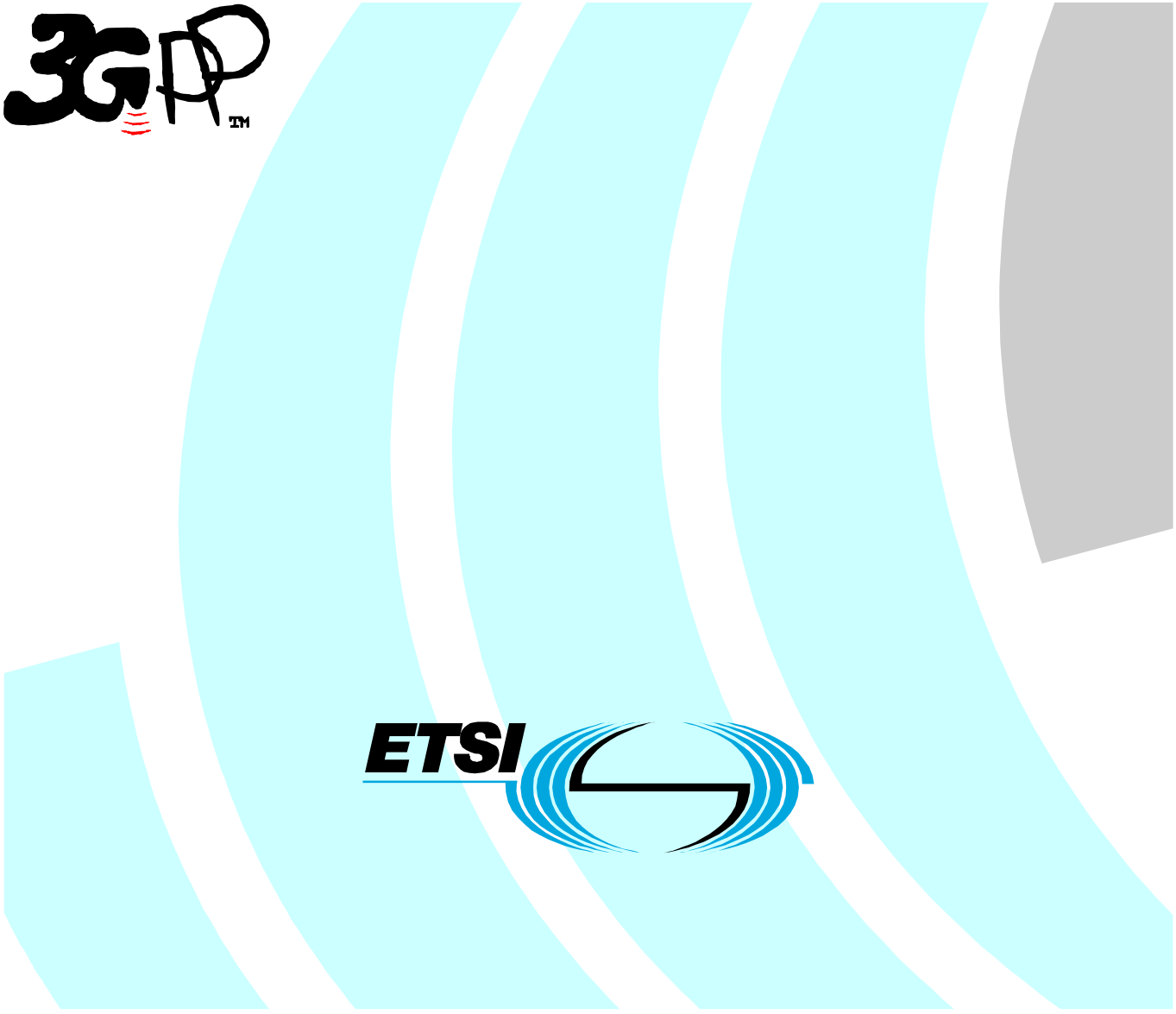
ETSI TS 129 161 V7.2.0 (2007-03)

Technical Specification

**Universal Mobile Telecommunications System (UMTS);
Interworking between the Public Land Mobile Network (PLMN)
supporting packet based services with
Wireless Local Area Network (WLAN) access
and Packet data Networks (PDNs)
(3GPP TS 29.161 version 7.2.0 Release 7)**



Reference
RTS/TSGC-0329161v720

Keywords
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://webapp.etsi.org/IPR/home.asp).

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.

Contents

Foreword

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

The present document describes the network interworking for the Packet Domain. Interworking to various external networks is defined together with the interworking for data forwarding while subscribers roam within the 3GPP system.

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

The present document defines the requirements for Packet Domain interworking between a:

a) PLMN with WLAN access and PDN;

b) PLMN with WLAN access and PLMN.

The present document also defines, in clause 12, the usage of Radius at the Pp Reference Point between the Packet Data Gateway and the Presence Network Agent, see 3GPP TS 23.141 [18].

2 References

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

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

[1] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[2] 3GPP TS 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[3] 3GPP TS 24.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

[4] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[5] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[6] IETF RFC 1034 (1987): "Domain names - concepts and facilities".

[7] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[8] IETF RFC 2131 (1997): "Dynamic Host Configuration Protocol".

[9] IETF RFC 3315 (2003) "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[10] IETF RFC 2865 (2000): "Remote Authentication Dial In User Service (RADIUS)".

[11] IETF RFC 3162 (2001): "RADIUS and IPv6".

[12] IETF RFC 2866 (2000): "RADIUS Accounting".

[13] IETF RFC 2373 (1998): "IP Version 6 Addressing Architecture".

[14] IETF RFC 2461 (1998): "Neighbor Discovery for IP Version 6 (IPv6)".

[15] IETF RFC 2462 (1998): "IPv6 Stateless Address Autoconfiguration".

[16] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[17] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[18] 3GPP TS 23.141: "Presence Service; Architecture and functional description".

[19] IETF RFC 4739, (2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[20] IETF RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[21] IETF RFC 4005 (2005): "Diameter Network Access Server Application".

