3GPP TR 23.827 V 0.43.01 (2007-098)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Feasibility Study of Mobility between 3GPP-WLAN Interworking and 3GPP Systems
(Release 8)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Keywords

UMTS, terminal, LAN, Mobility

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Formatted: English (United States)

Field Code Changed

Formatted: English (United States)

Formatted: English (United States)

Contents

Formatted: English (United States)

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 TR studies and defines the appropriate solutions for supporting mobility and roaming between 3GPP-WLAN Interworking system and 3GPP Systems so that ongoing 3GPP PS based services can be maintained with minimal impact on the end-user's perceived quality on the services at a change of the access network (between I-WLAN and 3GPP Access Systems). The solutions should impose minimum changes to the 3GPP PS core network and the terminals as well as the WLAN access.

Within the TR, different mechanisms are described along with their characteristics. A comparison of the pros and cons of the different mechanisms is included.

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 22. 234: Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 1

[2] 3GPP TS 23. 234: 3GPP system to Wireless Local Area Network (WLAN) interworking; System description; Stage 2

[3] H. Soliman (ed.), "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-04, March 2007

[4] A. Patel et al., "Authentication Protocol for Mobile IPv6", RFC 4285

[5] C. Perkins (ed.), "IP Mobility Support for IPv4", RFC 3344, August 2002

[6] D. Johnson et al., "Mobility Support in IPv6", RFC 3775, June 2004

[7] P. alhoun et al, "Diameter Mobile IPv4 Application", RFC4004, August 2005

[8] P Eronen (ed.), "IKEv2 and Multihoming Protocol (MOBIKE)", RFC4555, June 2006

[9] 3GPP TS23.402: Architecture Enhancemens for non-3GPP accesses, Release 8

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in TS 21.905 and the following apply.

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.

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.

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.

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.

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
Gn'	Reference point between GGSN and TTG'.
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)
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

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

AAA	Authentication, Authorisation and Accounting
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
IP	Internet Protocol
I-WLAN	Interworking WLAN
OCS	Online Charging System
PDG	Packet Data Gateway

PLMN	Public Land Mobile Network
SAE	System Architecture Evolution
SIM	Subscriber Identity Module
TTG	Tunnel Termination Gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	UMTS SIM
VPLMN	Visited PLMN
WAG	WLAN Access Gateway
WLAN	Wireless Local Area Network
WLAN UE	WLAN User Equipment

4 Requirements

Editor's note: this section describes the general requirements and the requirements on architectures, service and functions, etc.

4.1 General Requirements

- The mobility solution shall allow operators to support 3GPP services and Internet access.
- The solution should allow for easy introduction of the mobility mechanism with minimized complexity and cost on both terminals and the 3GPP Access systems.
- The solution shall support service continuity between 3GPP packet switched network and I-WLAN network.

4.2 Architecture Requirements

- The solution shall have minimum impact on the pre-Release 8 UE's and 3GPP PS and the I-WLAN systems.
- The I-WLAN architecture as defined in TS23.234 shall be used as the base line architecture for defining the solutions and possible enhancement.
- The solution shall consider an architecture that is independent of IP versions, i.e. it shall support both IPv4 and IPv6.
- Multiple simultaneous sessions established for a given user shall be maintained.
- Simultaneous 3GPP and I-WLAN access should be supported.

4.3 Mobility Requirements

- The solution shall support the change of access by the UE's between 3GPP PS system and the IWLAN while maintaining the service sessions without the need for changing the IP address(es).
- The solution should minimize the interruption to the operators' services or applications being provided to the end user.
- The solution shall be possible for users to be aware of the change of the access networks, 3GPP PS system or I-WLAN.
- In conditions where dual connections are available, the solution should be possible for operators to control the handover without compromising the mobility performance and the complexity on the system and the terminals.
- The solution shall be possible to disable the mobility function where applicable to the operators' needs.
- The solutions should be optimized in terms of transmission efficiency and control complexity.

4.4 Roaming Requirements

- The solution shall be possible to support the change of accesses between 3GPP PS system and the I-WLAN by terminals in a visited PLMN.
- The solution shall allow operators to re-use existing roaming interface(s) and protocol(s).

4.5 Charging Requirements

- The solution shall be possible for operators to re-use existing charging policies and mechanisms (Policy and Charging Enforcement Function (PCEF) based on TS 23.203).
- The solution shall be possible to make distinctions on the charging policies based on the current access by the terminals.
- The solution shall allow operators to use common charging control and policy rules for 3GPP PS system and the I-WLAN access.
- Charging information shall continue to be collected irrespective of whether the UE is attached to the 3GPP packet switched network or the I-WLAN network.

4.6 Security Requirements

- The solution shall not compromise any existing security measures taken by the end users and the operators.
- The solution shall be possible for operators to apply common access control based on TS33.234 regardless of the change of the accesses by the terminals.
- The solution shall allow operators to apply legal interception without impacting the user's preferred change of the accesses.

5 Evaluation Criteria

Editor's note: this section describes considerations for comoparing different solutions.

6 Solutions and Comparisons

6.1 The baseline architecture

The key considerations for defining the baseline architecture include:

- Re-use the Pre-SAE 3GPP PS system architecture and the I-WLAN architecture.
- Supporting and re-use the existing interfaces and protocols where possible.
- Supporting existing 3GPP PS services such as IMS, etc.
- Supporting roaming with I-WLAN in VPLMN.

Figure 6.1.1 shows the baseline architecture that shows the access to 3GPP PS Services (e.g. IMS) and PDN's via 3GPP PS systems and/or I-WLAN for UE's at home network.

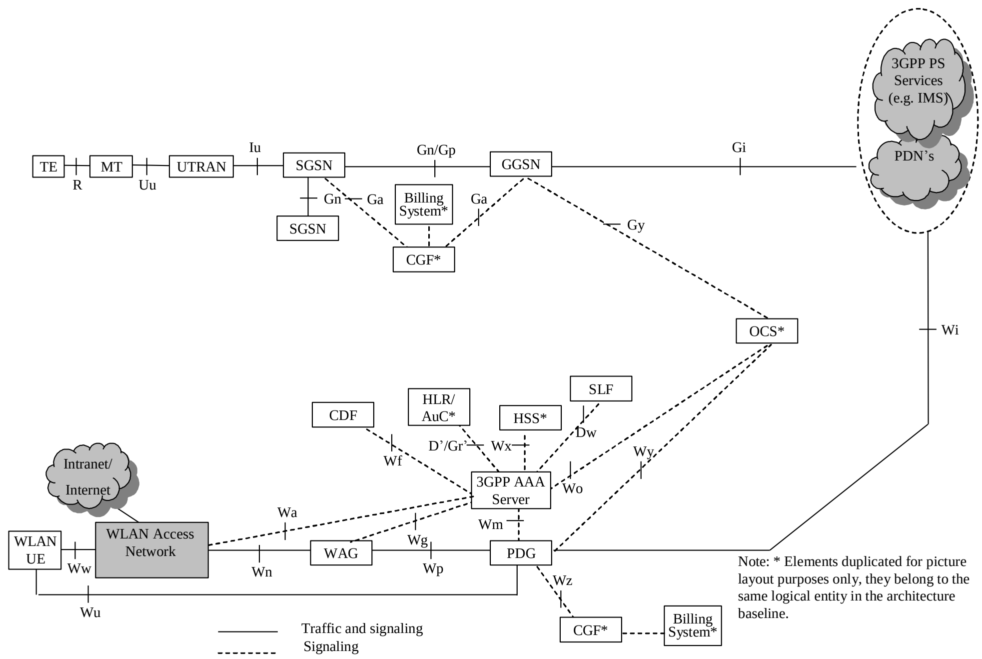


Figure 6.1.1. The baseline non-roaming architecture for defining mobility between 3GPP PS system and I-WLAN.

6.2 The Solutions

6.2.1 Alternative A

6.2.1.1 The Architecture

Figure 6.2.1 shows the architecture for the non-roaming case. There is a Gn interface between the SGSN and the TTG' element. Between the TTG' and the GGSN, there is again a Gn interface. The sessions for users who are subscribed to I-WLAN mobility service are anchored at the TTG'. UE traffic flows from the SGSN to the TTG' and then to the GGSN. The existing Gn interface between the SGSN and the GGSN may also be used at the same time, for e.g., for non-IWLAN subscribers.

Note that the Gn interface between the SGSN to the GGSN is shown only for informative purpose. It has no impact on the solution for IWLAN Mobility.

Note that the interface related to charging systems is not shown in the figures.

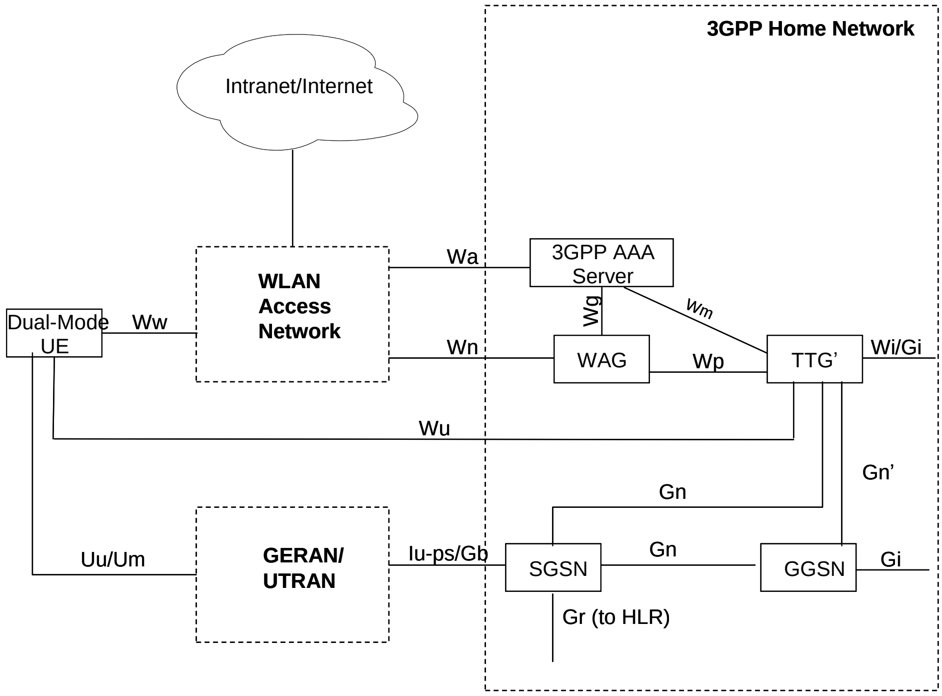


Figure 6.2.1 : Non-Roaming Architecture for I-WLAN Mobility

Figure 6.2.2 shows the architecture for the roaming case, with a Gp interface between the SGSN in the VPLMN and the TTG' in the HMPLMN. Between the TTG' and the GGSN, there is a Gn interface. The sessions for users who are subscribed to I-WLAN mobility service are anchored at the TTG'. UE traffic flows from the SGSN to the TTG' and then to the GGSN. The existing Gp interface between the SGSN and the GGSN may also be used at the same time, for e.g., for non-IWLAN subscribers.

Note that the Gp interface between the SGSN to the GGSN is shown only for informative purpose. It has no impact on the solution for IWLAN Mobility.

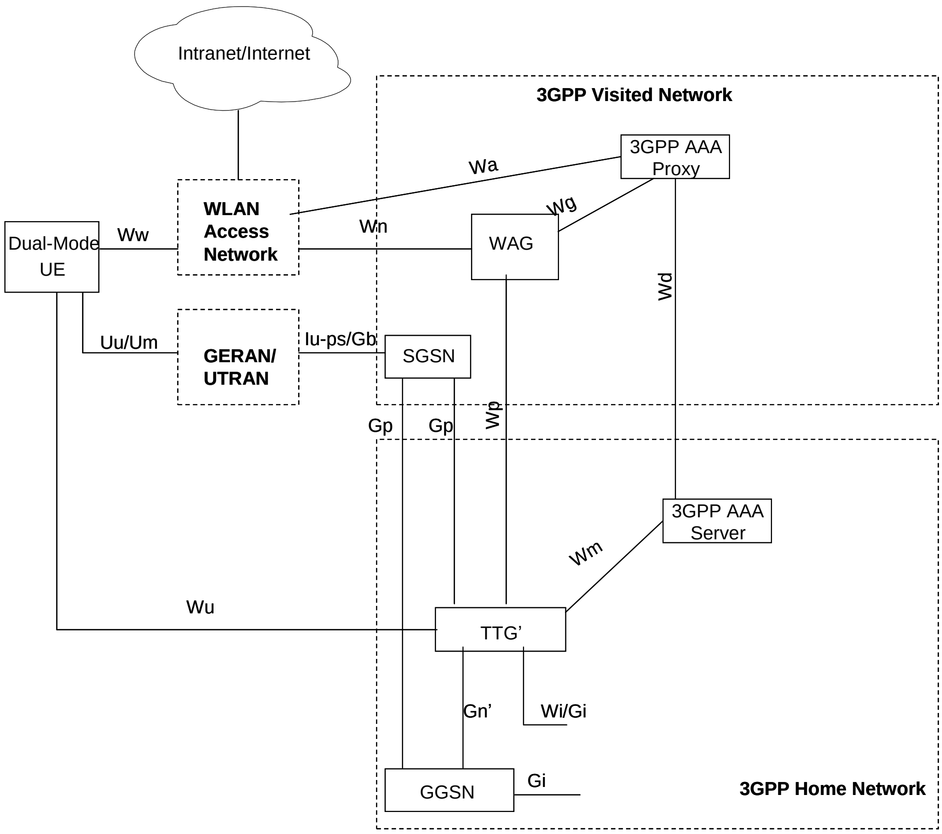


Figure 6.2.2 : Roaming Architecture for I-WLAN Mobility

In the proposed architecture, the following are the main changes done to enable I-WLAN mobility.

- TTG': The TTG' network element includes the functionalities and the interfaces as defined in TS 23.234. As a TTG, this node already has the Gn' interface toward GGSN and a GTP stack. Additional support of Gn/Gp interface toward SGSN is needed to support 3GPP-WLAN session/service continuity using this architecture. Note that this reference point is already applicable to the PDG since the PDG is defined as a combination of TTG and GGSN in TS 23.234.

  Figure 6.2.3 shows an implementation option for PDG from 23.234. It shows all the interfaces supported on the PDG. Figure 6.2.4 shows a modified version of this by adding a Gn/Gp interface towards the SGSN. T

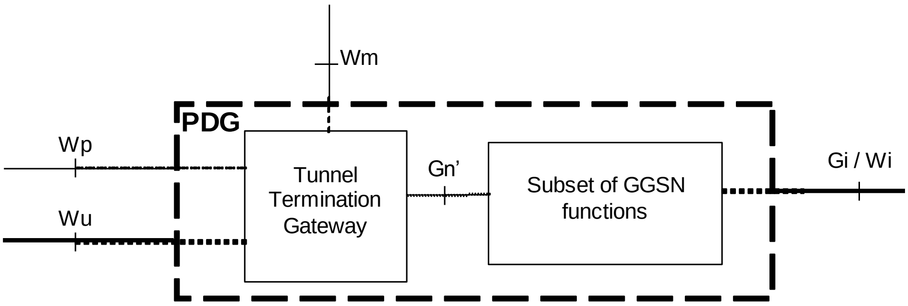


Figure 6.2.3 : PDG implementation re-using GGSN functionality (from 23.234)

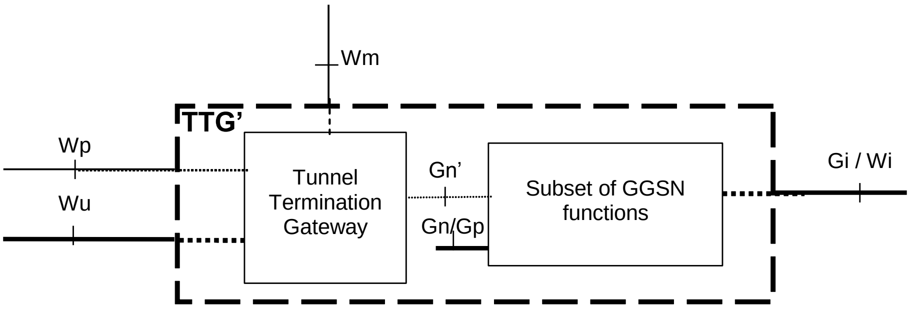


Figure 6.2.4 : TTG' implementation re-using GGSN functionality

Note that the DNS needs to be updated so that the TTG/PDG will be selected as a result of APN selection/DNS resolution as a GGSN address.

- HSS: The subscribed APN list needs to be modified to include the newly assigned APN for the 3GPP-WLAN subscribers.

No other existing network element is modified.

With this architecture, the TTG’ becomes the anchor point and the IP Point of Connectivity.

Editor’s Note: The UE impacts due to the requirement on the UE to support the use of same IP address on the interface associated with 2G/3G radios and the IPSec tunnel interface are FFS.

Editor’s Note: The architecture described in this solution needs to be evaluated against the requirements. This is FFS.

Editor’s Note: The architecture described above requires the TTG' selected by the UE while on IWLAN access to be the same as the TTG' selected by the SGSN. The means to deliver such functionality is FFS.

6.2.1.2 3G Access System to I-WLAN handover (Wi Services)

This section shows the call flows for a handover from 3GPP access system to I-WLAN with the services hosted on the TTG' via the Wi interface. The handset is assumed to comply with the existing specifications for 3GPP-WLAN interworking. 6.2.5 shows the overview call flow of the handover. Note that all the detailed message flows are not shown here for brevity.

1. The user is in pre-SAE 3GPP system coverage and requests the PDN or Operator IP service by sending 'Activate PDP context request' to SGSN. For the users that are subscribed to WLAN use, another APN will be provided for the same service. For example, if the normal APN is service1.operator.com, then the users with WLAN access will be provided with the APN w.service1.operator.com for the same service.

2. The TTG' is resolved as a GGSN, and the SGSN creates the PDP context toward the TTG'. The TTG' acts as a GGSN here and assigns the IP address of the user. The TTG' is selected at the SGSN by standard GPRS APN selection/DNS resolution. The operator's DNS entry needs to be modified so that the WLAN-converged subscribers will be routed to TTG'. In this procedure, the SGSN will authenticate/authorize the user with the APN, and if the subscriber profile in HSS contains the APN (i.e. w.service1.operator.com), then it proves that the user is allowed to access WLAN and the call will be routed to the TTG'. From the TTG' point of view, the fact that the create_PDP_context_request was provided from the SGSN means that the user is a valid WLAN subscriber.

3. The SGSN sends the response to the client with the assigned IP address, after it receives the 'create_PDP_context_ack' from the TTG'.

4. From SGSN point of view, the TTG' acts as normal GGSN and the GTP tunnel has been set up between SGSN and the TTG'. The TTG' provides the Wi interface towards PDN.

5. User is associated with WLAN.

6. The 3GPP-WLAN tunnel setup procedure starts by exchanging IKE_SA_INIT between the client and the TTG'. The TTG' is operating as specified in TS 23.234 and TS 33.234, and terminates the IKE and IPSec exchanges.

7. To authenticate and authorize the tunnel, the EAP-SIM/EAP-AKA procedure is performed inside the IKEv2 per TS 33.234. This authentication involves the client, TTG', AAA server, and HLR/HSS. Note that the TTG' assigns the **same IP address** that was used for GPRS session to the WLAN session. This is possible since the TTG' already has the knowledge of the user session through.

8. Now the traffic is switched by the TTG' from GPRS to the WLAN. The IPsec tunnel has been established between the client and the TTG' and the TTG' will route the traffic to PDN using the same Wi interface. Note that the TTG' works as the IP point of connectivity. It switches the traffic between the pre-SAE 3GPP system and the WLAN.

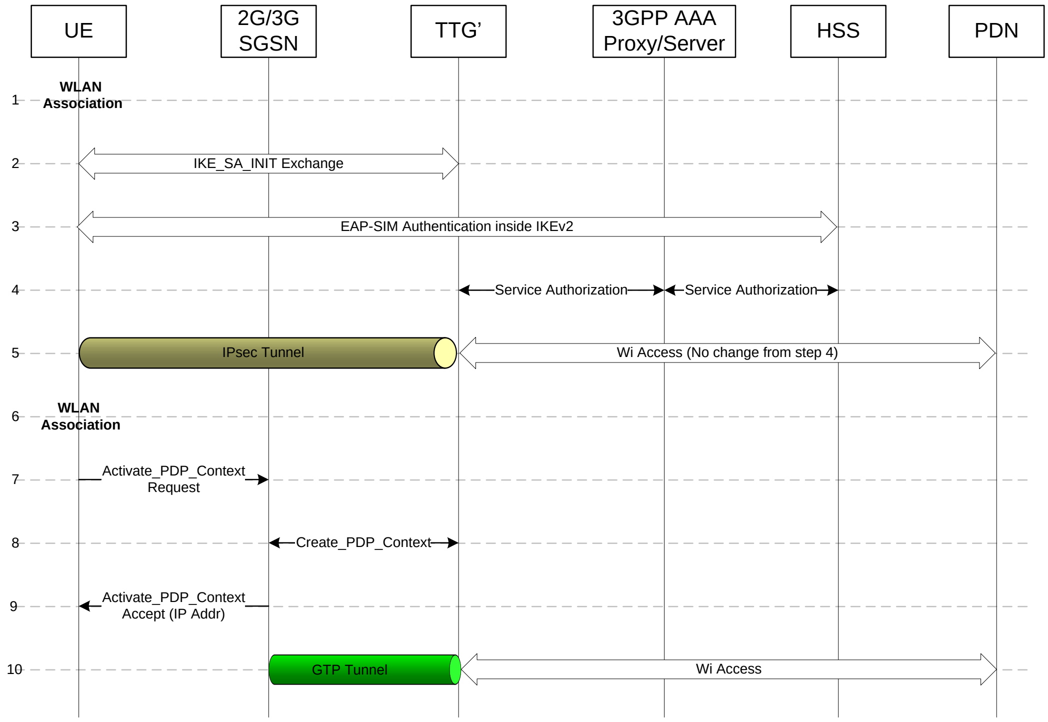


Figure 6.2.5 Handover from pre-SAE 3GPP to I-WLAN (Wi services)

Note that there are no extra messages needed during the 3GPP WLAN tunnel setup and the session is continued seamlessly as TTG' is acting as an anchor point. The TTG' manages the IP address, hence assigns the same IP address to the WLAN session as the one assigned by 3GPP session and the application is serviced without interruption. The make-before-break type handover is possible and the handover can be performed **without any service disruption** from user perspective.

6.2.1.3 I-WLAN to 3G Access System handover (Wi Services)

This section shows the call flows for a handover from I-WLAN to 3GPP access system with the services hosted on the TTG' via the Wi interface. This scenario covers mobility from I-WLAN to pre-SAE 3GPP access networks. Figure 6.2.6 illustrates the call flow. The TTG' is acting as the anchor point.

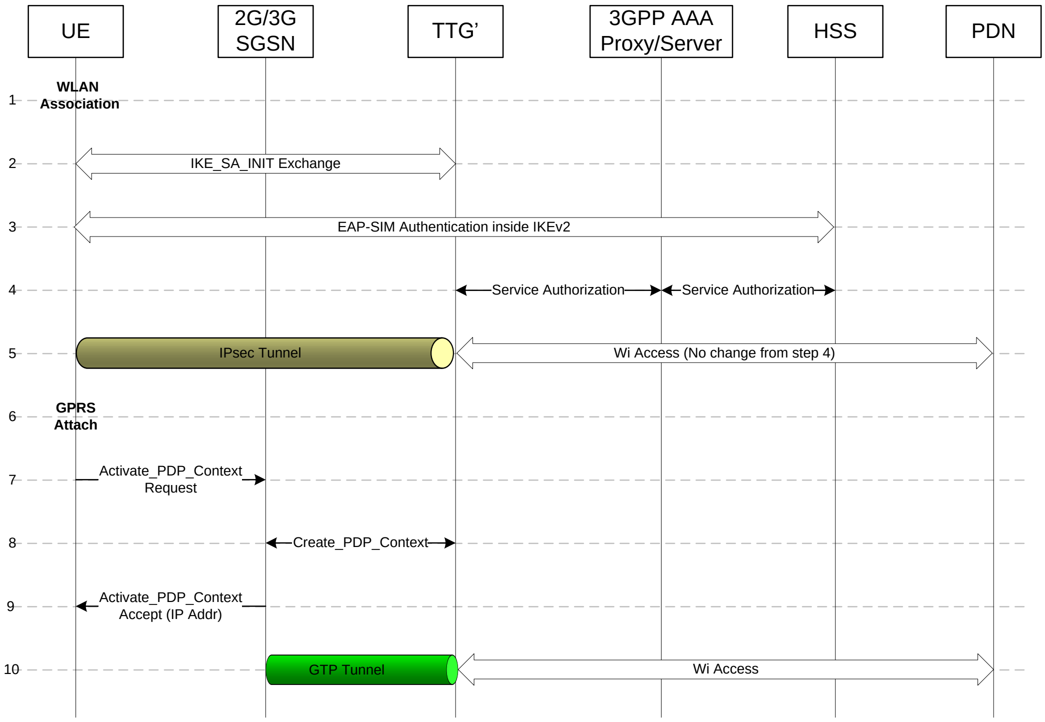


Figure 6.2.6 I-WLAN to pre-SAE 3GPP handover (Wi Services)

1. The user does not have any 3GPP connection yet, and is associated with the WLAN.
2. The client requests the 3GPP-WLAN tunnel setup to TTG'. TTG' terminates the IKE exchanges per TS 33.234.
3. The EAP-SIM authentication occurs inside IKEv2 to authenticate the user per TS 33.234. The EAP-SIM authentication involves the client, TTG', AAA server, and the HLR/HSS.
4. The service authorization occurs. The TTG' may consult AAA server or HSS for subscription profile.
5. The IPSec tunnel is established between the client and the TTG' and the TTG' provides the Wi interface to connect to PDN. This is the standard 3GPP-WLAN interworking procedure defined in TS 33.234.
6. The user is attached to a pre-SAE 3GPP system and decides to handover to this system (e.g. due to weak WLAN signal strength, etc).
7. The client requests the PDP context activation to the SGSN it is registered.
8. The SGSN sends the create_PDP_context request message to the TTG' after GGSN resolution. Since the TTG' already has the user session information, it only needs to switch the traffic route from WLAN to 3GPP. The Wi interface remains unchanged.
9. SGSN sends the response to the client.
10. The GTP has been established between SGSN and TTG'. The Wi interface remains unchanged.

6.2.1.4 3GPP Access System to I-WLAN handover (Gi Services)

This section shows the call flows for a handover from 3GPP access system to I-WLAN with the services hosted on the GGSN via the Gi interface. The existing GGSN is re-used to provide connectivity to the services as in current GPRS. This architecture works with the same concept as described in the section 6.2.1.2 and 6.2.1.3 and is provided here to describe that the proposed architecture can be used in either way, for operator's flexibility.

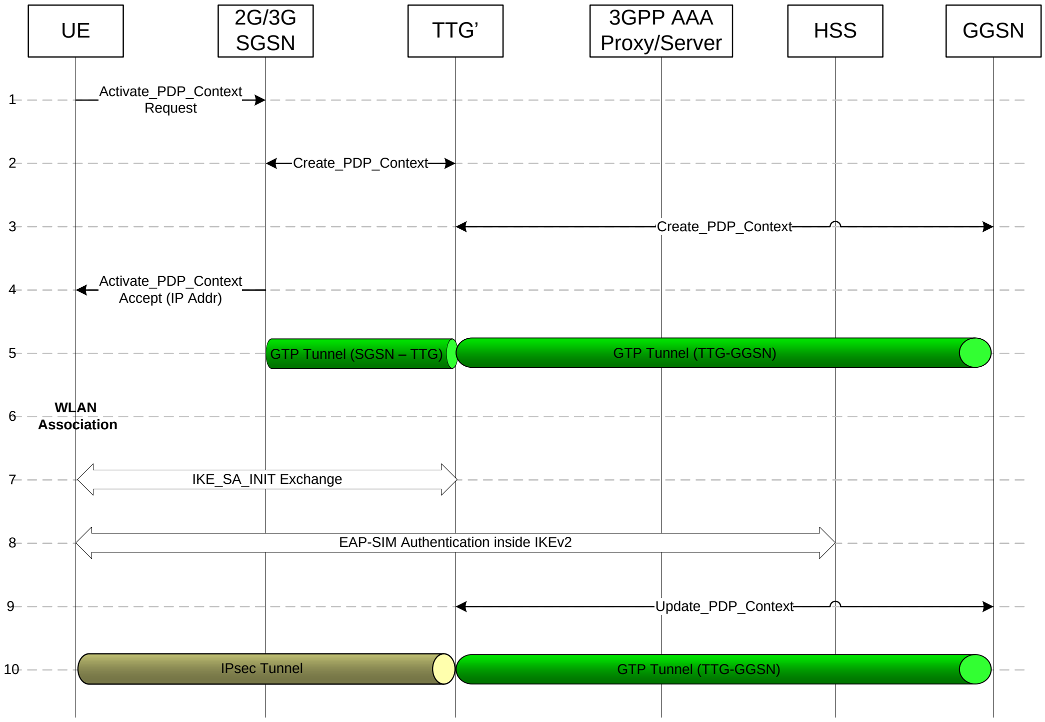


Figure 6.2.7 Pre-SAE 3GPP to WLAN handover (Gi Services)

1. The user is in pre-SAE 3GPP system coverage and requests the PDN or Operator IP service by sending 'Activate PDP context request' to SGSN.

2. The TTG' is resolved as a GGSN, and the SGSN creates the PDP context toward the TTG. The TTG' acts as a GGSN here.

3. TTG' resolves the GGSN address through which the service is to be provided and proxies the create_PDP_context request/response to and from the GGSN. The TTG' acts as a SGSN here.

4. The SGSN sends the response to the client with the assigned IP address, after it receives the 'create_PDP_context_ack' from the TTG.

5. There are two GTP legs – one between SGSN and TTG' and the other between TTG' and GGSN. Note that the optimization can be achieved using the user and control plane separation, already defined in GPRS specification. Note that if the TTG' is used in the operator's network, the TTG' will terminate the GTP tunnel for GPRS connection and route the traffic to the PDN.

6. User is associated with WLAN.

7. The 3GPP-WLAN tunnel setup procedure starts by exchanging IKE_SA_INIT between the client and the TTG. The TTG' is operating as specified in TS 23.234 and TS 33.234, and terminates the IKE and IPSec exchanges.

8. To authenticate and authorize the tunnel, the EAP-SIM procedure is performed inside the IKEv2 per TS 33.234. The EAP-SIM authentication involves the client, TTG, AAA server, and HLR/HSS. Note that the TTG' can assign the same IP address that was used for GPRS session to the WLAN session. This is possible since the TTG' already has the knowledge of the user session.

9. When the authentication is successful, the TTG' can now switch the access network from the pre-SAE 3GPP system to WLAN. Since there is already a GTP leg between the TTG' and GGSN to carry the traffic, there is no need for the TTG' to perform any further procedures toward the GGSN. However, for accounting purposes (to let the GGSN know that the access network has been changed from pre-SAE 3GPP to WLAN), the TTG' may optionally send the Update_PDP_context to the GGSN. Only the RAT (Radio Access Type) needs to be updated.

10. Now the traffic is switched by the TTG' from GPRS to the WLAN. The IPSec tunnel has been established between the client and the TTG, and one GTP tunnel is used between the TTG' and the GGSN. Note that if the TTG' is used in the operator's network, the TTG' will terminate the IPSec tunnel for WLAN connection and route the traffic to the PDN.

Also note that the all the traffic is terminated at the GGSN, so the existing GGSN service, e.g. APN based services and content/event based billing, can be provided without any implications.

6.2.2 Alternative B: Single Tunnel Serving-3gpp-Anchor solutions

6.2.2.1 Principles

The Single Tunnel Serving-3gpp-Anchor solution aims of supporting seamless mobility between 3GPP and WLAN Interworking systems for a user with multiple packet sessions, with reuse of existing and unchanged GGSN. It concerns the case where the operator has deployed or plans to deploy WLAN Interworking with a PDG made of GGSN and TTG, reusing the existing GGSN equipment, as described in TS 23.234 normative annex F [2].

It is based on following main principles:

- The architecture is based on the evolution of the TTG (defined in 3GPP TS 23.234) aiming at keeping the GGSN as an anchor point of user plane;
- No impact to existing SGSN;
- Configuration impacts to DNS servers and SGSN for APN resolution are FFS.
- No impact to existing GGSN;
- The reuse of GTP tunnelling that provides QoS differentiation, Charging information (e.g. RAT) in the same way as GPRS Core, allowing full continuity of bearer services with the GPRS/UMTS-PS system.
- It does not reuse the GTP Mobility Management, which is complex, and that is not required because of the WLAN specificities:
    1. LA/RA concept is not needed because the UE always establish an IPsec tunnel when camping on a WLAN cell;
    2. 3GPP and WLAN radios can be used simultaneously and this simplifies the handover mechanisms;
- A Serving-3gpp-Anchor (S3A) function is added, in the GPRS/UMTS-PS Core, that can be implemented e.g. either as a separate entity or in the TTG;
- Depending on operator's configuration (in the S3A), the user plane uses direct tunnelling between TTG and GGSN, or goes through the Serving-3gpp-Anchor; In the latter case, the Serving-3gpp-Anchor is both user plane and control plane anchor.
- A NAS Session Management protocol between the UE and the TTG is introduced to replace multiple IPsec tunnels by one single IPsec tunnel established at authentication, allowing the support of multiple sessions per APN and of multiple APN's by the establishment of independent sessions in separate IETF GRE tunnels [3]. Each UE-TTG GRE tunnel is connected to a TTG-GGSN GTP-u tunnel.
    - o It simplifies the terminal, which only has to support one single IPsec tunnel;
    - o It avoids a full re-authentication when establishing a session with a new APN;
    - o It allows providing same bearer services as in GPRS-UMTS coverage, thanks to the establishment of individual sessions;

- At handover, it allows maintaining the multiple GPRS/UMTS-PS sessions per APN or with multiple APNs, thanks to the re-establishment of individual sessions;
- Compared to annex F.2.3.2 of TS 23.234, where each end-to-end tunnel is systematically mapped to one primary and multiple secondary GTP tunnels (one per allowed DSCP of the user's 3GPP WLAN QoS profile), it minimizes the number of PDP Contexts between TTG and GGSN as they are established only if required;
- It reuses 24.008 Session Management messages (Activate PDP context request/accept/reject (primary and secondary), Modify PDP context request/accept/reject, Deactivate PDP context request/accept/reject).

- The solution can migrate to SAE architecture with the Serving-3gpp-Anchor evolving to a serving-SAEGW function. In this case,
  - The user plane flows of the I-WLAN UE(s) are indeed handled by the Serving-3gpp-Anchor (with the Serving-3gpp-Anchor acting as a relay between tunnels towards the radio side and tunnels towards the PDN-SAEGW).
  - The tunnels between evolved Serving-3gpp-Anchor and PDN-SAEGW may either correspond to GTP tunnels or correspond to IETF (PMIP) tunnels.

6.2.2.2 Architecture reference model (Non roaming model)

Figure 6.2.8 shows the Architecture reference model of I-WLAN Mobility solution for a split PDG.

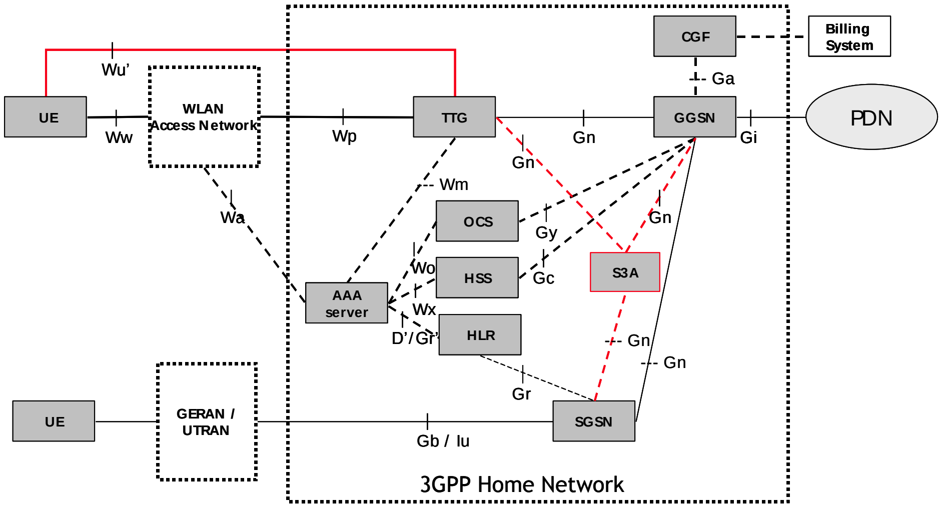


Figure 6.2.8 Non-Roaming Reference model for I-WLAN/3GPP Mobility

TTG: On top of the TTG functionalities already defined in TS 23.234, the TTG supports Wu'.

S3A (Serving-3gpp-Anchor): The S3A acts as an anchor point for the control plane and may (based on operator configuration in the S3A) act as an anchor point for the user plane. The S3A supports Gn interfaces toward SGSN, TTG and GGSN to provide the service continuity between 3GPP access systems and WLAN Interworking. These new interfaces are shown in red in the picture.

Wu' reference point: New enhanced Wu' interfaces should include a minimum set of Session Management messages (similar to 3GPP TS 24.008 messages) to provide multiple simultaneous sessions established for a given user and

Service equivalent to Network Requested Secondary PDP Context Activation. New Wu' interface should also support GRE tunnels in the user plane to distinguish the different data flows corresponding to the PDP contexts in the GPRS Core.

Gn interfaces between SGSN and GGSN, and between TTG and GGSN are only used for the user plane.

6.2.2.3 Description of mobility procedures

6.2.2.3.1 Handover mechanisms

As described in "Mobility concepts", this handover mechanism addresses the Mobile operators that reuse the GGSN deployments to implement the PDG functionality as described in TS 23.234 annex F (normative).

Taking benefit from the fact WLAN and GERAN/UMTS radios can operate simultaneously, the mobility mechanism consists in a make-before-break handover by establishing a second leg in the target RAT, switching the leg by the GGSN then releasing the first leg in the old RAT.

The GGSN is kept as a user plane anchor point even though the user moves between 3GPP and WLAN coverage.

To supply the mobility between WLAN Interworking and GERAN/UTRAN, the Serving-3gpp-Anchor (S3A) is introduced and it acts as an anchor point for control plane. This node is in charge of storing the context of the UE (such as the attached GGSN address) and to update the PDP context when the user changes of system coverage.

Note that there are two alternatives for the user plane anchor, depending on the operator's choice:

1- the user plane may use direct tunnelling between TTG and GGSN as described above,

2- alternatively, the Serving-3gpp-Anchor may act as an user plane switching function.

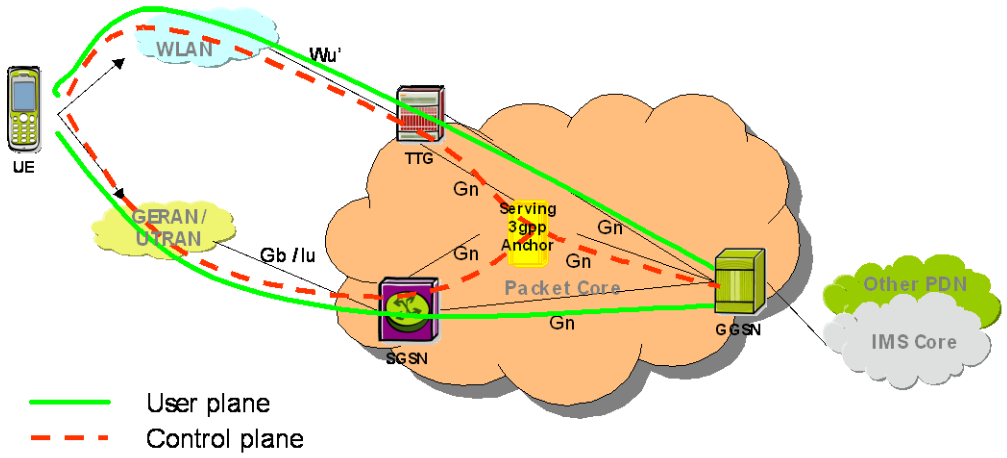


Figure 6.2.9 Handover mechanism for I-WLAN/3GPP Mobility

Tools used for mobility are:

1) NAS Session Management protocol (W-SM) protocol

The establishment of the legs (bearers) is performed via a NAS Session Management protocol,

- between the UE and the SGSN, via TS 24.008 procedures: Activate PDP Context, Modify PDP Context, Deactivate PDP Context, etc.
- between the UE and the TTG, via a new NAS Session Management protocol (W-SM) that reuses 24.008 messages and parameters.

This new NAS Session Management protocol (W-SM) is introduced to allow multiple sessions within a single IPsec tunnel (multiple sessions per APN and multiple APN's) by the establishment of independent sessions in separate IETF

GRE tunnels. It also allows to maintain the multiple sessions with their original QoS profile at handovers between GPRS/UMTS and WLAN.

2) Use of PCO field from 24.008 to retrieve the Serving-3Gpp-Anchor at 3GPP-WLAN handovers

The PCO container is used to exchange the Serving-3gpp-Anchor address between the UE and the Serving-3gpp-Anchor in both 3GPP and WLAN modes: via 24.008 messages under 3GPP, and via W-SM under WLAN. The PCO IE (Protocol Configuration Options) is specified in TS 24.008 to convey information from external protocols between the MS and the GGSN, and is transparent to the SGSN. The new container is processed by the Serving-3gpp-Anchor and, according to TS 29.060, ignored by the legacy GGSNs.

When a UE setups the first connection for a given APN, the access node (SGSN or TTG) chooses a Serving-3gpp-Anchor (S3A) according to its own criteria (DNS query) and sends a Create PDP context request message to the S3A. Then, the S3A forwards this request to the GGSN, replacing the control plane address[1] of the SGSN or TTG by its own. The IP address of the S3A is returned to the UE in the Accept message, thanks to the PCO field[2]. The PCO value is stored by the terminal and inserted in NAS messages in the target Radio Access Technology, allowing to retrieve the previously selected Serving-3gpp-Anchor.

6.2.2.3.2 First PDP context activation on the GERAN/UTRAN side

The current Radio Access in use is GERAN (or UTRAN) and the UE is attached. The scenario below describes the first activate PDP context procedure:

1. The UE sends Activate PDP context request to the SGSN, as defined in 3GPP TS 24.008. This PDP context has not yet been activated on any access, and so no "S3A_ADDR container" is set in the Protocol Configuration Options (PCO) field.
2. Since the SGSN is unchanged, it processes Activate PDP context request as defined in 3GPP TS 23.060 and 3GPP TS 29.060. The APN resolution provides the SGSN with a list of IP addresses of S3A. The SGSN sends a Create PDP context request to a selected S3A.
3. The S3A receives the Create PDP context request without S3A_ADDR container within the PCO information. So, the S3A creates a "PDP context" and among others:
    - It stores the parameters related to the Gn signalling (IP address of SGSN and TEID for signalling), as well as the source IP address of the received request, in GERAN/UTRAN Termination;
    - It allocates a TEID for GTP signalling for the Network Termination.

Then a DNS query may take place to translate FQDN (APN) into a GGSN IP address. The S3A replaces the received IP address and the TEID for GTP-C (signalling) with those of the S3A Network Termination and sends Creates PDP context request to the GGSN.

Depending on operator's configuration with regards to the user plane path rules, the IP address and TEID for GTP-U (user plane) remain those provided by the SGSN or they are replaced by S3A IP addresses and TEID for GTP-U.

4. The GGSN processes Create PDP context request as defined in 3GPP TS 23.060 and 29.060.
5. Upon receiving the response from the GGSN, the S3A:
    - Stores the IP address and the TEID for GTP-C (signalling) of the GGSN.
    - