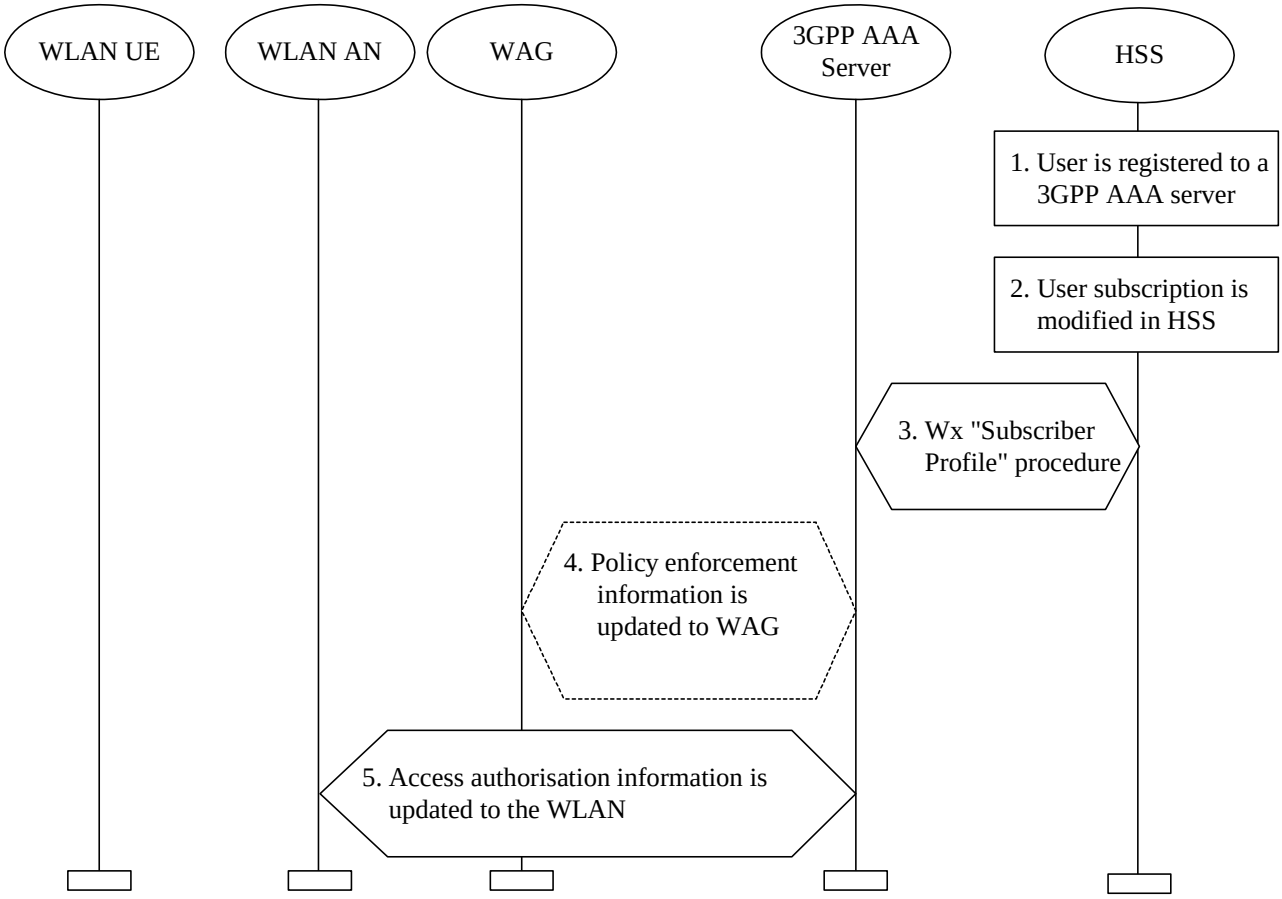


Figure 7.3: Subscriber Profile and access authorization info Update Procedure

1. User is registered to a 3GPP AAA Server
2. Subscribers subscription is modified in the HSS e.g. via O&M.
3. HSS updates the profile information stored in the registered 3GPP AAA Server by Wx reference point procedure "Subscriber Profile".
4. If the policy enforcement information updated in step 3 and the policy enforcement information was sent to the WAG beforehand (e.g., in step 5 of clause 7.2), it should be updated to the WAG in this step.
5. The WLAN access authorisation information of the associated connection is updated to WLAN as necessary. If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.

7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP IP Access.

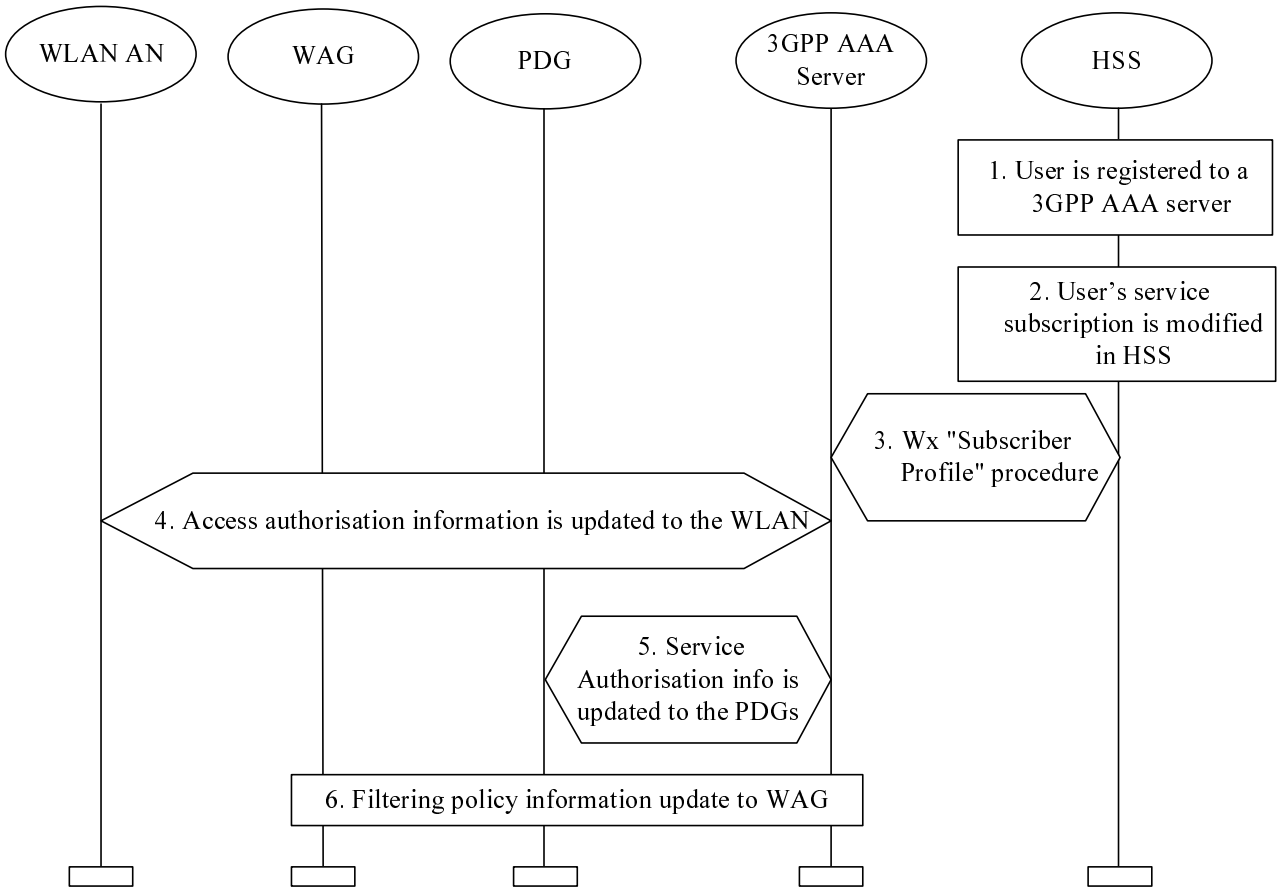


Figure 7.4: Authorization information Update Procedure

1. User is registered to a 3GPP AAA Server
2. User's service subscription is modified in the HSS e.g. via O&M,
3. HSS updates the profile information stored in the registered 3GPP AAA Server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN AN if necessary. If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.
5. The service authorisation information of the activated services is updated to PDGs if necessary. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.
6. The filtering policy information of the activated services is updated to WAG if necessary.

NOTE: The de-registration may be initiated by the 3GPP AAA Server to the HSS as necessary, i.e., the 3GPP AAA Server determines that the WLAN UE is unable to access any service upon the updated authorization.

7.4 Cancelling WLAN Registration

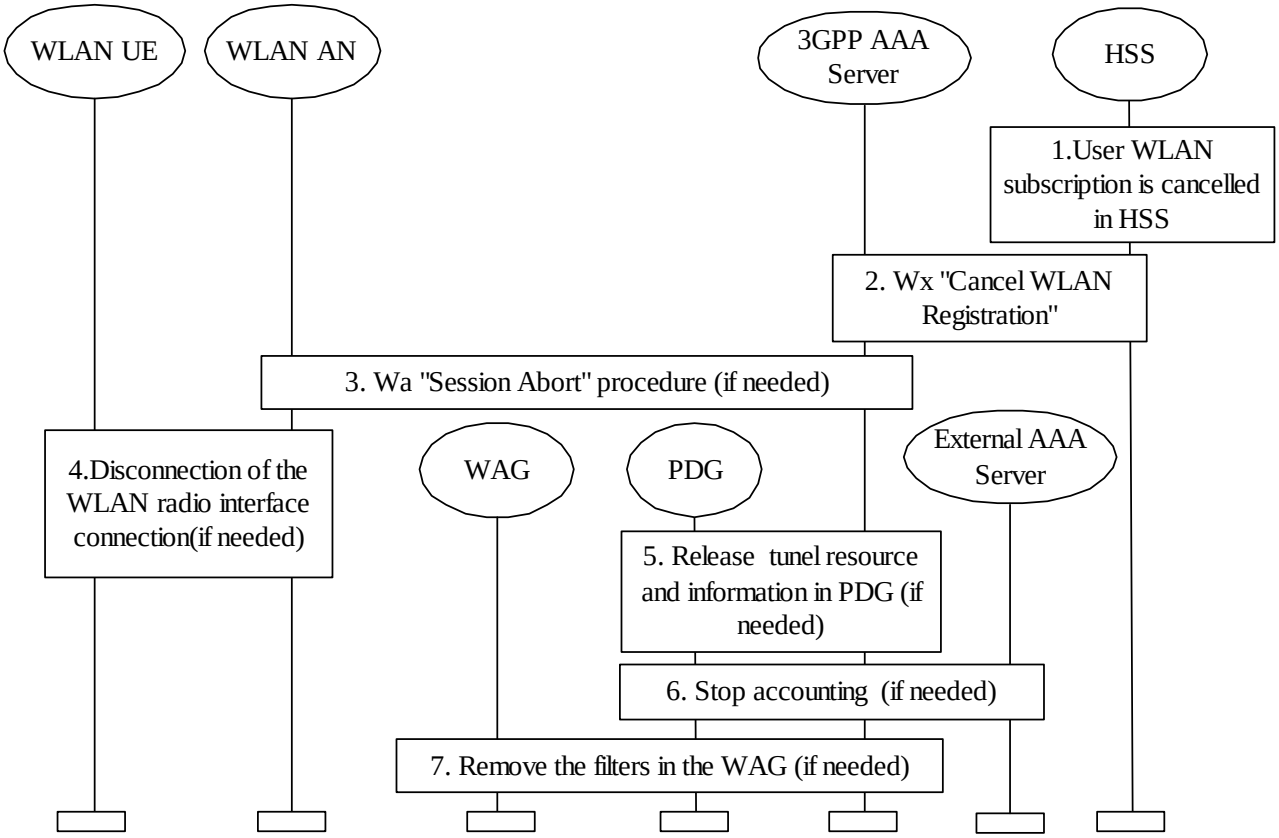


Figure 7.5: Cancellation of WLAN Registration Procedure

1. The 3GPP subscribers WLAN subscription is cancelled in HSS.
2. HSS cancels subscribers WLAN registration in the 3GPP AAA Server by Wx reference point procedure "Cancel WLAN Registration". In the messages subscriber is identified by his permanent identity.
3. If the subscriber's WLAN access connection still exists, Wa reference point procedure "Session Abort" procedure is executed towards WLAN.
4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA Server/Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. If accounting has been started in the External AAA Server, then the PDG initiates "Accounting Stop" procedure to the External AAA Server.
7. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

7.5 Disconnecting a Subscriber by WLAN

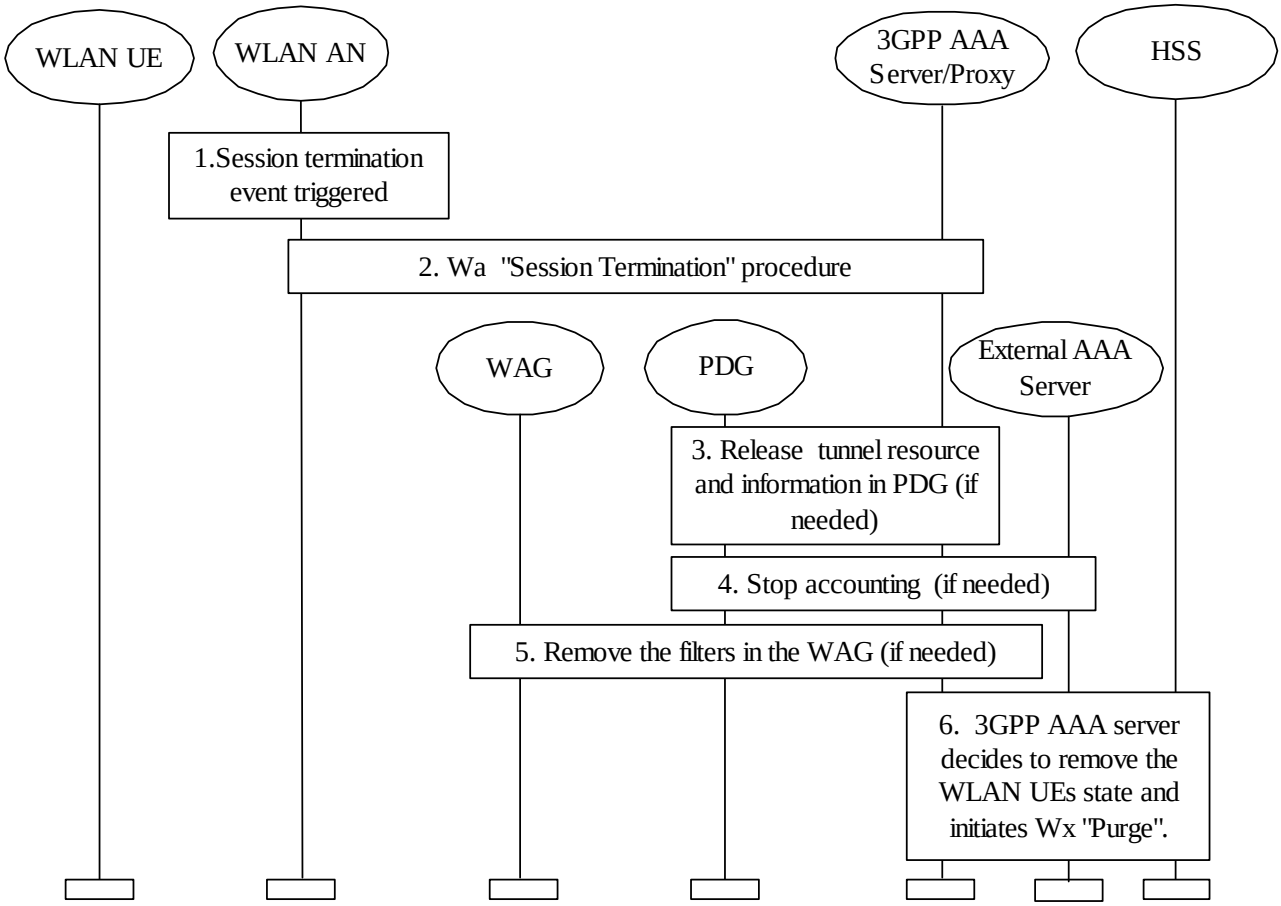


Figure 7.6: WLAN initiated disconnection procedure

1. WLAN detects that a Session related to a WLAN UE should be terminated towards the 3GPP AAA Server, e.g. when the WLAN UE has disappeared from WLAN coverage.
2. WLAN initiates Wa Session Termination procedure towards 3GPP AAA Server.
3. If the subscriber has a tunnel connection with one or more PDGs, and the 3GPP AAA Server/Proxy needs to remove the connections, it informs the PDG(s) over the Wm reference point to remove the tunnel related information and resource.
4. If accounting has been started in the External AAA Server, then the PDG initiates "Accounting Stop" procedure to the External AAA Server.
5. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.
6. In case when the 3GPP AAA Server decides to remove the WLAN UEs state from the 3GPP AAA Server, the 3GPP AAA Server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. HSS removes the state related to that 3GPP AAA Server, e.g., the address of the serving 3GPP AAA Server for the identified subscriber.

7.6 Disconnecting a Subscriber by Online Charging System

7.6.1 The OCS initiated WLAN AN access disconnection

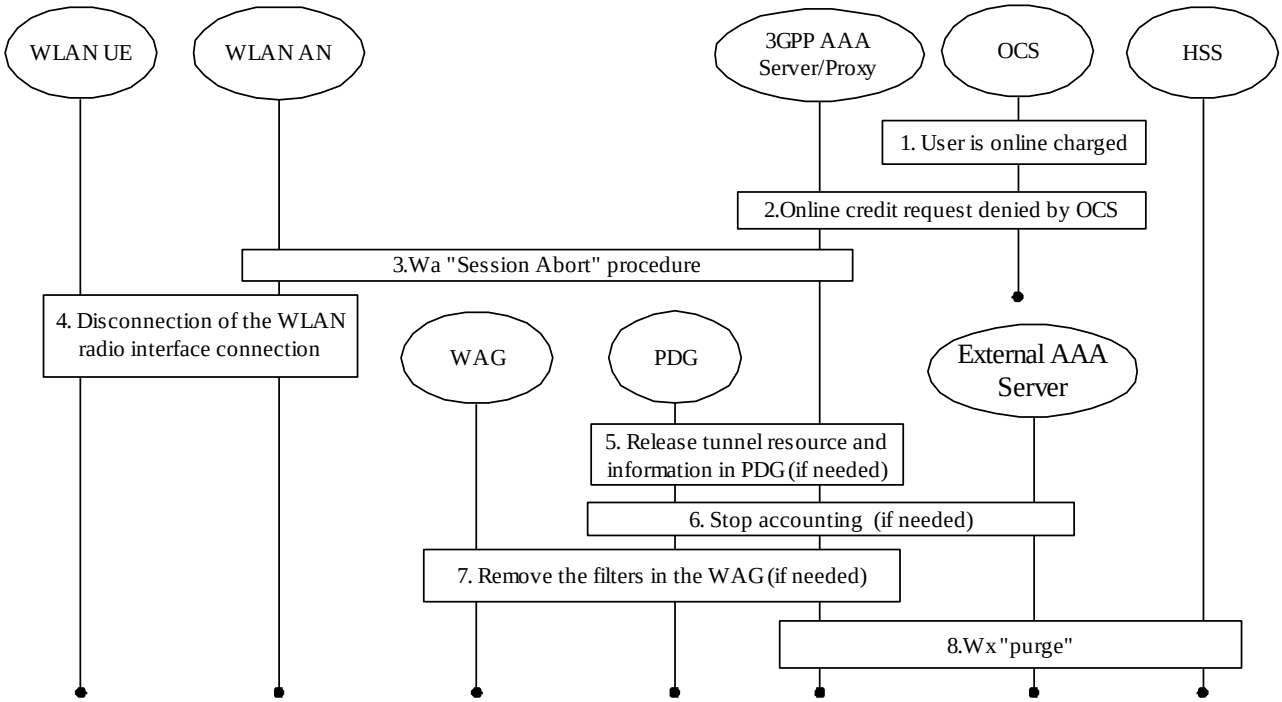


Figure 7.7: The OCS initiated WLAN AN access disconnection procedure

This section applies to the case when an online charged user runs out of credit and is totally disconnected from WLAN.

1. A subscriber is online charged by 3GPP AAA Server for WLAN access.
2. The OCS (Online Charging System) denies credit request from the 3GPP AAA Server for WLAN access. The possibly already retrieved online credit runs out.
3. To disconnect the subscriber's connection, Wa reference point procedure "Session Abort" procedure is executed towards the WLAN AN.
4. The WLAN AN disconnects the radio interface connection by WLAN technology specific mechanisms.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA Server/Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. If accounting has been started in the External AAA Server, then the PDG initiates "Accounting Stop" procedure to the External AAA Server.
7. If filters were deployed to WAG for the tunnel(s) during the tunnel establishment, then they are removed.
8. If no Wx "Purge" procedure was already initiated in step 3, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge"

7.6.2 The OCS initiated tunnel disconnection

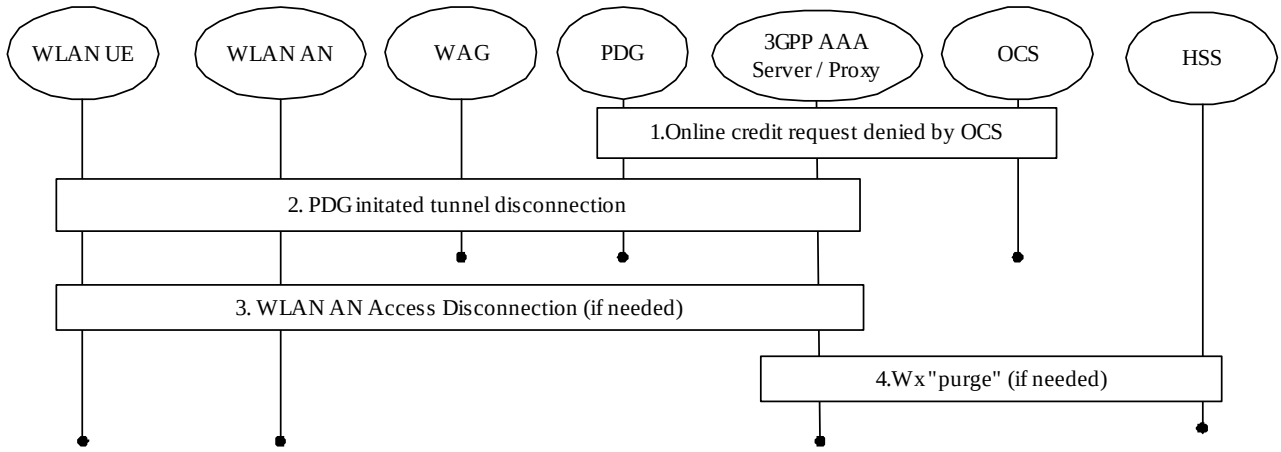


Figure 7.8a: The OCS initiated tunnel disconnection procedure

This section applies to the case when the tunnels of an online charged user are disconnected due to the lack of credits.

1. The Online Charging System (OCS) denies the credit request from the PDG. The possibly already retrieved online credit runs out.

2. The PDG disconnects the tunnels that require new credits using the network initiated tunnel disconnection procedure (clause 7.10.2). The tunnels that do not require new credits (e.g., the tunnels using free of charge W-APNs) will not be disconnected.

3 If all tunnels of the subscriber have been disconnected in the previous step then the 3GPP AAA Server may decide to totally disconnect the subscriber by performing "Session Abort" towards the WLAN AN (i.e. step 3 and 4 of clause 7.6.1).

4. If the subscriber is disconnected from the WLAN AN in step 3 and no Wx "Purge" procedure was already initiated, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge".

7.7 Charging offline charged subscribers

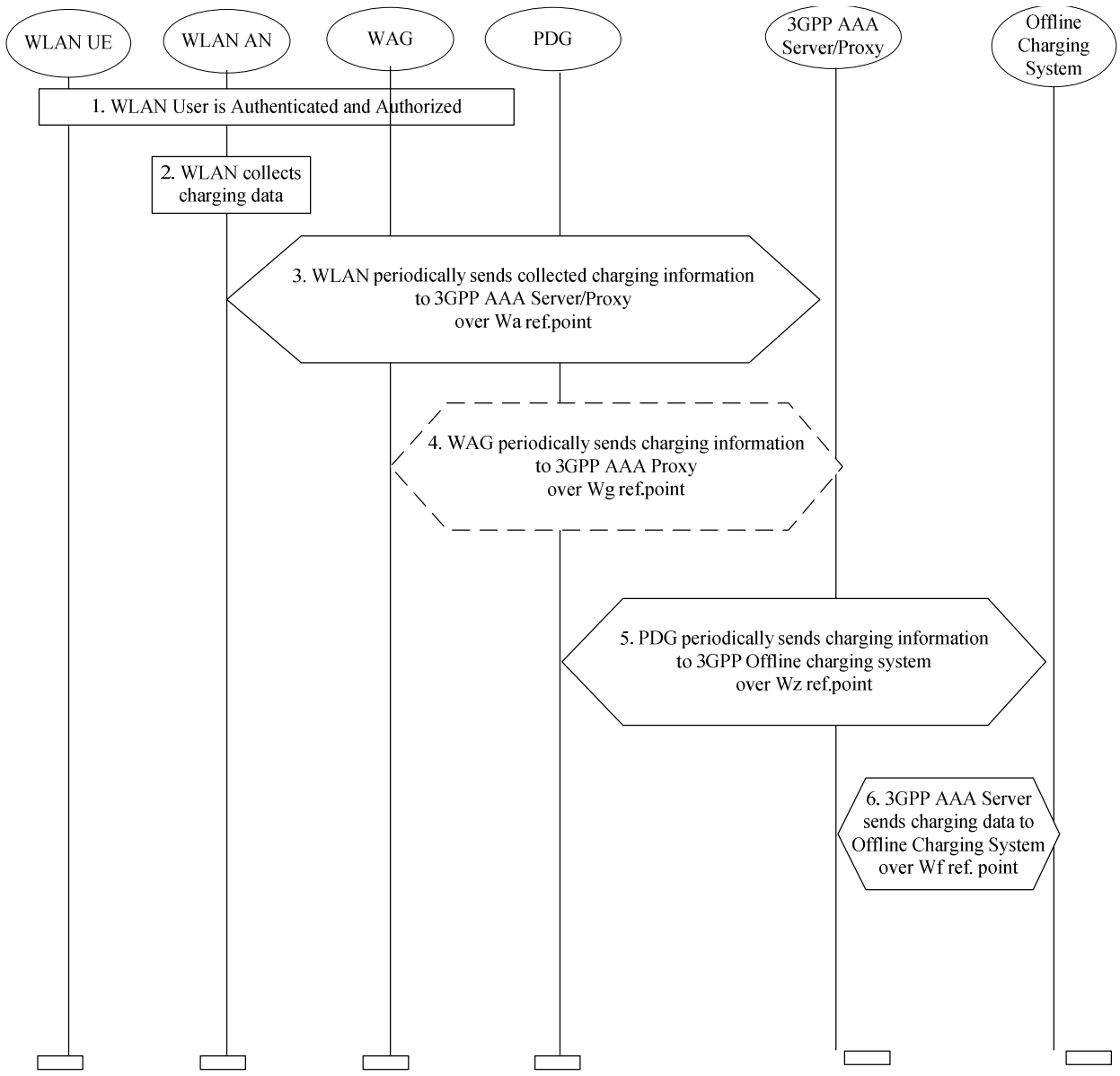


Figure 7.8: Charging Procedure for Offline Charged Subscribers

1. The WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA Server. Part of the profile is information that the user is to be offline charged.

2. The WLAN AN collects charging data related to access or services locally consumed.

3. The WLAN AN periodically forwards collected charging information to the 3GPP AAA Server over Wa reference point. While roaming, the 3GPP AAA Proxy in VPLMN then relays this information to VPLMN's offline charging system over Wf interface and to the 3GPP AAA Server in HPLMN over Wd interface.

4. This step only happens in roaming case as shown in figure 6.2a: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network. In this case the WAG in VPLMN periodically sends charging information to the 3GPP AAA Proxy in VPLMN over Wg reference point. The 3GPP AAA Proxy in VPLMN then relays this information to VPLMN's offline charging system over Wf interface.

5. In case UE establishes IPsec Tunnel with PDG. The PDG periodically sends charging information to the 3GPP Offline charging system over Wz reference point.

6. The 3GPP AAA Server forwards charging information to the HPLMN's Offline Charging System over the Wf reference point.

NOTE: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local Offline Charging System over the Wf reference point.

7.8 Charging online charged subscribers

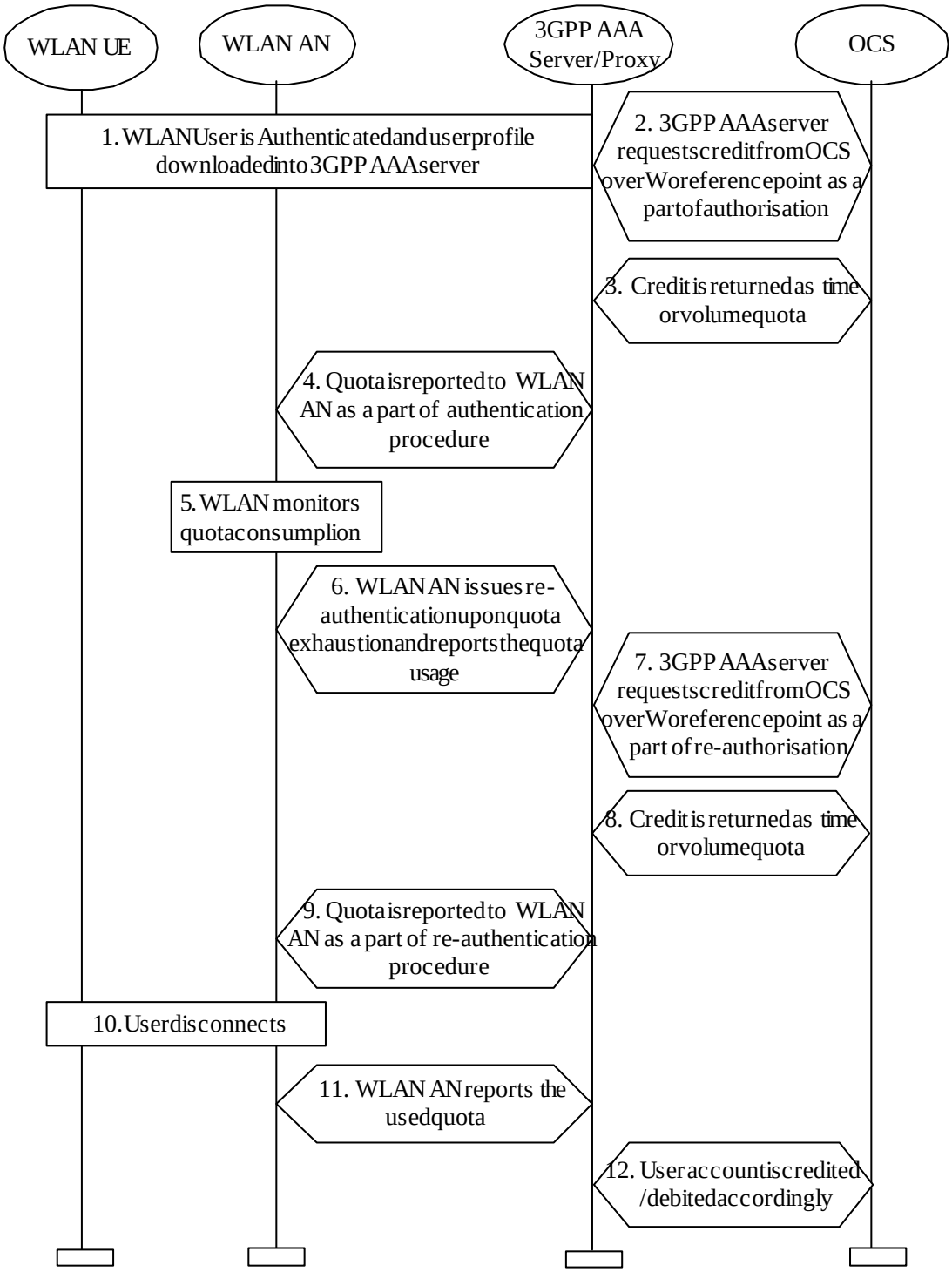


Figure 7.9: Charging Procedure for Online Charged Subscribers

1. The WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA Server. Part of the profile is information that the user is to be online charged.

2. The 3GPP AAA Server requests online charging credit from the OCS.
3. The OCS returns credit as time and/or volume quota.
4. The allocated quota is indicated to the WLAN AN.
5. The WLAN AN monitors the quota consumption.
6. When quota is almost used, the WLAN AN issues re-authentication message over Wa reference point. Used quota is indicated in the request.
7. The 3GPP AAA Server requests more credit from the OCS.
8. The OCS returns credit as time and/or volume quota.
9. The allocated new quota is indicated to the WLAN AN.
10. The user disconnects from WLAN AN.
11. The WLAN AN reports the used quota to the 3GPP AAA Server over Wa reference point.
12. The user account is debited / credit according the usage information in the final message.

NOTE: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local Online Charging System over Wf reference point. In home network the 3GPP AAA Server may also report the usage to the Online Charging System over the Wf reference point using offline charging procedures for statistical or other purposes.

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. Allocation of the WLAN UE's local IP address and optionally WLAN Access Authentication and Authorisation which may depend on the home operator policy as well as the policy of the provider of the WLAN Access Network.

NOTE 1: The authentication and authorization for WLAN Direct IP access and WLAN 3GPP IP access may be performed independently according to the home operator's policy. (For example, the WLAN Access Authentication and Authorisation procedure can be skipped when the home operator allows).

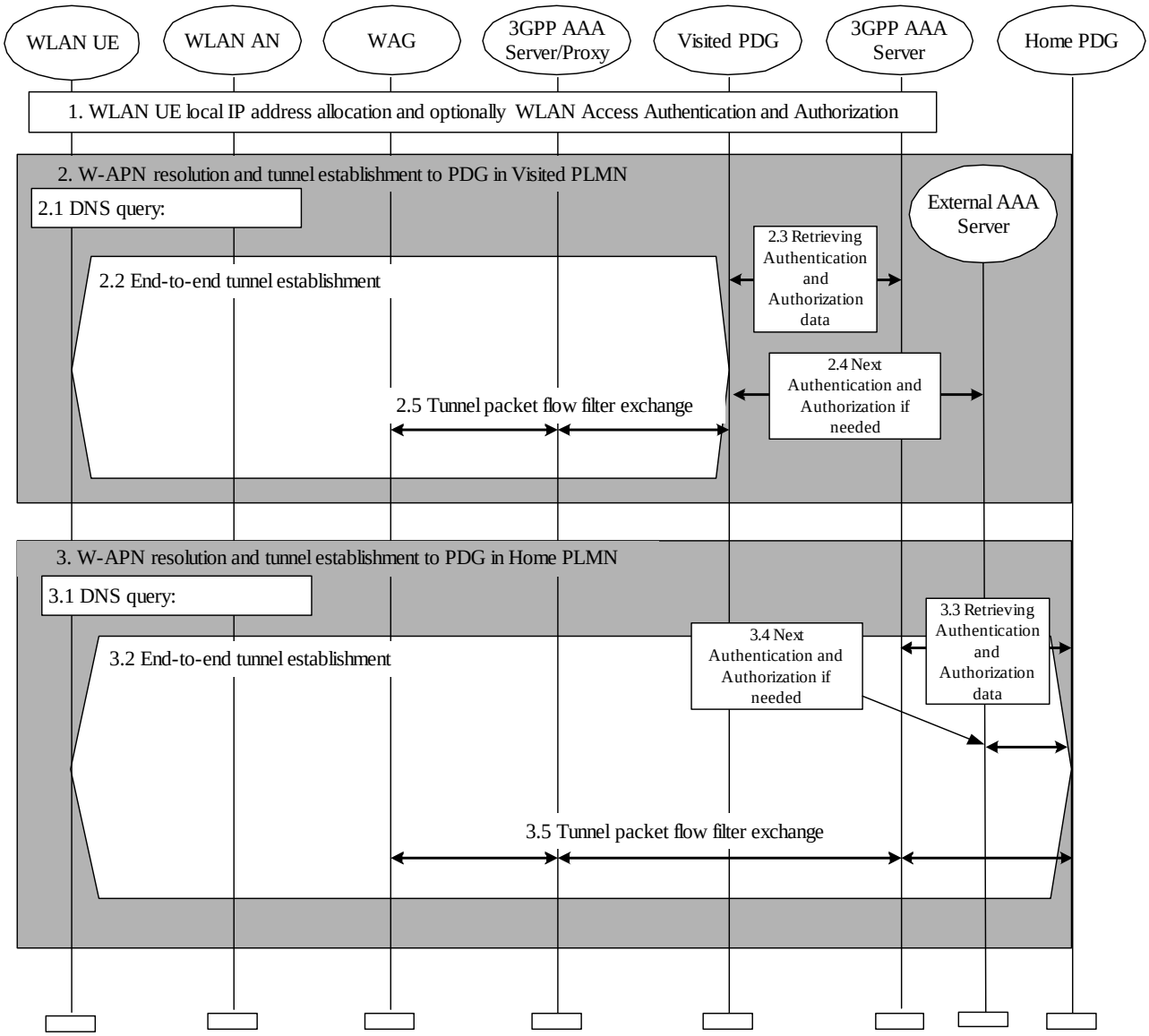


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

For the case of IMS Emergency Calls, a W-APN shall be used to indicate emergency access to PS domain. The emergency call W-APN defaults to the visited/local PDG.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

NOTE 2: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.

2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA Proxy for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment. The authorized 3GPP WLAN QoS profile shall be sent to the PDG if QoS mechanisms are applied. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS.
The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the PDG.
The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics. If it is not possible to establish the tunnel with any of the PDGs received from step2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3. Otherwise, the visited PDG shall dynamically assign a remote IP address for the WLAN UE or shall request it from an external IP network using standard mechanisms (such as DHCP, Radius).

NOTE 3: The access to emergency W-APN shall not require any subscription. Tunnel establishment towards the local emergency W-APN shall not be rejected based on check of user's subscribed services or that user is not allowed to use a PDG from the visited network. However, authorization procedures may be used on Wm to register the PDG at the 3GPP AAA Server as serving the user for the emergency W-APN.

2.4 If the specified W-APN requires the next authentication and authorization with the External AAA Server, the PDG initiates the next authentication and authorization with the External AAA Server after the successful authentication and authorisation in step 2.3. The Accounting start message is sent to the External AAA Server if the specified W-APN requires.

2.5 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc). The PDG binds the remote IP address with the local IP address of the WLAN UE. The remote IP address is communicated to the WLAN UE.

3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.

3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.

3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. The authorized 3GPP WLAN QoS profile shall be sent to the PDG if QoS mechanisms are applied. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS. The 3GPP AAA Server shall be able to check that the

user requesting the tunnel establishment has been already WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the Home PDG. The 3GPP AAA Server shall provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used. Otherwise the home PDG shall dynamically assign a remote IP address for the WLAN UE or shall request it from an external IP network using standard mechanisms (such as DHCP, Radius) The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics.

3.4 If the specified W-APN requires the next authentication and authorization with the External AAA Server, the PDG initiates the next authentication and authorization with the External AAA Server after the successful authentication and authorisation in step 3.3. The Accounting start message is sent to the External AAA Server if the specified W-APN requires.

3.5 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG. The PDG binds the remote IP address with the local IP address of the WLAN UE. The remote IP address is communicated to the WLAN UE.

7.9.1 Void

7.9.2 Subsequent authentication

In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process and to perform fast re-authentication. .Fast re-authentication is an optional feature and its activation is performed in the home operator's network.

7.9.3 Use of DNS

Operators may to restrict the propagation of DNS information used for the above mechanism to DNS servers controlled by the PLMNs and to DNS servers available only to authorised 3GPP WLAN UEs (i.e. those WLAN UEs which have successfully connected to a 3GPP Interworking WLAN). It is an operators' decision whether such propagation of this DNS information is restricted or not.

It shall be possible to configure multiple PDG addresses against a single FQDN in a manner which allows the load to be shared across these PDGs. It shall be possible to configure IPv4 and IPv6 addresses against a single FQDN and to return these addresses together to the WLAN UE. See TS 23.003 [5] for more information on PDG addressing (W APNs).

7.9.4 Subsequent tunnel establishment

The subsequent tunnel establishment should follow the same procedure as in the first tunnel establishment.

7.10 Tunnel disconnection procedures

Tunnel disconnection can be either:

- Initiated from the WLAN UE, as a result of an explicit deactivation/de-registration from the service.
- Initiated from the PDG, e.g. due to timeout of the tunnel connection or request from the 3GPP AAA Server or other network entities.

Tunnel disconnection is specified for the following situations:

- Normal service termination resulting from an end user requesting termination of the end-to-end tunnel connection using tunnel control signalling or deletion of the IP bearers associated with a service,
- Service termination resulting from network operator intervention,
- Loss of radio connections which are used to transport the tunnel signalling.

The tunnel disconnection message exchanges between the WLAN UE and the PDG are performed basing on the specific tunnel control signalling protocol. The WLAN UE and the PDG release the control information associated with the tunnel during the exchange, and the PDG should send a tunnel release report to the 3GPP AAA Server to update the corresponding subscriber's service connection information and status in the 3GPP AAA Server, e.g. the service/tunnel connection activation info, the allocated IP address, etc. The filtering policy information applied on the WAG should also be removed. if necessary.

7.10.1 WLAN UE initiated tunnel disconnection

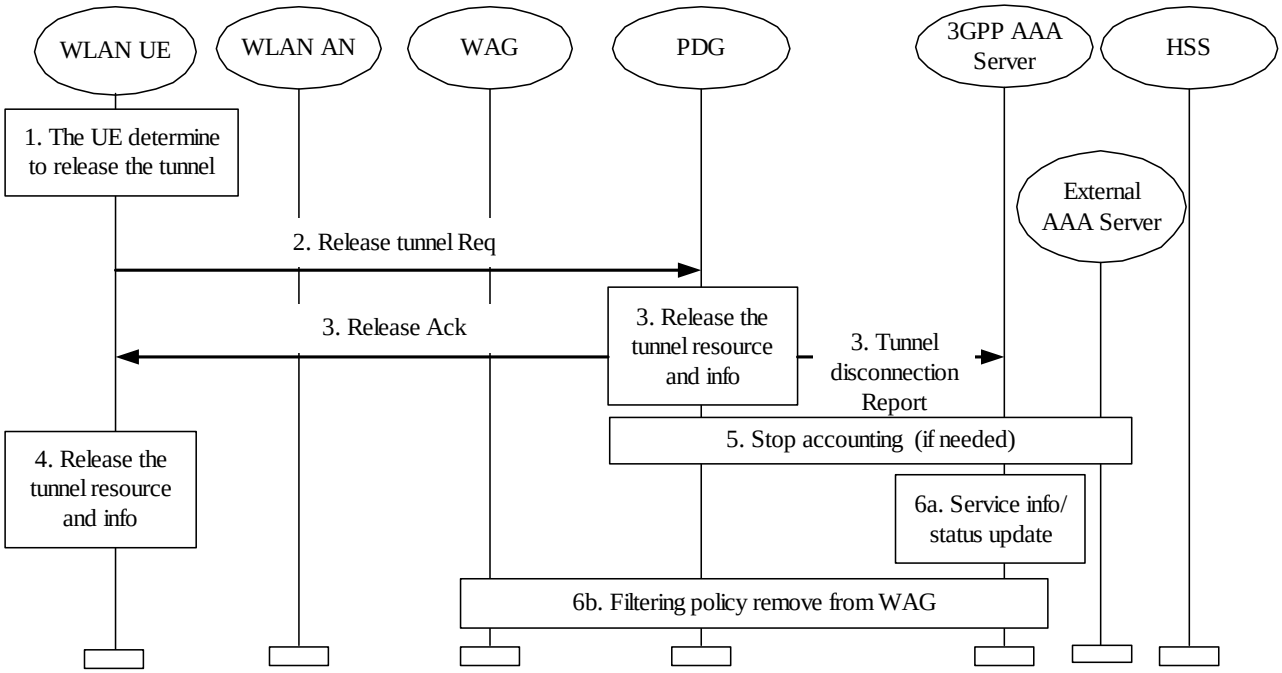


Figure 7.12: WLAN UE initiated tunnel disconnection

1. The WLAN UE determine to release the tunnel, e.g. due to the normal service termination operation.
2. The WLAN UE send a Release tunnel request to the PDG.
3. Upon receiving the Release tunnel request, the PDG sends a Release acknowledgement to the WLAN UE, releases the resources and the associated control information of the tunnel, and sends a Tunnel disconnection report to the 3GPP AAA Server.
4. Upon receiving the Release acknowledgement, the WLAN UE releases the resources and the control information of the tunnel.
5. If accounting has been started in the External AAA Server, then the PDG initiates "Accounting Stop" procedure to the External AAA Server.
6. Upon receiving the Tunnel disconnection report, the 3GPP AAA Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

7.10.2 The network initiated tunnel disconnection

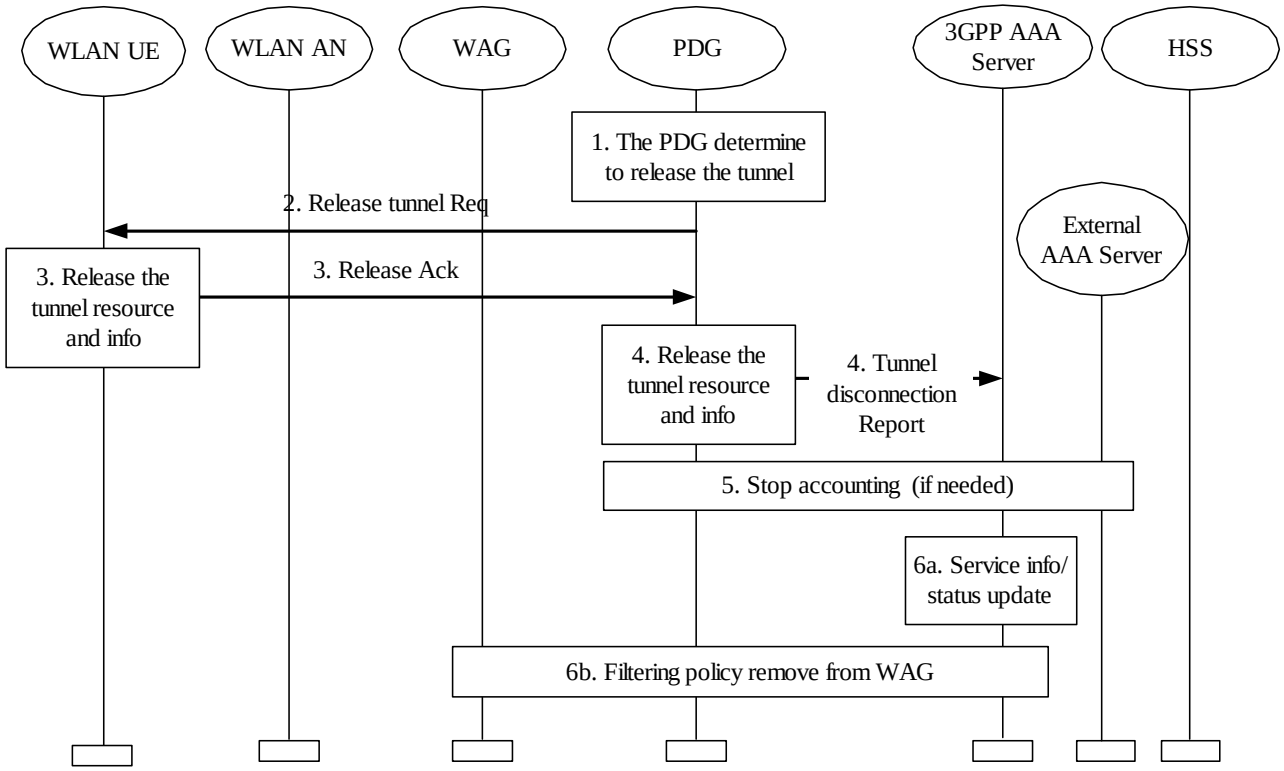


Figure 7.13: The network initiated tunnel disconnection

1. The PDG determines to release the tunnel, e.g. due to timeout of the tunnel connection or a request from the 3GPP AAA Server, or due to a network initiated normal service termination or a service termination resulting from network operator intervention.

2. The PDG sends a Release tunnel request to the WLAN UE.

3. Upon receiving the Release tunnel request, the WLAN UE releases the resources and the associated control information of the tunnel, and sends the Release acknowledgement to the PDG.

4. Upon receiving the release acknowledgement, the PDG releases the resources, the associated control information of the tunnel, and the related service authorization information; and sends a Tunnel disconnection report to the 3GPP AAA Server.

5. If accounting has been started in the External AAA Server, then the PDG initiates "Accounting Stop" procedure to the External AAA Server.

6. Upon receiving the Tunnel disconnection report, the 3GPP AAA Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

7.10.3 Disconnection of the last tunnel for a WLAN UE

If the PDG detects that the disconnected tunnel is the last tunnel between the PDG and the WLAN UE, then all the WLAN UE related authorization and profile information could be removed from the PDG during the tunnel disconnection process.

In case the 3GPP AAA Server decides to disconnect the WLAN UE from the WLAN after disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6.1 (steps 3-4).

After the WLAN UE was disconnected from the WLAN, the 3GPP AAA Server notifies the HSS using the Wx procedure "Purge" that the WLAN UE's registration in the 3GPP AAA Server has been deleted. In this case the HSS de-registers the 3GPP AAA Server (WLAN de-registration procedure).

7.11 The WLAN UE initiated WLAN AN Access disconnection

The WLAN UE may disconnect the from WLAN AN by:

- initiating a disconnection of the WLAN radio connection;
- initiating a disconnection of the WLAN IP connectivity.

Disconnection of the WLAN radio connection

Upon receiving a WLAN radio disconnection request (e.g., Disassociation in case of IEEE802.11 WLAN AN) from the WLAN UE with the WLAN access connection, the WLAN AN should perform the "disconnecting a subscriber by WLAN AN" (section 7.5) during or after the WLAN radio disconnection, with or without confirm message to the WLAN UE.

Disconnection of the WLAN IP connectivity

The UE initiated disconnection of the WLAN IP connectivity is usually performed before the disconnection of the WLAN radio connection and after the disconnection of the 3GPP PS access tunnels. However the WLAN UE may initiate a WLAN IP connectivity disconnection before the 3GPP PS access tunnels are disconnected. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

If the WLAN UE initiates a disconnection of the WLAN IP connectivity:

1. The WLAN UE may initiate a disassociation after the disconnection procedure.
2. The WLAN AN stops the connection under the request of the WLAN UE, e.g. close the opened port to the WLAN UE.
3. The WLAN AN should perform the "disconnecting a subscriber by WLAN AN" during or after the disconnection of WLAN access connection.

   The WLAN AN should initiate an authentication or a disconnection of WLAN radio connection with this WLAN UE, if the WLAN UE keeps the WLAN radio connection without subsequent indication or requests in a certain period of time.

The 3GPP PS Access tunnel disconnection

The UE initiated tunnel disconnection is usually performed before the disconnection of WLAN IP connectivity and the disconnection of the WLAN radio connection. However, the WLAN UE may directly initiate a disconnection of the WLAN radio connection as a fast disconnection option when tunnel connections with PDG exist. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

7.12 User identity to HSS resolution

7.12.1 General

This section describes the resolution mechanism, which enables the 3GPP AAA Server to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. This resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is a server farm architecture. The NAI will be used as user identifier towards the SLF.

The subscription locator is accessed via the Dw reference point. The Dw reference point is the standard interface between the 3GPP AAA Server and the SLF. The synchronisation between the SLF and the different HSSs is an O&M issue.

The subscription locator is already defined in TS 23.228 [24] for Cx and Sh interfaces.

The Dw interface provides:

- an operation to query the subscription locator from 3GPP AAA Server
- a response to provide the HSS name towards 3GPP AAA Server.

By sending the Dw-operation DW_SLF_QUERY the 3GPP AAA Server indicates a user identity of which it is looking for an HSS. By the Dw-operation DW_SLF_RESP, the SLF responds with the HSS address. The 3GPP AAA Server may optionally store the HSS address for a given subscriber so subsequent queries to the SLF are not needed.

Subclause 7.12.2 presents an example of the session flow when the 3GPP AAA Server needs to query the SLF.

7.12.2 SLF query

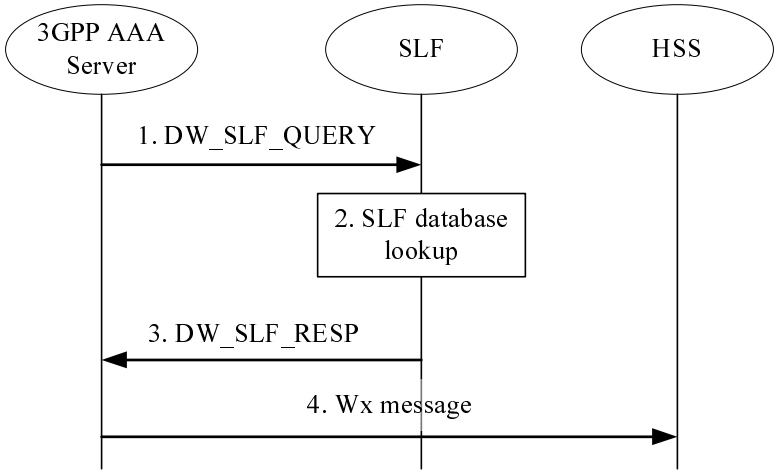


Figure 7.14: Query through SLF

1. 3GPP AAA Server detects that it requires the user profile, the registration or new authentication vectors for a given 3GPP subscriber, so has to query for the location of the user's subscription data. The 3GPP AAA Server sends a DW_SLF_QUERY to the SLF and includes as parameter the user identity of the subscriber.
2. The SLF looks up its database for the queried user identity.
3. The SLF answers with the HSS address in which the user's subscription data can be found.
4. The 3GPP AAA Server can proceed by querying the appropriate HSS by Wx protocol.

7.13 Disconnecting a Subscriber by the External AAA Server

7.13.1 The External AAA Server initiated tunnel disconnection

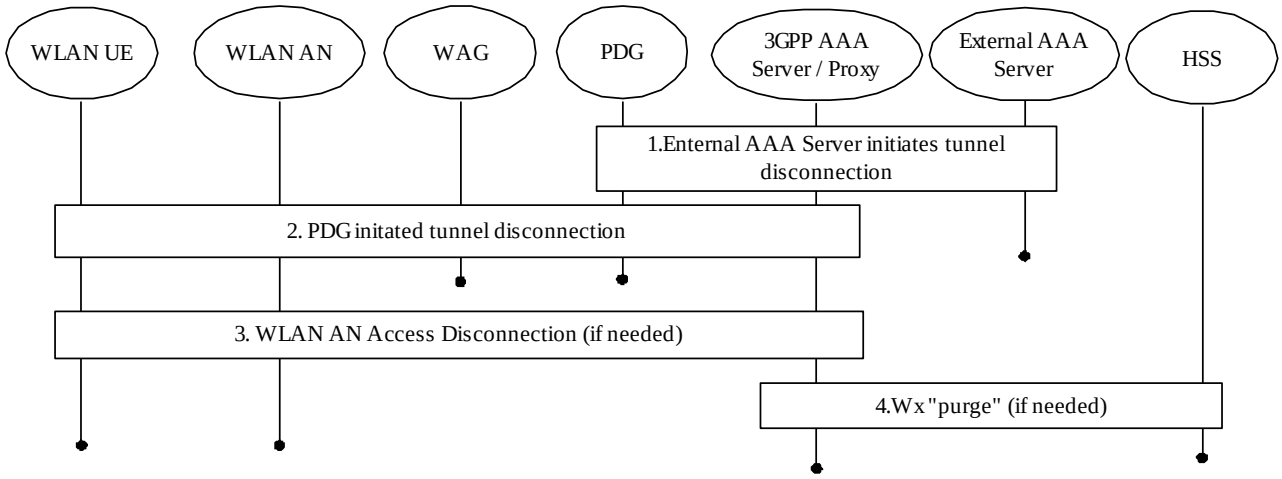


Figure 7.15: The External AAA Server initiated tunnel disconnection procedure

This section applies to the case when the tunnel disconnection is initiated by the External AAA Server.

1. Some IP applications, for example, the authorization of usage of the W-APN expired, could need to interwork with the PDG to terminate a particular session. For this purpose, the External AAA Server may initiate the tunnel disconnection.

2. The PDG disconnects the tunnels using the network initiated tunnel disconnection procedure (clause 7.10.2).

3 If all tunnels of the subscriber have been disconnected in the previous step then the 3GPP AAA Server may decide to totally disconnect the subscriber by performing "Session Abort" towards the WLAN AN (i.e. steps 3 and 4 of clause 7.6.1).

4. If the subscriber is disconnected from the WLAN AN in step 3 and no Wx "Purge" procedure was already initiated, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge".

Annex A (informative):
Void

Annex B (informative):
Void

Annex C (informative): Possible interworking architectures between WLAN AN and PLMN

C.1 WLAN shared by (or connected to) multiple ISPs and PLMNs

This is typically when a WLAN AN is owned by an independent entity such as a hotel and the owner allows subscribers of ISPs to use their WLAN AN by using the ISP network. However, WLAN AN owned by an ISP or a PLMN may also allow other ISP/PLMN subscribers to use the WLAN in a similar way.

In this situation, the WLAN AN may be connected to multiple ISPs and PLMNs in the layer 2 for WLAN 3GPP IP Access as shown in Figure C.1.1. Another solution using DNS and NAT is described in C.2.3.

To this end, VLAN or other layer 2 tunnelling capabilities may be implemented in APs or access controller in WLAN AN in order to separate traffic of different networks.

The interface between the WLAN AN and the PLMN may be a Layer 2 tunnel, such as VLAN, Martini, or VPLS, etc. The WAG takes the role of the access router of the WLAN AN. This enables end to end tunnelling for WLAN 3GPP IP Access, even when the IP address of the PDG is not routable on the Internet.

The local IP address of a WLAN UE, when using WLAN 3GPP IP Access, belongs to the PLMN's IP address space. So, all the packets to a WLAN UE shall pass through the PLMN.

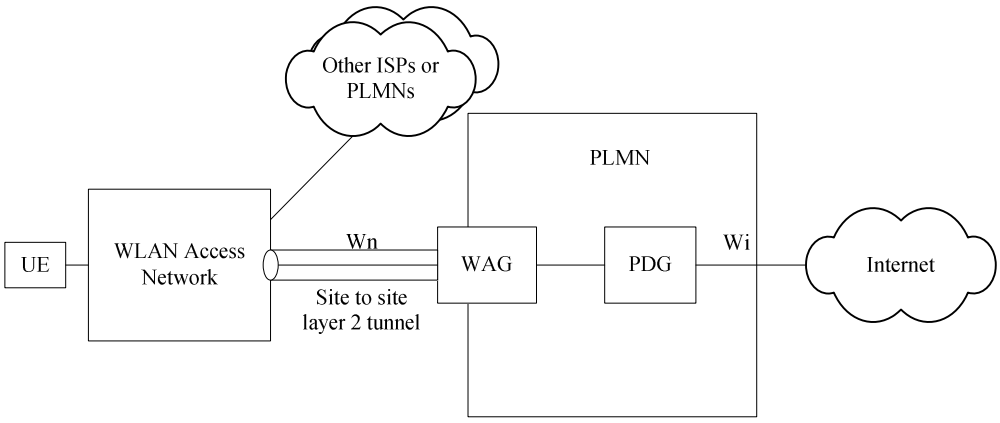


Figure C.1.1: Wn Interface when WLAN is connected to multiple ISPs and PLMNs

C.2 Routing packets from WLAN UE when WLAN AN is connected to multiple VPLMNs/ISPs and it provides direct Internet access

C.2.1 Separating traffic for different VPLMNs

When a WLAN AN providing direct Internet access has connections to multiple VPLMNs it is necessary to route all the users' non-Internet traffic to the correct VPLMN whilst Internet traffic is routed directly to the Internet. The VPLMN identity is known to the WLAN AN at initial user authentication/authorisation, since the AAA signalling is routed to that VPLMN, and the Access-Accept received from that VPLMN.

Therefore, for each VPLMN there must be a separate (logical) router in the WLAN AN which has a connection to that VPLMN and also to the Internet (note: this is a 'logical' router – it doesn't represent a restriction on WLAN AN's physical architecture). This router will receive all the traffic from WLAN UEs that are authenticated through that VPLMN. We call this the "WLAN AN Border Router for VPLMN X".

Various techniques could be used to ensure that all the WLAN UEs traffic is sent to the correct (logical) router, including:

- VLANs

  A separate VLAN is defined for each VPLMN. The WLAN AN Border Router for a given VPLMN is only accessible from that VPLMN's VLAN. Appropriate RADIUS AVPs can be used to place the user onto a particular VLAN. On receiving this instruction, the WLAN AP performs VLAN tagging of all frames from the user. Since the WLAN AN knows the identity of the correct VPLMN at initial authentication/authorisation time, this instruction can be sent to the AP at this time.

  As a result, all traffic from the user will be sent to the correct router.

- Compulsory tunnelling

  Standard RADIUS AVPs are used to request the WLAN AP to establish a compulsory tunnel for the WLAN UEs frames towards the correct router. Again, this can be done at initial authentication/authorisation time.

Other techniques may also exist, but since there is no requirement for signalling from VPLMN to WLAN AN, the technique chosen is entirely a matter for the WLAN AN operator.

C.2.2 Routing the traffic

The WLAN AN Border Router for a given VPLMN must distinguish Internet traffic (which should be sent directly to the Internet) from non-Internet traffic (i.e. packets to PDGs – which should be sent to the VPLMN).

One way to achieve this is for the WLAN AN to recognise the addresses of PDGs. Traffic to a known PDG address is routed to the VPLMN and other traffic to the Internet. There are several ways the WLAN AN could discover the PDG addresses:

- Statically – HPLMNs inform VPLMNs of their PDG addresses and VPLMNs inform WLAN ANs of these addresses together with any VPLMN PDG addresses. The addresses are statically configured in the routing tables of the WLAN AN Border Router.

- Dynamically - using standard IP routing protocols – HPLMNs must advertise routes to their PDGs across the inter-operator backbone. VPLMNs simply pass these advertisements to WLAN ANs along with advertisements of their own PDG addresses.

Configuration or advertisement of these addresses into the WLAN AN does not make these addresses routable from the Public Internet. Only users who are Authenticated and Authorised 3GPP WLAN UEs will be able to send packets to the (logical) WLAN AN Border Router, so only these devices can send packets to the configured/advertised addresses.

The above two approaches require that the addresses or prefixes configured or advertised are **not** also advertised over the public Internet. This is because although an address/prefix may be configured/advertised, there may be firewall rules or policies in the VPLMN which prevent packets being routed over the inter-operator backbone to that address. In that case, packets to that address would be dropped, meaning that any device re-using that address would not be routable at all from the WLAN UEs.

The solution is summarised in the figure below (assuming the VLAN option for dealing with multiple VPLMNs). Note that this is a logical view – the existence of two Border Routers with links to the Internet does not imply two physical elements/links.

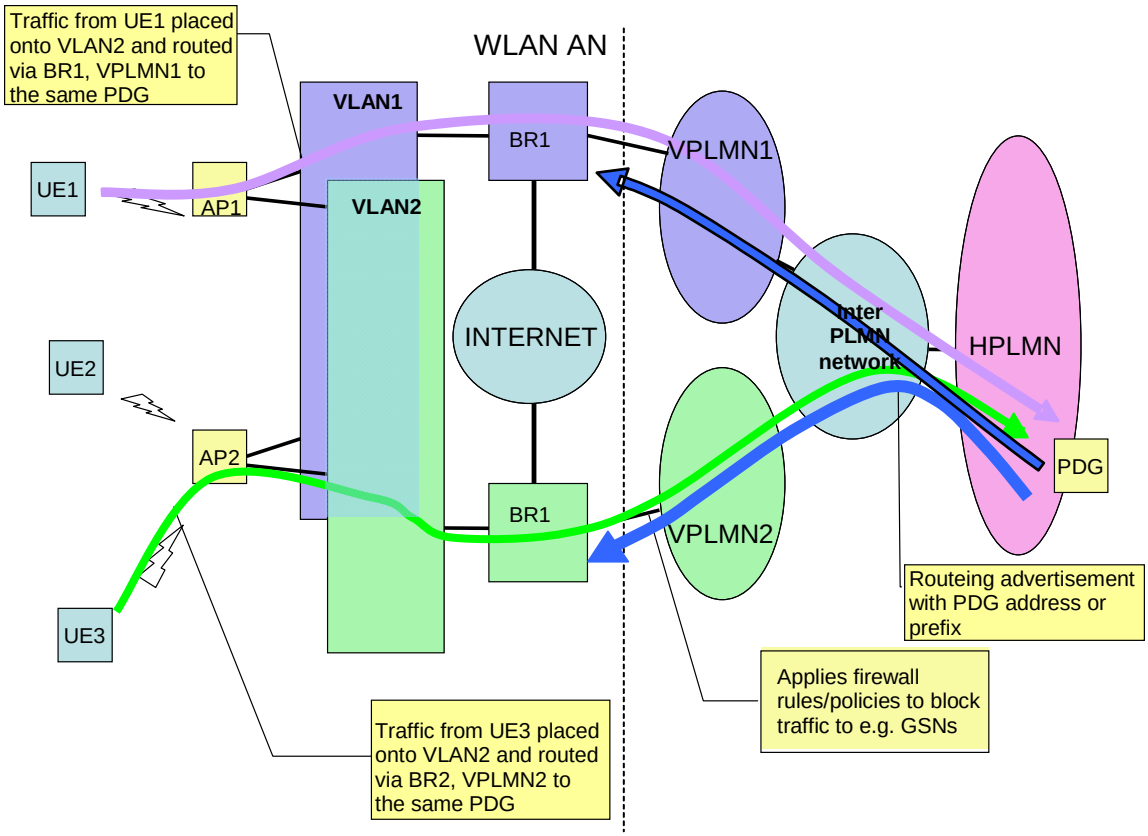


Figure C.2.1: Traffic routeing based on the use of VLANs in the WLAN AN

C.2.3 Separating traffic to different VPLMNs using a combined DNS/NAT approach

If the WLAN UE is associated to the WLAN AN and authenticated through EAP, it can access the Internet directly (for WLAN Direct IP Access) or establish a tunnel to a PDG in the VPLMN/HPLMN to access 3GPP PS based services (for WLAN 3GPP IP Access). Both cases must be enabled in parallel. The WLAN UE performs a DNS query to resolve a W-APN to a PDG address. This IP address is the tunnel endpoint in the PLMN. If the PDG resides in the HPLMN, it must be possible to route traffic to the PDG through the selected VPLMN. The combined DNS/NAT approach as described in this chapter adds no requirements to the WLAN UE and HPLMN and uses only normal IP routing capabilities in the VPLMN.

The main idea is to use some kind of "reverse NAT" in the VPLMN that maps the PDG address received in the answer to the WLAN UE's DNS request to an address out of the address range of the VPLMN. Each PDG address is mapped to one VPLMN address, which may be a private address, depending on the addresses used in the WLAN AN. For simplicity (no new protocol needed) and performance reasons the VPLMN DNS proxy and the desired reverse NAT function are implemented on the WAG. Thus, inside of the NAT is the HPLMN address space, outside is the WLAN AN address space.

As the WLAN is directly connected to the VPLMN it is aware about the VPLMN IP addresses and can easily route WLAN 3GPP IP Access traffic to the correct VPLMN. The VPLMN maps the destination address of the IP packet to the stored PDG address and forwards the packet to the HPLMN. WLAN Direct IP Access traffic goes to the default route configured in the WLAN edge router, i.e. to the Internet.

The following figure shows the process of W-APN resolution and NAT in the VPLMN. The figure shows a local DNS server in the WLAN AN while it is also possible that the WLAN UE receives the address of a DNS server in the VPLMN by DHCP or during EAP authentication. If the WLAN UE wants to access a PDG in the HPLMN, the W-APN indicates the HPLMN and optionally the VPLMN, otherwise the W-APN indicates the VPLMN only.

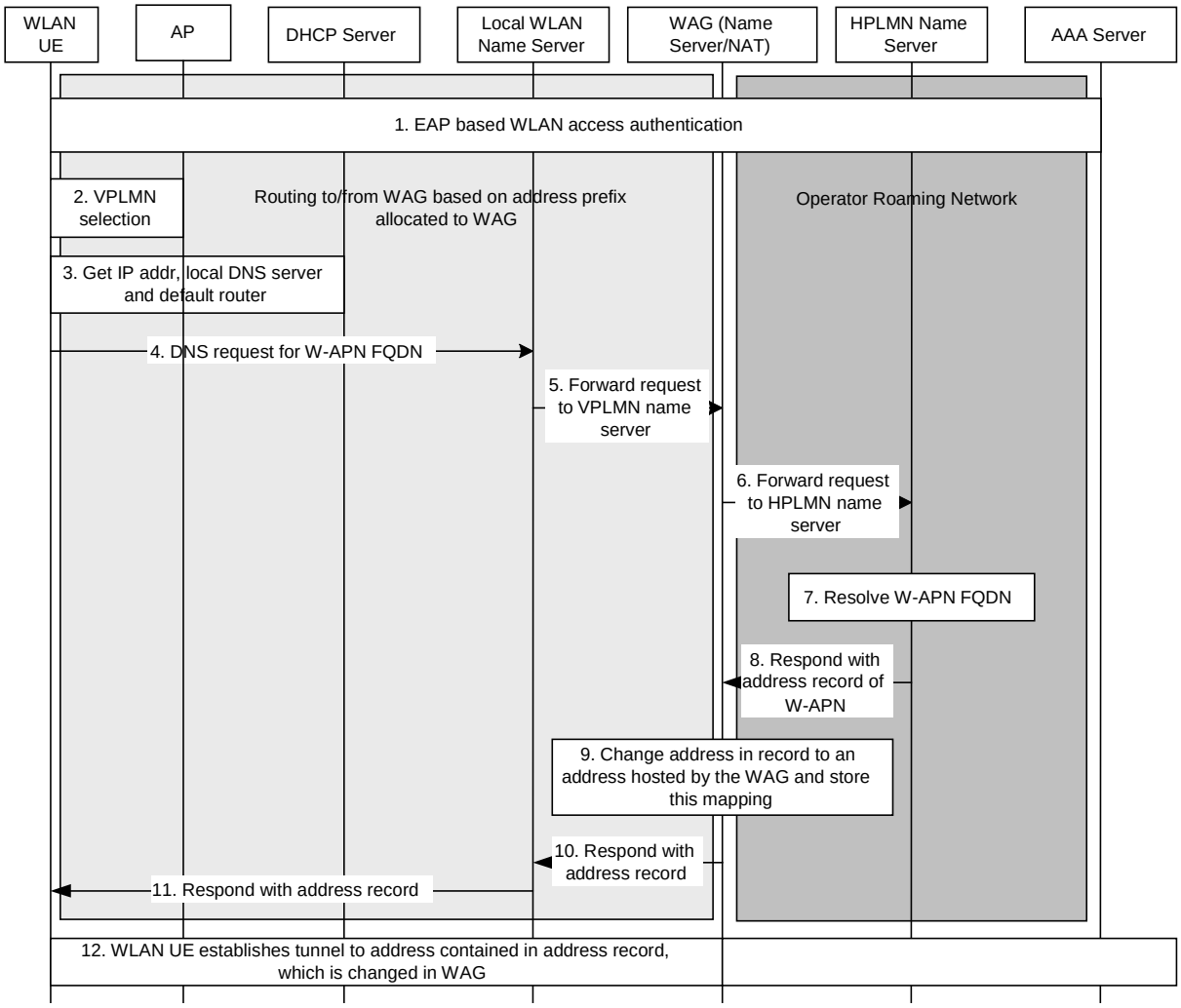


Figure C.2.2: DNS controlled reverse NAT procedure

1. WLAN access authentication procedure between WLAN UE and AAA server based on EAP.
2. WLAN UE retrieves PLMN list from WLAN and selects a preferred VPLMN.
3. WLAN UE gets transport IP address, local name server (optionally) and default router address via DHCP.
4. WLAN UE builds W-APN FQDN indicating VPLMN (optionally) and HPLMN and sends DNS request to local name server or directly to the name server in the VPLMN.
5. Local name server inspects W-APN FQDN and forwards DNS request to VPLMN name server. VPLMN name server is implemented together with a "reverse" NAT and probably a Firewall on the WAG.
6. VPLMN name server inspects W-APN FQDN and forwards DNS request to HPLMN name server through GPRS roaming network.
7. HPLMN name server resolves W-APN.
8. HPLMN name server responds to VPLMN name server with an address record of the W-APN.
9. VPLMN name server (acting as DNS Proxy) optionally changes the PDG address contained in the address record to an address of the WAG address space (this address may be a private address) and stores the mapping between the two addresses. The new address must be routable within the WLAN to the WAG. Changing the addresses may be an option configurable by the operator.
10. VPLMN name server responds the address record to local name server.
11. Local name server responds the address record to WLAN UE.

12. WLAN UE establishes tunnel to the address contained in the address record. This may be an address hosted by the WAG (otherwise it is the PDG address). This address is changed ("NATted") at the WAG to the "real" PDG address.

C.3 WLAN AN exclusively owned by and connected to a single PLMN

This is when a PLMN operator installs its own WLAN AN without any connections to other ISPs or PLMNs.

In this case, WLAN AN can be regarded as an extension of the PLMN's IP network and no tunnel is required between WLAN AN and PLMN. The local IP address of a WLAN UE in WLAN 3GPP IP Access belongs to the PLMN's IP address space.

C.4 WLAN AN connected to a single ISP

This is when WLAN AN is solely connected to an ISP's backbone network. WLAN AN is regarded as an extension of the ISP's backbone network. Many legacy WLAN ANs can be categorized to this case

The connectivity between the WLAN AN and the PLMN is in layer 3 through the ISP's backbone network as shown in figure C.4.1.

This kind of WLAN AN supports WLAN Direct IP Access as defined in the TS 23.234, i.e. the authenticated WLAN UE can access the Internet directly via the ISP.

For WLAN 3GPP IP Access, the local IP address of a WLAN UE is generally allocated by the ISP and it belongs to the ISP's IP address space. When PLMN allocates WLAN UE's local IP address, a layer 2 tunnel is required.

When the end to end tunnelling is used between a WLAN UE and a PDG and the IP address of the PDG is non-routable in the Internet, an additional means is required for routing the packets to the PDG and to meet the routing enforcement requirement.

It is FFS for methods to enable WLAN 3GPP IP Access for this kind of WLAN AN.

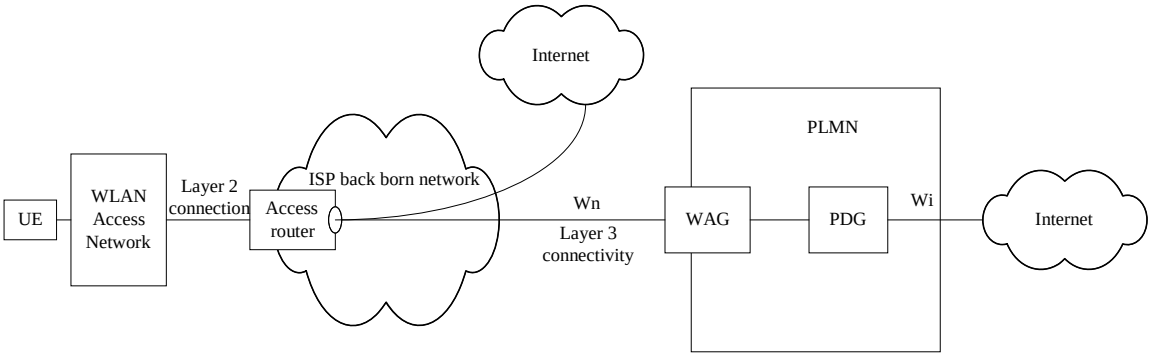


Figure C.4.1: Wn Interface when WLAN is connected to a PLMN through an ISP

Annex D (normative): Short Message Service

D.1 Architecture for support of SMS

The architecture for support of IP delivery of SMS messages is specified in TS 23.204 [39].

D.2 Void

D.3 Void

Annex E (informative):
Void

Annex F (normative): Information on re-using the GGSN to implement the PDG function

This annex does not introduce new normative requirements for the PDG.

F.1 Introduction

This section provides information on how to re-use existing GGSN deployments to implement the PDG functionality via using a subset of the Gn reference point (denoted here as Gn'). The Gn' reference point provides means where GPRS mobile operators can reuse existing infrastructure and functionality for a user accessing from a WLAN UE. By using this existing standardized reference point, interoperability towards the Gateway GPRS Support Nodes (GGSN) is assured. Such a PDG implementation allows re-use of existing GGSN functionality without upgrading GGSNs. For example, GGSN functions, which are used in this case are:

- Charging Gateway interfaces;
- IP address allocation;
- Authentication in external networks;
- Single access to 3GPP PS domain services.

Traffic Plane Functionality in the GGSN for online and offline service data flow charging (IP flow level bearer charging introduced in Rel-6, Policy and Charging Enforcement Function (PCEF) in Rel-7), may also be re-used.

If QoS mechanisms are applied policy control functionality (e.g. service based QoS control or gating) according to TS 23.203 [36] may be re-used.

The following figure depicts a PDG implementation that re-uses GGSN functionality. It shall be noted that only a subset of the GGSN is reused for this purpose.

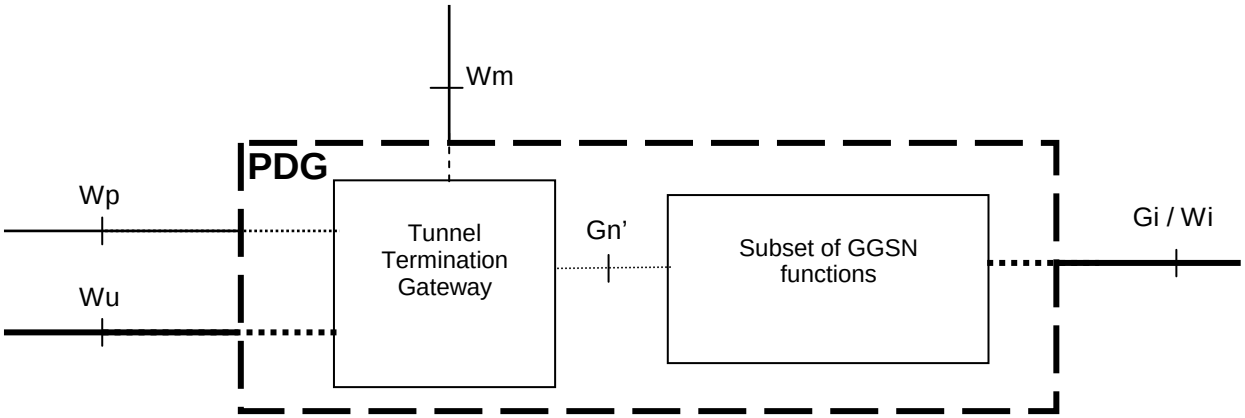


Figure F.1: PDG implementation re-using GGSN functionality

The PDG functionality described in this specification may be implemented using the architecture described above in Figure F.1. In case this implementation is applied, the TTG and GGSN parts of the PDG shall be in the same PLMN. This type of PDG implementation shall remain transparent to the other functional elements of the network.

F.2 Mapping between E2E tunnel and GTP tunnel

F.2.1 General

The end-to-end tunnel between the WLAN UE and the PDG is setup according to the procedure described in this specification. In a configuration when the Gn' reference point is used, the end-to-end tunnel setup is terminated by the TTG of the PDG, and the setup of GTP tunnel(s) is triggered towards the GGSN part of the PDG. The GTP tunnel(s) between the TTG part and the GGSN part of the PDG are established using the two messages Create PDP Context Request and Create PDP Context Response. A GTP tunnel is identified in each node with a TEID (Tunnel End-point Identifier - an integer), an IP address and a UDP port.

The W-APN provided over the end-to-end tunnel shall be forwarded in the Create PDP Context Request message to the GGSN to select the external network.

The IMSI of the WLAN UE shall be forwarded to the GGSN in the Create PDP Context Request message.

For further details on GTP tunnel management please refer to TS 29.060 [28].

F.2.2 No re-use of policy control functionality in the GGSN

Each end-to-end tunnel is mapped one-to-one to a GTP tunnel.

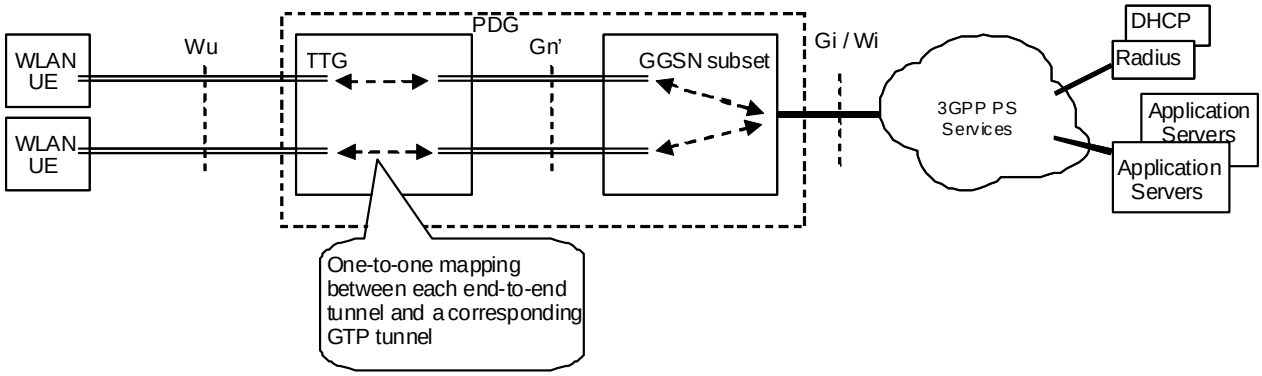


Figure F.2.2: Mapping between E2E tunnel and a single GTP tunnel

F.2.3 Re-use of policy control functionality in the GGSN

F.2.3.1 Usage of DiffServ marking of the GTP tunnel

The GGSN may have the additional capability to put a policed DiffServ marking onto the GTP IP header, based on the DSCP marking of the received DL IP packet and the applied policy. In this case no additional secondary PDP contexts are needed.

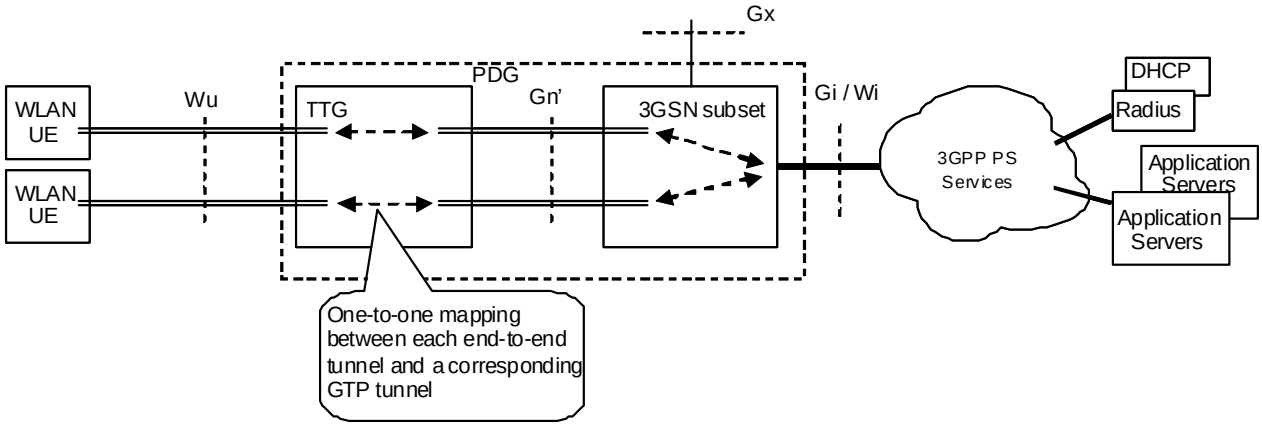


Figure F.2.3.1: Mapping between E2E tunnel and a single GTP tunnel

F.2.3.2 Usage of QoS profile of the GTP tunnels

Each end-to-end tunnel is mapped to one primary and multiple secondary GTP tunnels (one per allowed DSCP of the user's 3GPP WLAN QoS profile). The secondary PDP-context activation may be either network-initiated, or TTG initiated (where the TTG acts as MS). Network initiated secondary PDP context activation takes place if enabled in the TTG and also the GGSN supports it. In case of TTG initiated secondary PDP-context activation the TTG initiates a secondary PDP-context for each allowed DSCP of the user's 3GPP WLAN QoS profile at the time of end-to-end tunnel setup. The TFTs for these secondary PDP contexts are statically configured in the TTG.

The TFTs statically configured in the TTG shall only use DSCP as filtering criteria to allow the selection of the appropriate PDP context by the TTG. There shall be one PDP context without TFT to be able to transfer packets in case the DSCP marking of an incoming packet does not match to any TFT.

NOTE: The GGSN may apply DiffServ edge control functions of uplink IP packets which may result in re-classification (re-marking the DSCP) or discarding of IP packets.

The end-to-end tunnel is released by the TTG when the last active GTP tunnel to the GGSN is released.

In the DL direction the correct GTP tunnel is selected based on the active predefined PCC rules.

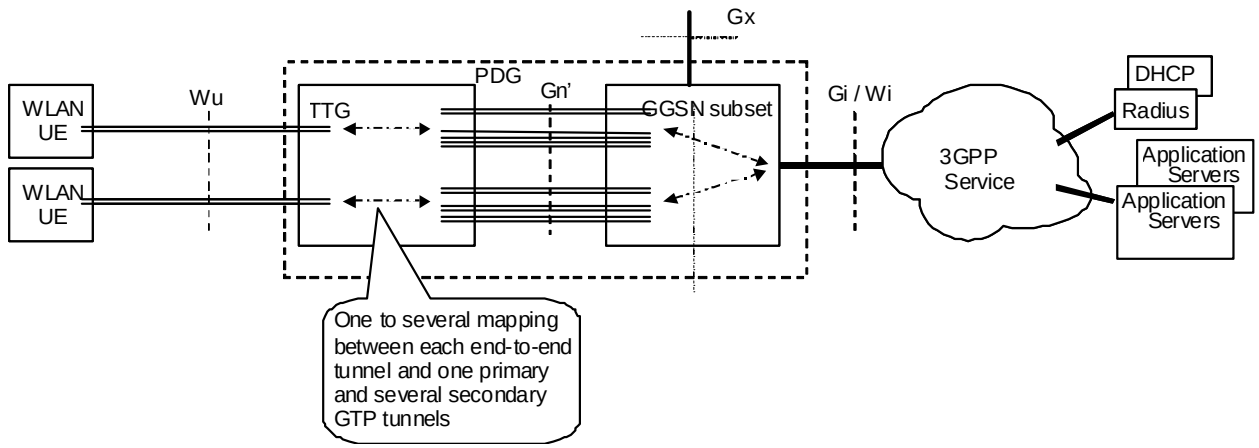


Figure F.2.3.2: Mapping between E2E tunnel and one primary and several secondary GTP tunnel(s)

F.3 Gn' considerations

Editor's note: The Gn' procedures shall comprise a subset of the Gn reference point procedures. There shall be no enhancements to Gn applied.

F.3.0 General

A minimum set of interworking procedures over the Gn' reference point would include the following messages from the Gn reference point messages and procedures specified in TS 29.060 [28]:

- Create PDP Context Request / Response;
- Update PDP Context Request / Response;
- Delete PDP Context Request / Response;
- Error Indication;
- Version Not Supported;
- GTP Payload Forwarding.

The TTG must be provided with information, e.g. MCC and MNC of the VPLMN, needed to include the RAI Information Element within the messaging to the GGSN to enable simple position based billing and to enable the HPLMN to restrict certain content to those countries depending on that country's legal requirements.

The assignment of the remote IP address should be done from a pool of IP address belonging to the GGSN/RADIUS server or at least "address range coordinated" with those to enable correct routing on Gi. The End-user-address IE must be provided in the Create PDP Context Request. If address assignment is done by the GGSN/RADIUS, the IE shall be empty in the request message (indicating dynamic address assignment by GGSN/RADIUS), which makes the GGSN/RADIUS assign and return an IP address in the Response message.

The NSAPI value to be provided over the Gn' reference point is allocated in the TTG, see subclause F.5.

If a certain charging profile should be applied in GGSN the Charging Characteristics IE may be included. In that case this information needs to be available in the TTG. The Charging Characteristics may be used to give special charging for WLAN in the GGSN. The Charging Characteristic is defined per subscriber and is stored in HLR. For GPRS the Charging Characteristic is sent to SGSN at attach and is forwarded to GGSN at PDP context creation. For WLAN interworking, the TTG may for example get this information from HLR via the 3GPP AAA Server.

F.3.1 Interworking procedure over Gn' - Tunnel establishment procedure

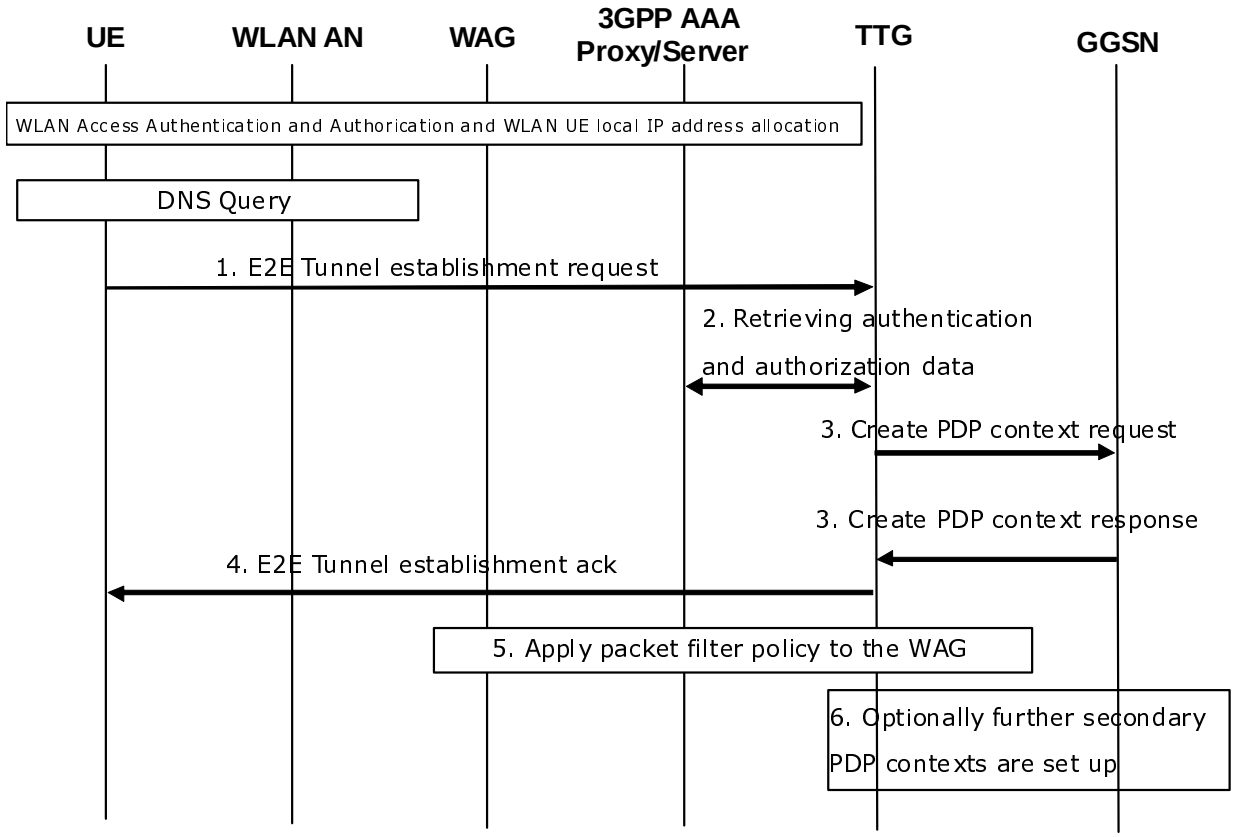


Figure F.3.1: Tunnel establishment procedure

1) The UE performs a DNS query to resolve the W-APN and sends E2E tunnel establishment request (W-APN, user identity) to the TTG (see subclause 7.9).

2) The TTG contacts the 3GPP AAA Server in the HPLMN possibly via the AAA proxy for authorization and authentication of the WLAN UE (see subclause 7.9). Additionally, the TTG retrieves the IMSI, MSISDN, and serving network identity from the AAA server.

3) The TTG performs PDP Context Activation procedure towards the GGSN by using Create PDP Context Request message and Create PDP Context Response message (see TS 23.060 [7]).

4) The TTG returns E2E tunnel establishment acknowledgement (remote IP address) to the WLAN UE.

5) The TTG provides filtering information to the WAG (see subclause 7.9).

6) If policy control functionality in the GGSN is re-used according to clause F.2.3.2 further secondary PDP contexts are established.

F.3.2 Interworking procedure over Gn' - Tunnel disconnection procedure

F.3.2.1 UE initiated tunnel disconnection

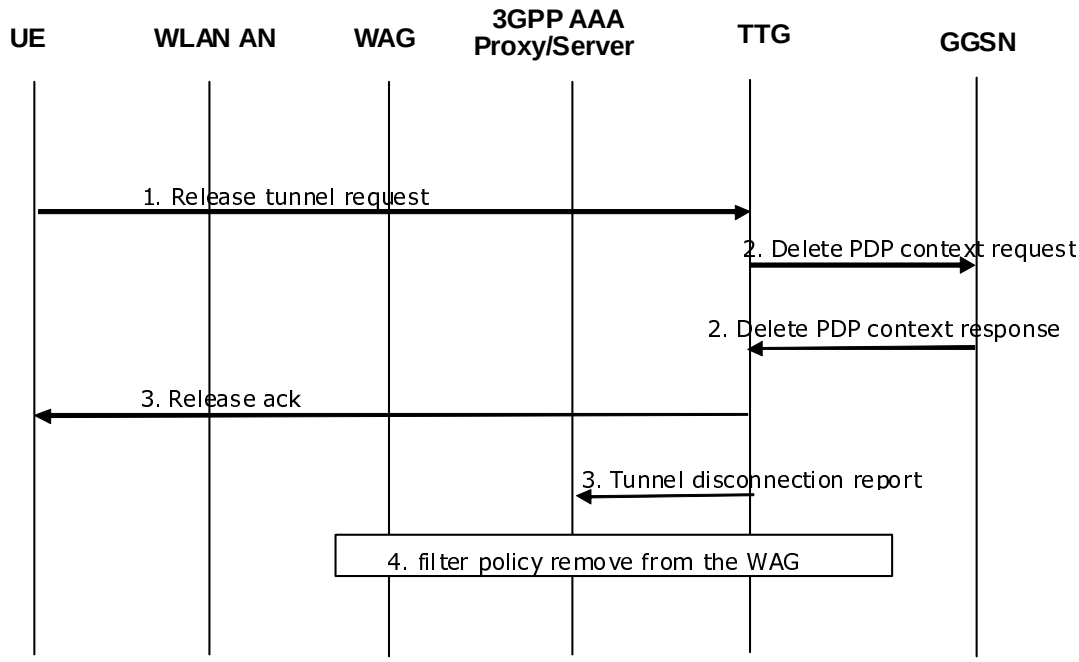


Figure F.3.2.1: UE initiated tunnel disconnection procedure

1) The WLAN UE determines to release the tunnel and sends a Release tunnel request to the TTG (see subclause 7.10.1).

2) Upon receiving the Release tunnel request, the TTG performs PDP Context Deactivation procedure for the primary and possibly established secondary PDP contexts towards the GGSN by using Delete PDP Context Request message and Delete PDP Context Response message (see TS 23.060 [7]).

3) The TTG sends a Release acknowledgement to the WLAN UE and Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.1).

4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.1).

F.3.2.2 Network initiated tunnel disconnection

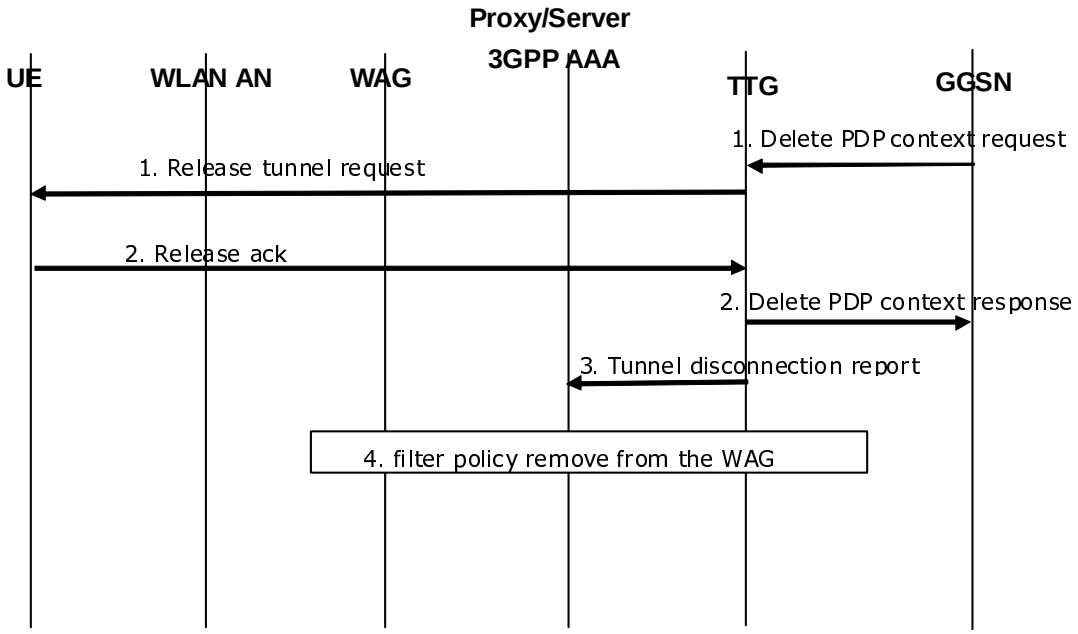


Figure F.3.2.2: Network initiated tunnel disconnection procedure

1) The GGSN determines to release the last active GTP tunnel and sends Delete PDP Context Request message towards the TTG (see TS 23.060 [7]). The TTG then sends a Release tunnel request to the WLAN UE (see subclause 7.10.2).

2) Upon receiving the Release tunnel request, the WLAN UE sends a Release acknowledgement to the TTG (see subclause 7.10.2). The TTG sends a Delete PDP Context Response message to the GGSN (see TS 23.060 [7]).

3) The TTG sends a Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.2).

4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.2).

NOTE: Network initiated tunnel disconnection procedure may also be triggered by the TTG (e.g. request from AAA server).

F.4 Void

F.5 Tunnel Terminating Gateway (TTG) functionality

The functionality of the TTG shall cover all aspects of the PDG that are not covered by the GGSN.

The TTG shall be responsible for allocating NSAPI values before sending the Create PDP Context Request message to the GGSN. Although the TTG acts like the SGSN in terms of GTP tunnel establishment, it also manages NSAPI allocation as WLAN UE's proxy for the purpose of leaving the Gn' based PDG transparent to the WLAN UE.

If the network supports simultaneous GPRS and WLAN connections, the TTG shall ensure that the NSAPI values allocated do not overlap with those used by the UE for GPRS PDP Contexts.

NOTE: This can be achieved by restricting TTG allocated NSAPI values to those which are reserved on the mobile radio layer 3 interface in this case.

The TTG shall reject a tunnel establishment request if all available NSAPI values for this user in this GGSN have already been allocated. However, the TTG should not explicitly indicate the exhaustion of the NSAPI values to the UE in such a case.

NOTE: The mechanism above implies that it may not be possible to deploy distinct TTGs providing service for a single user for W-APNs which are then served from the same GGSNs. For a given user, all tunnels towards W-APNs served from the same GGSNs should be directed to the same TTG; the method by which this will be done is FFS.

Annex G:
Void

Annex H (informative): Work in other bodies

H.1 QoS Mapping

IEEE 802.11 WLAN ANs Wi-FiTM Alliance's WMM guidelines provide a mapping from IEEE 802.11e QoS priority categories to 802.1D priority levels. This mechanism is shown in Figure H.1. See Annex H for further details on these specifications.

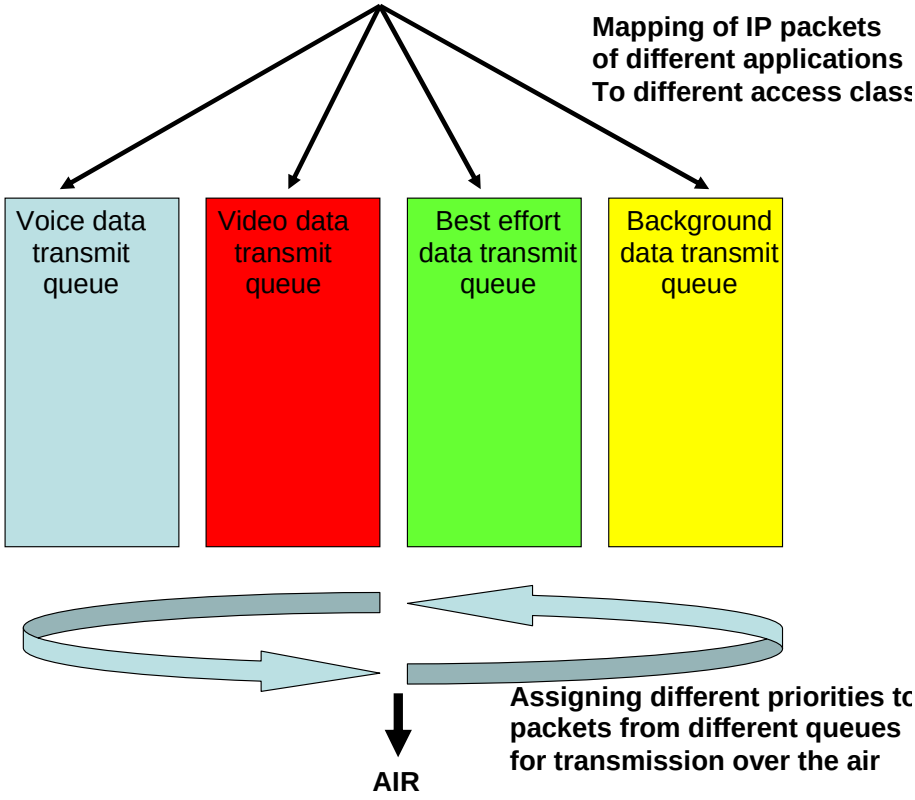


Figure H.1: QoS Mapping

Once the QoS provisioning has been accomplished during the authentication phase, based on the information included in Table 1 and Table 2 of Annex H, it is possible to map different types of traffic from the home network to DiffServ Code Points (DSCPs) and then onwards to IEEE 802.11e classes and IEEE 802.1D tags in the WLAN AN. Similarly the WLAN UE can appropriately mark the traffic in the reverse direction.

The provisioned WLAN QoS profile may include for example information on bandwidth and maximum DSCP allowed for the user. The point of enforcement of bandwidth and maximum DSCP policies within the 3GPP system is the PDG. The WLAN Access Gateway in the WLAN AN can implement similar enforcement. The entities responsible for proper DSCP marking are the end points of the tunnel (namely the WLAN UE and the PDG). If there is an inconsistent marking of QoS request from the WLAN UE between layer 2 and layer 3 (for fraudulent reasons or due to error), the inconsistency is resolved in the favour of layer 3 marking. once the packet enters the 3GPP system.

H.2 WMM specifications from Wi-FiTM Alliance

WMM defined by Wi-Fi™ Alliance, is a profile based on IEEE 802.11e draft specifications. WMM provides support for multimedia applications by defining four access categories derived from 802.1D specifications. These access categories as shown in the following table H.1, map to priority levels in 802.1D specifications of IEEE.

Table H.1: Mapping of WMM access categories and 802.1d tags

Access Category	802.1d Tags
WMM Voice Priority	7,6
WMM Video Priority	5,4
WMM Best Effort Priority	0,3
WMM Background Priority	2,1

H.3 802.1D specifications from IEEE

The IEEE 802.1D specification is the IEEE standard for bridges that also addresses how to prioritise different classes of user traffic at layer 2. Section 6.4 of 802.1D specifications provide the following definition of user priority:

> *"The user_priority parameter is the priority requested by the originating service user. The value of this parameter is in the range 0 through 7.*

NOTE: The default user_priority value is 0. Values 1 through 7 form an ordered sequence of user_priorities, with 1 being the lowest value and 7 the highest. See 7.7.3 and Annex G (informative) for further explanation of the use of user_priority values."

Annex H in 802.1D specifications provide traffic class mapping as shown in the following table H.2:

Table H.2: Traffic class mapping according to the number of queues

Number of queues in the system	Types/classes of traffic supported by the queues
1	{Best Effort, Excellent effort, Background, Voice, Controlled Load, Video, Network Control}
2	{Best Effort, Excellent effort, Background} {Voice, Controlled Load, Video, Network Control}
3	{Best Effort, Excellent effort, Background} {Controlled Load, Video} {Voice, Network Control}
4	{Background} {Best Effort, Excellent effort} {Controlled Load, Video} {Voice, Network Control}
5	{Background} {Best Effort, Excellent effort} {Controlled Load} {Video} {Voice, Network Control}
6	{Background} {Best Effort} {Excellent effort} {Controlled Load} {Video} {Voice, Network Control}
7	{Background} {Best Effort} {Excellent effort} {Controlled Load} {Video} {Voice} {Network Control}

H.4 IR 34 specifications from GSMA

GSMA's IREG 34 is a specification for the GRX. It also describes how DiffServ's bits are interpreted by the inter PLMN backbone (GRX). Table H.3 shows this mapping.

Table H.3: QoS mapping in GRX

3GPP QoS Information		Diffserv PHB	DSCP	QoS Requirement on GRX				Service Example
Traffic Class	THP			Max Delay	Max Jitter	Packet Loss	SDU Error Ratio	
Conversational	N/A	EF	101110	20ms	5ms	0.5%	10^{-6}	VoIP, Video Conferencing
Streaming	N/A	$AF4_1$	100010	40ms	5ms	0.5%	10^{-6}	Audio/Video Streaming
Interactive	1	$AF3_1$	011010	250ms	N/A	0.1%	10^{-8}	Transactional Services
	2	$AF2_1$	010010	300ms	N/A	0.1%	10^{-8}	Web Browsing
	3	$AF1_1$	001010	350ms	N/A	0.1%	10^{-8}	Telnet
Background	N/A	BE	000000	400ms	N/A	0.1%	10^{-8}	E-mail Download

Annex I (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2005-12	SA #30	SP-050672	0141	2		Technical requirements for private network access from WLAN 3GPP IP Access	6.7.0	7.0.0
2006-03	SA #31	SP-060134	0142	3		Procedures for the private network access from WLAN 3GPP IP Access	7.0.0	7.1.0
2006-03	SA #31	SP-060123	0144	2		Correction of some references	7.0.0	7.1.0
2006-03	SA #31	SP-060134	0145	-		PAP authentication capability supporting for I-WLAN Private Network Access	7.0.0	7.1.0
2006-03	SA #31	SP-060123	0150	1		Update of references	7.0.0	7.1.0
2006-06	SA #32	SP-060276	0151	4		QoS and Policy Aspect for Interworking WLAN	7.1.0	7.2.0
2006-06	SA #32	SP-060285	0152	-		Update the IETF reference	7.1.0	7.2.0
2006-06	SA #32	SP-060276	0153	2		Adjustment needed on Ww Reference Point to be in phase with updated scope	7.1.0	7.2.0
2006-09	SA #33	SP-060570	0155	1	F	Annex D Short Message Service Correction	7.2.0	7.3.0
2006-09	SA #33	SP-060584	0156	3	B	Inclusion of QoS Support for WLAN 3GPP IP Access	7.2.0	7.3.0
2006-09	SA #33	SP-060570	0158	1	A	Correction on functions of Wd	7.2.0	7.3.0
2006-09	SA #33	SP-060656	0159	2	C	Addition of details of IMS emergency call functionality to the I-WLAN procedures	7.2.0	7.3.0
2006-09	SA #33	SP-060579	0160	1	C	Addition of requirements text to support of IMS Emergency Call functionality	7.2.0	7.3.0
2006-12	SA #34	SP-060832	0162	3	F	Corrections related to QoS and Policy Aspect for Interworking WLAN	7.3.0	7.4.0
2007-03	SA #35	SP-070099	0165	2	F	Update reference	7.4.0	7.5.0
2007-12	SA #38	SP-070805	0166	4	F	I-WLAN Off-line Charging	7.5.0	7.6.0
2008-06	SA #40	SP-080390	0171	2	F	Assignement of remote IP address for the WLAN UE and binding with the local IP address at the PDG	7.6.0	7.7.0
2008-12	SA #42	-	-	-	-	Update to Rel-8 version (MCC)	7.7.0	8.0.0
2009-12	SA #46	-	-	-	-	Update to Rel-9 version (MCC)	8.0.0	9.0.0
2011-03	SA#51	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	**11.0.0**
2014-09	SA#65	SP-140426	0172	2	C	I-WLAN maintenance	11.0.0	**12.0.0**

History

Document history		
V12.0.0	September 2014	Publication