[22] IETF RFC 3588 "Diameter Base Protocol".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.234 [1] and the following apply:

3GPP - WLAN Interworking: used generically to refer to interworking between the 3GPP system and the WLAN family of standards

interworking WLAN: WLAN that interworks with a 3GPP system

Serving WLAN: interworking WLAN that the user is connected to, i.e. either a visited or a home WLAN

Visited WLAN: interworking WLAN that Interworks only with a visited PLMN

WLAN UE: UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [5] and the following apply:

APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
I-WLAN	Interworked / interworking WLAN
LAN	Local Area Network
MTU	Maximum Transfer Unit
PDG	Packet Data Gateway
PDN	Packet Data Network
PPP	Point-to-Point Protocol
PS	Packet Switched
RADIUS	Remote Authentication Dial In User Service
TCP	Transmission Control Protocol
W-APN	WLAN APN
WLAN	Wireless Local Area Network

3.3 Symbols

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

Wi	Reference point between a Packet Data Gateway and an external IP Network
Pp	Reference point between a Packet Data Gateway and a Presence Network Agent

4 Network characteristics

4.1 Key characteristics of PLMN

The PLMN is fully defined in the 3GPP technical specifications. The key characteristics of 3GPP - WLAN Interworking are found in 3GPP TS 23.234 [1].

4.2 Key characteristics of IP Networks

Refer to 3GPP TS 29.061 [4].

5 Interworking classifications

Refer to 3GPP TS 29.061 [4].

6 Access reference configuration

Refer to scenario 3 in the clause Interworking Architecture in 3GPP TS 23.234 [1].

7 Subscription checking

Subscription is checked during the WLAN attach procedure and at the tunnel establishment as described in 3GPP TS 23.234 [1].

8 Interworking with PDN (IP)

NOTE: The application of procedures in this subclause is not recommended if user authentication and authorisation with AAA server is required because of the following reason: In order to perform RADIUS Authentication, the user ID and password information have to be passed from WLAN UE to PDG. However, this function is missing in the IKEv2 protocol that 3GPP TS 33.234 [16] refers in this release. In addition, user authentication and authorisation with AAA server will be standardised in release 7.

8.1 General

Packet Domain with the 3GPP - WLAN Interworking access shall support interworking with networks based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

8.2 PDN Interworking Model

When interworking with the IP networks, the Packet Domain with the 3GPP - WLAN Interworking access can operate IPv4 or IPv6. The interworking point with IP networks is at the Wi reference point, refer to scenario 3 in the clause Interworking Architecture in 3GPP TS 23.234 [1].

The PDG for interworking with the IP network is the access point of the Packet Domain. In this case the Packet Domain network will look like any other IP network or subnetwork.

Typically in the IP networks, the interworking with subnetworks is done via IP routers. The Wi reference point is between the PDG and the external IP network. From the external IP network's point of view, the PDG is seen as a normal IP router. The L2 and L1 layers are operator specific.

It is out of the scope of the present document to standardize the router functions and the used protocols in the Wi reference point.

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

No user data or header compression is done in the PDG.

8.2.1 Access to Internet, Intranet or ISP through Packet Domain

The access to Internet, Intranet or ISP may involve specific functions such as user authentication, user's authorization, end to end encryption between the UE and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, IPv6 address autoconfiguration, etc.

For this purpose the Packet Domain may offer:

- either direct transparent access to the Internet; or
- a non-transparent access to the Intranet/ISP. In this case the Packet Domain, i.e. the PDG, takes part in the functions listed above.

8.2.1.1 Transparent access to the Internet

The WLAN UE is given an IPv4 address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix is given either at subscription in which case it is a static address or at the WLAN session authorization in which case it is a dynamic address. This address or IPv6 Prefix is used for packet forwarding between the Internet and the PDG and within the packet domain. With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the terminal. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per W-APN.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a bearer service for a tunnel to a private Intranet. For details of this specific case, refer to 3GPP TS 29.061 [4], subclause "Transparent access to the Internet".

8.2.1.2 IPv4 Non Transparent access to an Intranet or ISP

The WLAN UE is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at the WLAN session authorization in which case it is a dynamic address. This address is used for packet forwarding within the PDG and for packet forwarding on the Intranet/ISP. This requires a link between the PDG and an address allocation server, like AAA or DHCP belonging to the Intranet/ISP.

Access to the ISP/Intranet may require the authentication and authorization with the External AAA Server. The PDG may 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 autorisation with the 3GPP AAA Server. Details on the multiple authentications are specified in IETF RFC 4739 [19]. Whether or not multiple authentications and authorizations are required is configured on a W-APN basis in the PDG.

If the UE requests an IP address from a DHCP server, refer to RFC 2131 [8], the tunnel establishment acknowledgement brings the IP address from the PDG to the WLAN UE, refer to 3GPP TS 24.234 [3].

Figure 1 describes the access signalling between the PDG and the ISP/Intranet in the IPv4 Non-Transparent case.

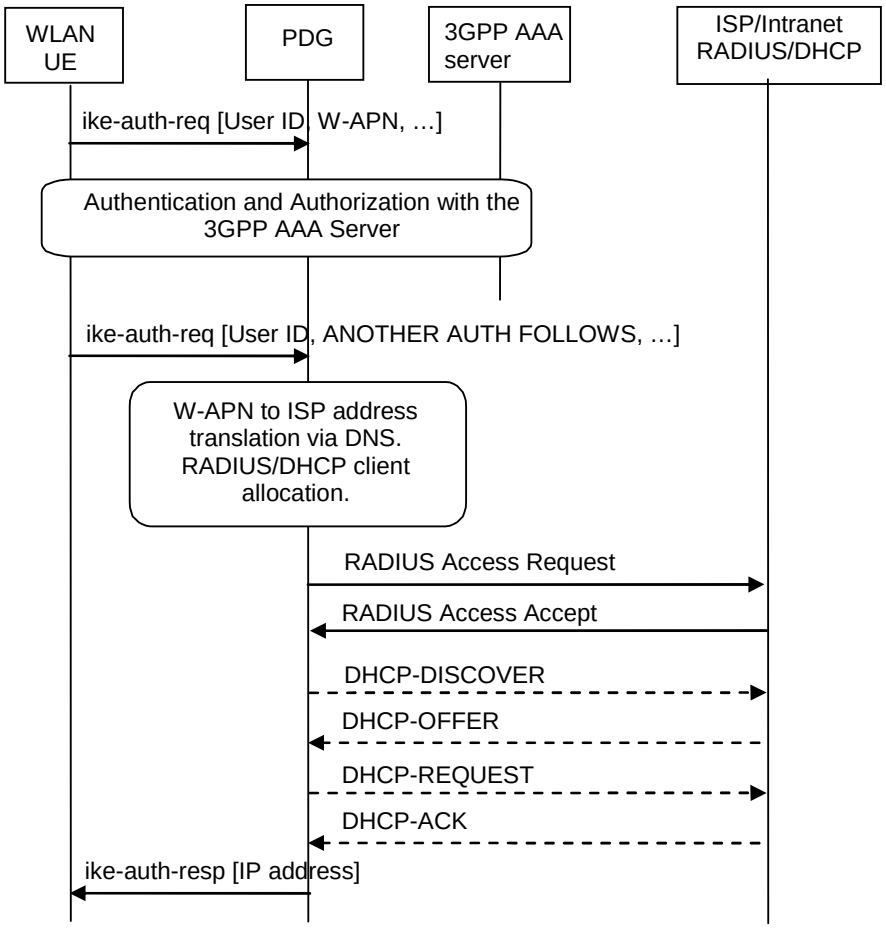


Figure 1: IPv4 Non-Transparent access to an Intranet or ISP

8.2.1.3 IPv6 Non Transparent access to an Intranet or ISP

When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the WLAN access authentication and authorization and tunnel establishment. The second signalling phase is done in the user plane.

The user plane signalling phase shall be either stateless or stateful. The stateless procedure, which involves only the WLAN UE and the PDG, is described in subclause "IPv6 Stateless Address Autoconfiguration". The stateful procedure, which involves the WLAN UE, PDG (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP, is described in subclause "IPv6 Stateful Address Autoconfiguration".

Whether to use stateless or stateful address autoconfiguration procedure is configured per W-APN in the PDG. For W-APNs configured as stateless, the PDG shall only use the Prefix part of the IPv6 address for forwarding of UE terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [13].

The selection between Stateful and Stateless Autoconfiguration is dictated by the Router Advertisements sent by the PDG as described in the corresponding subclauses below and according to the principles defined in RFC 2461 [14] and RFC 2462 [15].

8.2.1.3.1 Tunnel establishment and Intranet/ISP access authorization

The PDG provides the WLAN UE with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP. The WLAN UE may send an authentication request at the tunnel establishment and the PDG may request user authentication from a server, e.g. AAA, belonging to the Intranet/ISP.

Access to the ISP/Intranet may require the authentication and authorization with the External AAA Server. The PDG may 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 autorisation with the 3GPP AAA Server. Details on the multiple authentications are specified in IETF RFC 4739 [19]. Whether or not multiple authentications and authorizations are required is configured on a W-APN basis in the PDG.

In order to avoid any conflict between the link-local address of the WLAN UE and that of the PDG, the Interface-Identifier used by the UE to build its link-local address shall be assigned by the PDG. The PDG ensures the uniqueness of this interface-identifier.

Figure 2 describes the tunnel establishment between the WLAN UE and the PDG in the IPv6 Non-Transparent case.

The PDG deduces from local configuration data associated with the W-APN:

- IPv6 address allocation type (stateless or stateful);
- the source of IPv6 Prefixes in the stateless case (PDG internal prefix pool, or external address allocation server);
- any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [17]);
- the protocol e.g. RADIUS, to be used with the server(s);
- the communication and security feature needed to communicate with the server(s).

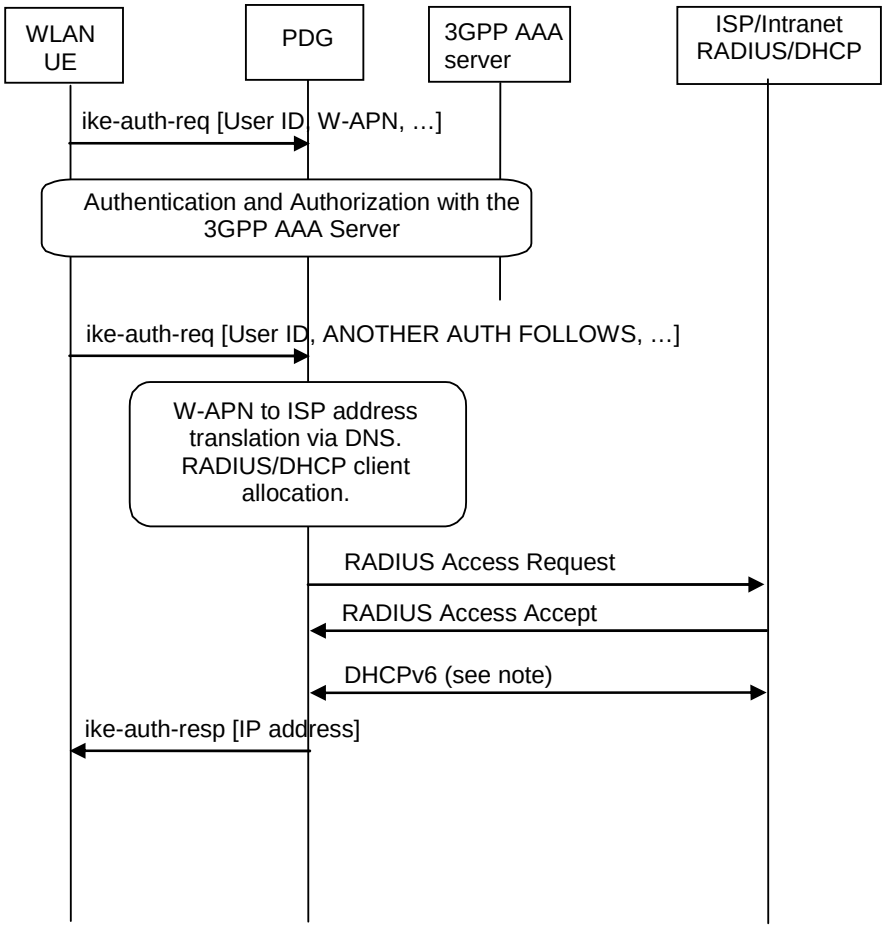
As an example the PDG may use one of the following options:

- PDG internal Prefix pool for IPv6 prefix allocation and no authentication;
- PDG internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The External AAA Server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the PDG;
- RADIUS for authentication and IPv6 prefix allocation. The External AAA Server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the PDG.

DHCPv6 may be used for IPv6 prefix allocation.

IPv6 Prefixes in a PDG internal Prefix pool shall be configurable and structured per W-APN.

The PDG shall return an IPv6 address composed of a Prefix and an Interface-Identifier in the tunnel establishment acknowledgement message (ike-auth-resp). The Interface-Identifier may have any value and it does not need to be unique within or across W-APNs. It shall however not conflict with the Interface-Identifier the PDG has selected for its own side of the UE-PDG link. The Prefix assigned by the PDG or the External AAA Server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this W-APN. If, on the other hand, stateful address autoconfiguration is configured on the W-APN, the Prefix part of the IPv6 address returned to the UE shall be set to the link-local prefix (FE80::/64).



NOTE: DHCPv6 may be used or IPv6 prefix allocation.

Figure 2: Tunnel establishment and Intranet/ISP access authorization

8.2.1.3.2 IPv6 Stateless Address Autoconfiguration

The tunnel establishment and Intranet/ISP access authorization is followed by a stateless address autoconfiguration procedure, which provides the WLAN UE with an IPv6 Global or Site-Local Unicast Address for the Intranet/ISP. (A terminal, e.g. a PC or a PDA with the WLAN UE may not have been able to receive the IP address during the 3GPP specific tunnel establishment signalling).

The procedure describing W-APNs configured to use Stateless Address Autoconfiguration may be as follows, (for details refer to RFC 2462 [15] and RFC 2461 [14]):

- After the tunnel establishment, the PDG starts sending Router Advertisements periodically in the tunnel towards the WLAN UE, with the M-flag cleared to indicate stateless address autoconfiguration.
- The UE may issue a Router Solicitation directly after the user plane establishment. This shall trigger the PDG to send a Router Advertisement immediately.
- The Prefix sent in the Router Advertisements shall be identical to the Prefix returned earlier in the tunnel establishment acknowledgement.

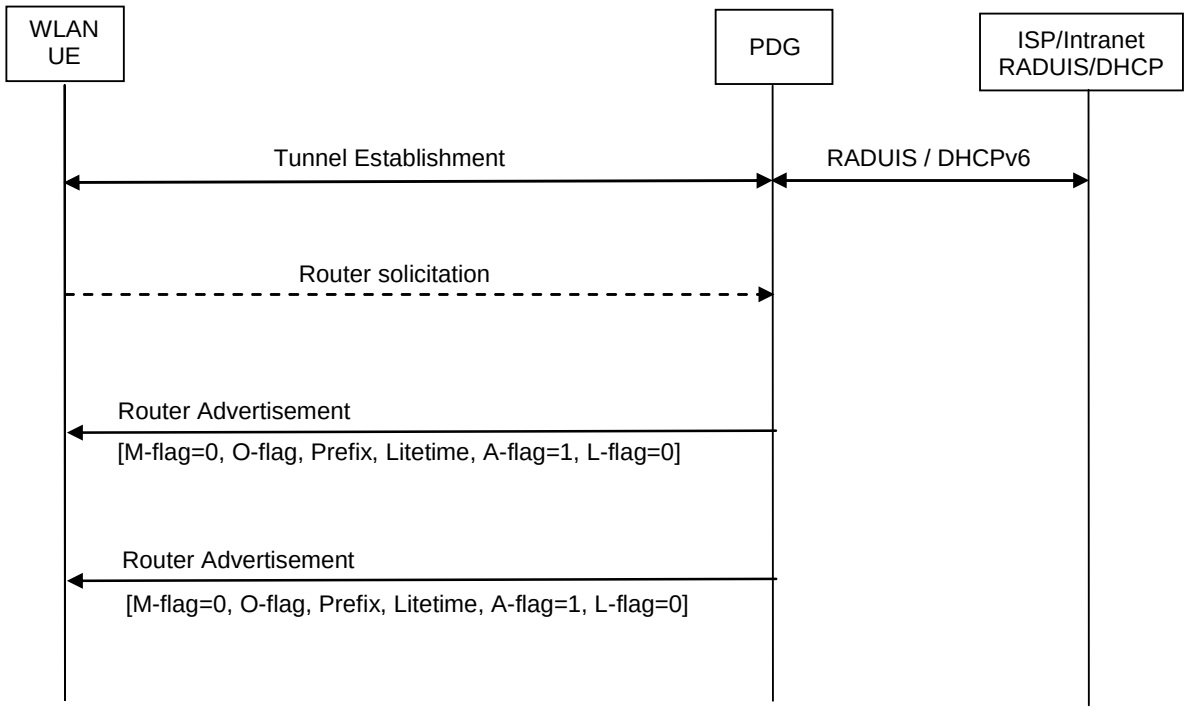


Figure 3: IPv6 Stateless Address Autoconfiguration

8.2.1.3.3 IPv6 Stateful Address Autoconfiguration

The tunnel establishment and Intranet/ISP access authorization is followed by a stateful address autoconfiguration procedure, which provides the WLAN UE with an IPv6 Global or Site-Local Unicast Address from the Intranet/ISP. The address has not yet been available during the tunnel establishment phase, but the UE requests the address from the Intranet/ISP by the stateful address autoconfiguration procedure. The PDG acts as a DHCP relay agent.

The procedure describing W-APNs configured to use Stateful Address Autoconfiguration may be as follows, (for details refer to RFC 2461 [14] and RFC 3315 [9]):

- The UE issues a Router Solicitation after the user plane establishment.
- This triggers the PDG to start sending Router Advertisements periodically in the tunnel towards the WLAN UE, with the M-flag set to indicate stateful address autoconfiguration and with no IPv6 prefix.
- When the UE receives the Router Advertisement with the M-flag set, it starts a DHCPv6 configuration including a request for an IPv6 address.

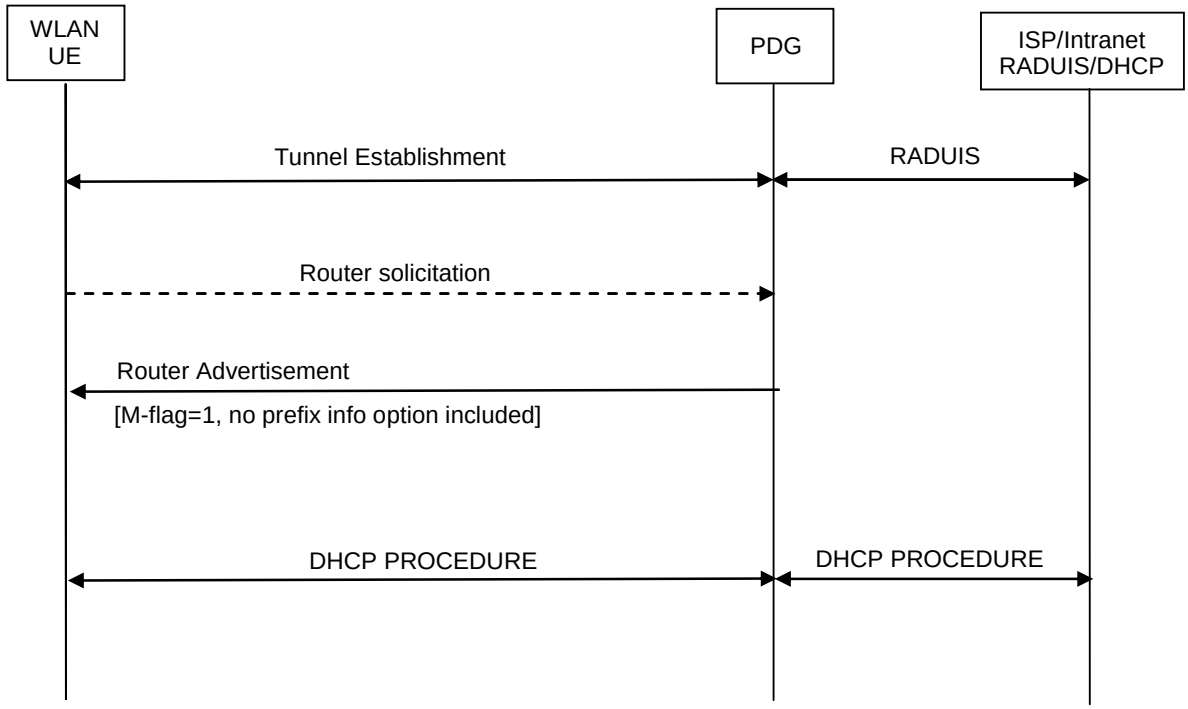


Figure 4: IPv6 Stateful Address Autoconfiguration

8.2.1.3.4 IPv6 Router Configuration Variables in the PDG

Refer to 3GPP TS 29.061 [4], subclause "IPv6 Router Configuration Variables in the GGSN".

8.3 Numbering and addressing

Refer to 3GPP TS 23.234 [1] and 3GPP TS 29.061 [4].

8.4 Charging

Refer to 3GPP TS 23.234 [1] and 3GPP TS 29.234 [2].

8.5 Domain Name System server (DNS Server)

Provision of Domain Name services shall be provided by the PLMN operators in the transparent case and the ISP in the non-transparent case. (DNS documentation is provided in RFC 1034 [6] and RFC 1035 [7]).

8.6 IP Multicast access

The Packet Domain with 3GPP – WLAN interworking access may allow an access to IP Multicast traffic coming from an external network. The support of IP Multicast in the Packet Domain is optional.

In order for the Packet Core Network with WLAN interworking access to support Multicast traffic that allows the WLAN UE to subscribe to multicast groups from outside the PLMN, the PDG shall support IGMP (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

For details, refer to 3GPP TS 29.061 [4], subclause "IP Multicast access".

9 Interworking with PDN (DHCP)

9.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, RFC 2131 [8]) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6, RFC 3315 [9]). It provides a mechanism for passing a large set of configuration parameters to hosts connected to a TCP/IP network (IP address, sub-net mask, domain name, MTU, etc.) in an automatic manner. Moreover DHCP may assign IP addresses to clients for a finite lease time, allowing for sequential reassignment of addresses to different users.

The lease time is chosen by the administrator of the DHCP server (in the external network), and is therefore out of the scope of the present document.

The Packet Domain offers the end user the possibility to run DHCP end-to-end the same way as he does when connected directly to a LAN (e.g. an enterprise Intranet). No modifications should be required in common implementations of DHCP clients and servers. However a Packet Domain-specific DHCP relay agent, refer to RFC 2131 [8] and RFC 3315 [9],is needed in the PDG so as to allow correct routing of DHCP requests and replies between the WLAN UE and the DHCP servers.

9.2 Address allocation by the Intranet or ISP

Address allocation schemes using DHCP are described in subclause "Access to Internet, Intranet or ISP through Packet Domain", with details for IPv4 in RFC 2131 [8] and for IPv6 in RFC 3315 [9].

9.3 Other configuration by the Intranet or ISP (IPv6 only)

When using IPv6, in some situations the WLAN UE may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [17]). If the UE is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the UE may use a procedure as in the example in figure 5 to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The PDG shall in this case indicate to the UE that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per W-APN in the PDG.

The following bullets describe an example of a signal flow, where the UE directs an Information-Request to the All_DHCP_Relay_Agents_and_Servers multicast address. The UE may also direct the message to a specific server instead of all servers. For a detailed description of the DHCPv6 messages refer to the DHCPv6 RFC 3315 [9]. The sequence is depicted in figure 5.

1) A Router Advertisement with the O-flag set is sent from the PDG to the UE to indicate to it to retrieve other configuration information.

2) The UE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 RFC 3315 [9]. The source address shall be the link-local address of the UE. The DHCP relay agent in the PDG shall forward the message.

3) DHCP servers receiving the forwarded INFORMATION-REQUEST message reply by sending a RELAY-REPLY message, with the "Relay Message" option including a REPLY message with the requested configuration parameters.

   The UE chooses one of the possibly several REPLY messages and extracts the configuration information.

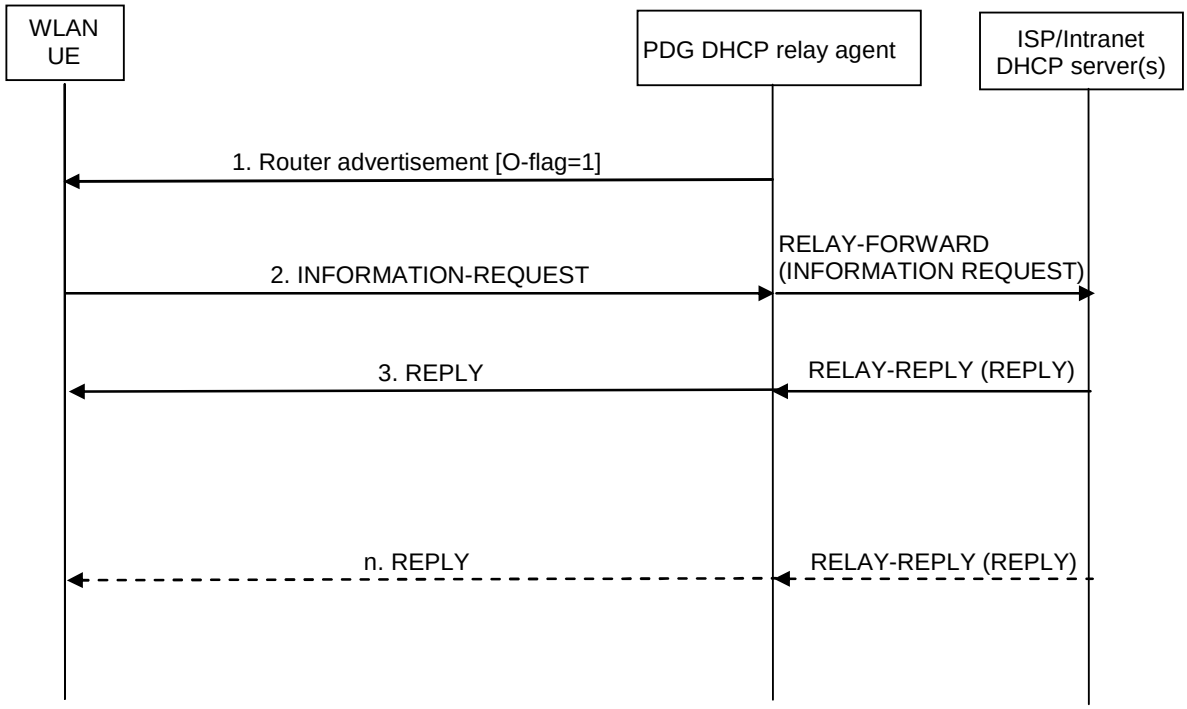


Figure 5: DHCPv6 other configuration signal flow

10 Interworking between Packet Domains

Refer to 3GPP TS 23.234 [1].

11 Usage of RADIUS on Wi interface

NOTE: The application of procedures in subclause 11.1 is not recommended. The application of procedures in subclause 11.3 is only recommended if user authentication and authorisation is not required. The procedures of those flows are incomplete for the following reason: In order to perform RADIUS Authentication, user ID and password information have to be passed from WLAN UE to PDG. However, this function is missing in the IKEv2 protocol that 3GPP TS 33.234 [16] refers in this release. In addition, user authentication and authorisation with AAA server will be standardised in release 7.

A PDG may, on a per W-APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an External AAA (Authentication, Authorization and Accounting) server.

11.1 RADIUS Authentication and Authorization

RADIUS authentication and authorization shall be used according to RFC 2865 [10] and RFC 3162 [11].

The RADIUS client function may reside in a PDG. When the PDG receives a tunnel establishment request, the RADIUS client function may initiate the authentication and authorization procedure with the External AAA Server after the successful authentication and autorisation with the 3GPP AAA Server.

The following procedure may take place depending on an ability of the External AAA Server. Details on the following procedures are specified in 3GPP TS 33.234 [16].

- The EAP procedure
  This procedure is the most preferable configuration for the ISP/Intranet access. In this procedure, the External AAA Server shall support EAP extensions specified in the RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP) [20].

- The PAP procedure
  This procedure is applied if the External AAA server performs PAP procedure.

- The CHAP procedure
  This procedure is applied if the External AAA server performs CHAP procedure.

The External AAA Server checks that the user can be accepted. The response (when positive) may contain network information, such as an IPv4 address or IPv6 prefix for the user.

The information delivered during the RADIUS authentication and authorization can be used to automatically correlate the users identity to the IPv4 address or IPv6 prefix, assigned/confirmed by the PDG or the External AAA Server respectively. The same procedure applies, in case of sending the authentication and authorization to a 'proxy' authentication server.

11.2 RADIUS Accounting

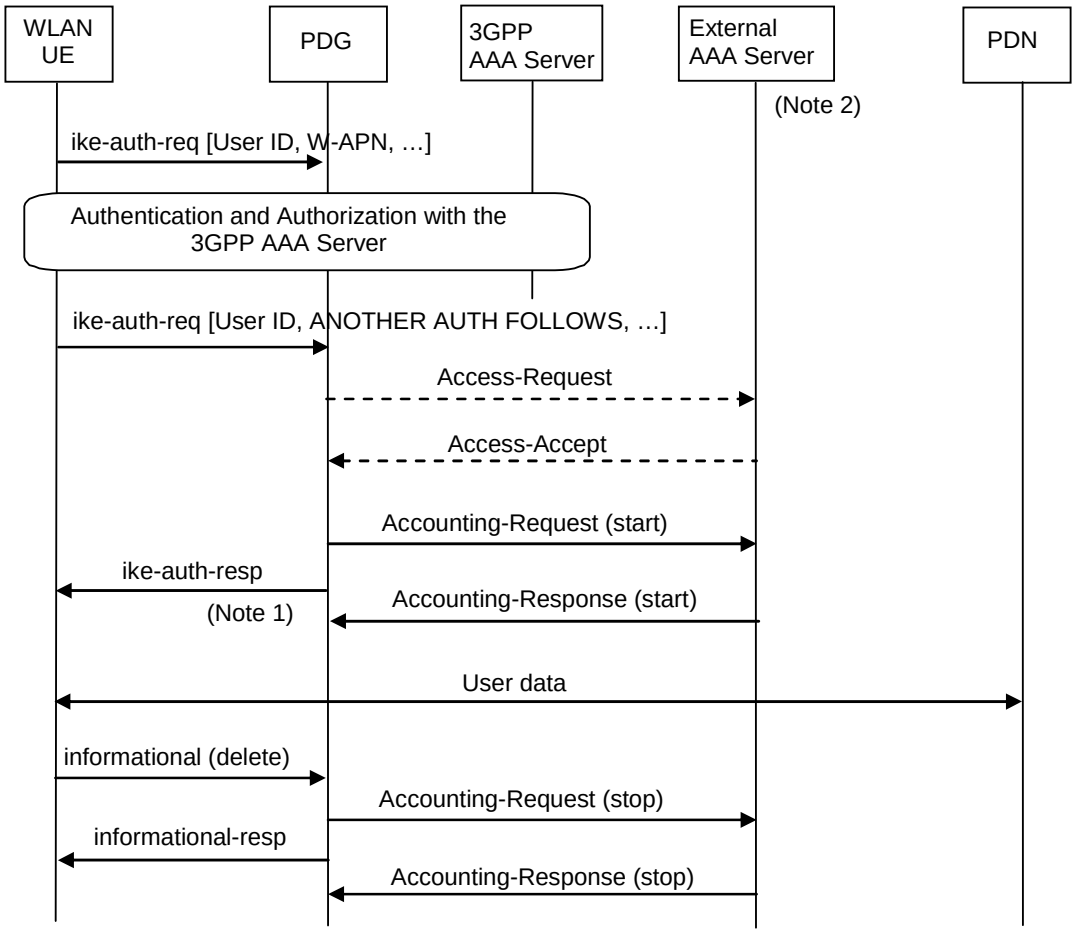
RADIUS Accounting shall be used according to RFC 2866 [12] and RFC 3162 [11].

The RADIUS accounting client function may reside in a PDG. The RADIUS accounting client may send information to an accounting server, which is identified during the W-APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the 3GPP network has authenticated the subscriber.

The Accounting-Request STOP and the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronized with the PDG information.

11.3 Authentication, Authorization and Accounting message flows

Figure 6 presents the RADIUS message flows between a PDG and an Authentication, Authorization and Accounting (AAA) server. For details of the tunnel establishment and deletion signalling, refer to 3GPP TS 24.234 [3].



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected W-APN (PDG) may be configured in such a way that the PDG drops user data until the Accounting Response (START) is received from the External AAA server. The PDG may wait for the Accounting Response (START) before sending the ike-auth response. The PDG may reject the tunnel establishment, if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 6: RADIUS message flow

When a PDG receives a tunnel establishment request (IKE-AUTH request) for a given W-APN, the PDG may (depending on the configuration for this W-APN) send a RADIUS Access-Request to an External AAA Server after the successful authentication and autorisation with the 3GPP AAA Server. The External AAA server authenticates and authorizes the user. If RADIUS is also responsible for IPv4 address or IPv6 prefix allocation, the External AAA Server shall return the allocated IPv4 address or IPv6 prefix in the Access-Accept message.

Even if the PDG was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an External AAA Server. This message contains parameters, e.g. the tuple, which includes the user-id and IPv4 address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the External AAA Server that the user session has started. The session is uniquely identified by the Acct-Session-Id that is composed of the Charging-Id and the PDG-Address.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected W-APN (PDG) may be configured in such a way that the PDG drops user data until the Accounting Response (START) is received from the AAA server. The PDG may wait for the Accounting Response (START) before sending the tunnels establishment response (IKE-AUTH response). The PDG may reject the tunnel establishment request, if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each W-APN.

At a stateful address autoconfiguration, no IPv4 address or IPv6 prefix is available at tunnel establishment. In that case the PDG may wait to send the Accounting-Request START message until the WLAN UE receives its IP address in a DHCP-REPLY.

When the PDG receives a delete tunnel request (*informational (delete)*) and providing a RADIUS Accounting-Request START message was sent previously, the PDG shall send a RADIUS Accounting-Request STOP message to the External AAA Server, which indicates the termination of this particular user session. The PDG shall immediately send a delete tunnel response (*informational-resp*), without waiting for an Accounting-Response STOP message from the AAA server.

The External AAA Server shall deallocate the IPv4 address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the PDG to the External AAA Server to ensure the correct synchronization of the session information in the PDG and the External AAA Server.

The PDG may send an Accounting-Request ON message to the External AAA Server to indicate that a restart has occurred. The External AAA Server may then release the associated resources.

Prior to a scheduled restart, the PDG may send Accounting-Request OFF message to the External AAA Server. The External AAA Server may then release the associated resources.

If an Access-Challenge is sent to the PDG when an Access-Request message is pending, the PDG shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [10].

11.4 List of RADIUS attributes

Refer to the 3GPP TS 29.061 [4], subclause "List of Radius attributes".

11a Usage of Diameter on Wi interface

As an operator option, it is also possible to use the Diameter protocol in order to provide Authentication, Authorization and Accounting services.

A PDG may, on a per W-APN basis, use Diameter authentication to authenticate a user and Diameter accounting to provide information to a Diameter server.

11a.1 Diameter Authentication

Diameter Authentication shall be used according to RFC 4005 [21].

The PDG and the Diameter server shall advertise the support of the Diameter NASREQ Application by including the value of the appropriate application identifier in the Capability-Exchange-Request and Capability-Exchange-Answer commands as specified in RFC 3588 [22].

The Diameter client function may reside in a PDG. When the PDG receives a tunnel establishment request, the Diameter client function may send the authentication information to an authentication server, which is identified during the W-APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IPv4 address or IPv6 prefix for the user.

The information delivered during the Diameter authentication can be used to automatically correlate the users identity to the IPv4 address or IPv6 prefix, assigned/confirmed by the PDG or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

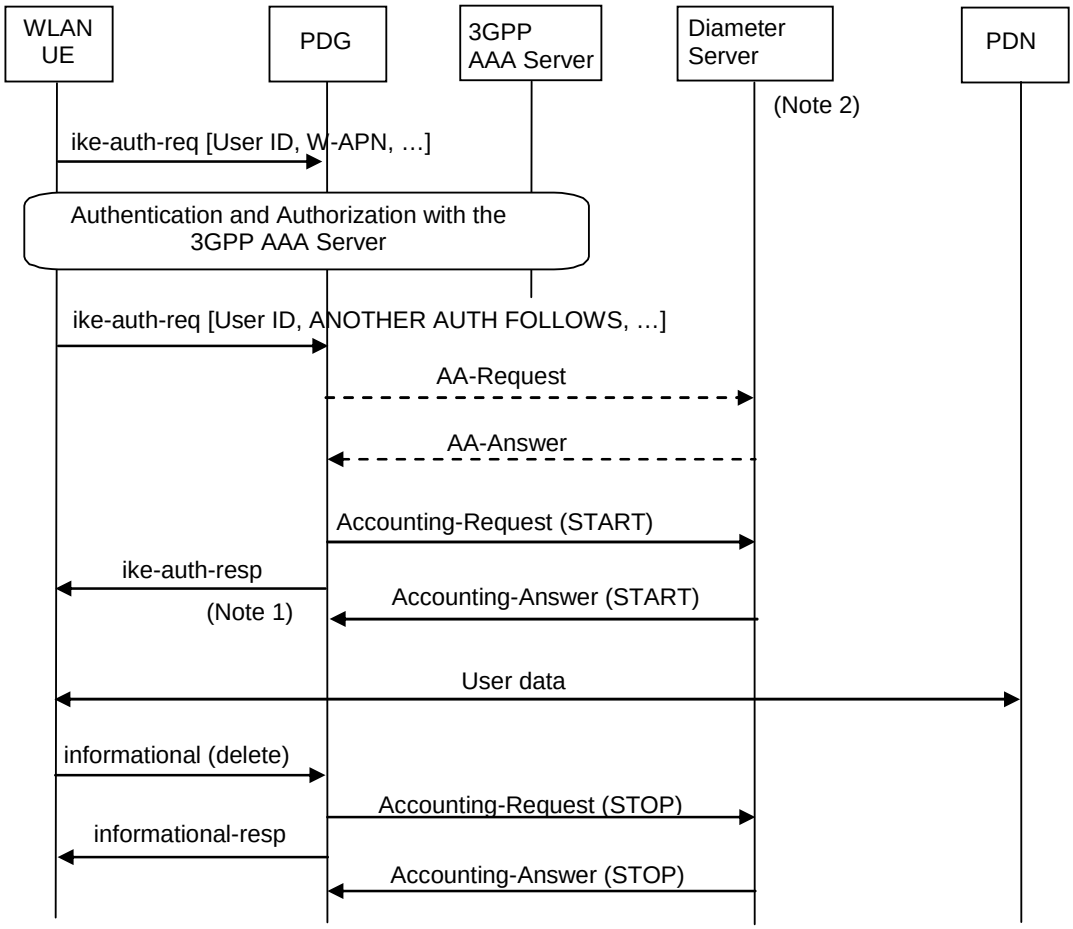
11a.2 Diameter Accounting

Diameter Accounting shall be used according to RFC 4005 [21].

The Diameter accounting client function may reside in a PDG. The Diameter accounting client may send information to an accounting server, which is identified during the W-APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the 3GPP network has authenticated the subscriber.

11a.3 Authentication and accounting message flows

Figure 6a presents the Diameter message flows between a PDG and a Diameter server. For details of the tunnel establishment and deletion signalling, refer to 3GPP TS 24.234 [3].



NOTE 1: If some external applications require Diameter Accounting request (START) information before they can process user packets, then the selected W-APN (PDG) may be configured in such a way that the PDG drops user data until the Accounting Answer (START) is received from the External AAA server. The PDG may wait for the Accounting Answer (START) before sending the ike-auth response. The PDG may reject the tunnel establishment, if the Accounting Answer (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Accounting-Request (START) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 6a: Diameter message flow

When a PDG receives a tunnel establishment request (IKE-AUTH request) for a given W-APN, the PDG may (depending on the configuration for this W-APN) send a Diameter AA-Request to a Diameter Server after the successful authentication and autorisation with the 3GPP AAA Server. The Diameter server authenticates and authorizes the user. If Diameter is also responsible for IPv4 address or IPv6 prefix allocation, the Diameter Server shall return the allocated IPv4 address or IPv6 prefix in the AA-Answer message.

Even if the PDG was not involved in user authentication (e.g. transparent network access mode), it may send a Diameter Accounting-Request (START) message to a Diameter Server. This message contains parameters, e.g. the tuple, which includes the user-id and IPv4 address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the Diameter Server that the user session has started.

If some external applications require Diameter Accounting request (START) information before they can process user packets, then the selected W-APN (PDG) may be configured in such a way that the PDG drops user data until the Accounting Answer (START) is received from the Diameter server. The PDG may wait for the Accounting Answer (START) before sending the tunnels establishment response (IKE-AUTH response). The PDG may reject the tunnel establishment request, if the Accounting Answer (START) is not received. The authentication and accounting servers may be separately configured for each W-APN.

At a stateful address autoconfiguration, no IPv4 address or IPv6 prefix is available at tunnel establishment. In that case the PDG may wait to send the Accounting-Request (START) message until the WLAN UE receives its IP address in a DHCP-REPLY.

When the PDG receives a delete tunnel request (*informational (delete)*) and providing a Diameter Accounting-Request (START) message was sent previously, the PDG shall send a Diameter Accounting-Request (STOP) message to the Diameter Server, which indicates the termination of this particular user session. The PDG shall immediately send a delete tunnel response (*informational-resp*), without waiting for an Accounting-Answer (STOP) message from the Diameter server.

The Diameter Server shall deallocate the IPv4 address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

11a.4 Wi Diameter messages and AVPs

Refer to the 3GPP TS 29.061 [4], subclauses "Gi Diameter messages" and "Gi specific AVPs".

12 Usage of RADIUS on Pp interface

12.1 General

The Pp interface is defined in 3GPP TS 23.141 [18] and allows the PDG to report presence relevant events to the Presence Network Agent (such as tunnel establishment/removal, allocation of the remote IP address for the WLAN UE). The Pp interface is implemented by reusing mechanisms of RADIUS authentication and accounting via Wi interface as defined in clause 11.

12.2 Radius Profile for Pp interface

The RADIUS interface on Wi reference point as defined in Clause 11 is used for the Pp Reference Point as clarified in the Profile in this Clause.

Only the following messages are required for the Radius Profile for the Pp reference Point:

- Accounting-Request START
- Accounting-Response START
- Accounting-Request STOP
- Accounting-Response STOP

For the Radius Profile for the Pp Reference Point, only the mandatory Parameters within the Accounting-Request START and Accounting-Request STOP messages according to 3GPP TS 29.061 [4] Clauses 16.4.3 and 16.4.4, respectively, and the Parameter "Calling-Station-Id" need to be supported. The usage of other parameters is optional. They may be ignored by the Presence Network Agent.

12.3 Interconnecting the Presence Network Agent and the PDG

The Presence Network Agent may be directly attached to the PDG or via a Radius Proxy.

If the PDG needs to connect both to some AAA server via the Wi interface and a Presence Network Agent via the Pp interface for the same APN, but supports only a single RADIUS interface, the PDG can be directly attached to that AAA server. The Presence Network Agent can in turn be attached to that AAA server, which acts as a RADIUS proxy. If the AAA server is configured as a RADIUS Proxy between the Presence Network Agent and the PDG, the Radius Profile for the Pp Reference Point shall be applicable on the interface between the Presence Network Agent and the AAA server.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-09	25	NP-040344			Approved by CN Plenary and placed under change control	2.0.1	6.0.0
2005-06	28	CP-050041	002	2	Pp Interface	6.0.0	6.1.0
2006-06	32	CP-060348	005	4	Depreciating authentication and authorization functions	6.1.0	6.2.0
2006-06	32	CP-060226	003	1	Introduction of I-WLAN Private Network Access	6.2.0	7.0.0
2006-06	32	CP-060225	004	1	Usage of Diameter over the Wi interface	6.2.0	7.0.0
2006-12	34	CP-060628	006	2	Authentication, Authorization, and Accounting message flows for Diameter Wi interface	7.0.0	7.1.0
2006-12	34	CP-060622	008	1	Correcting a reference to TS 29.061 in TS 29.161	7.0.0	7.1.0
2007-03	35	CP-070093	009	1	Update reference	7.1.0	7.2.0

History

Document history		
V7.2.0	March 2007	Publication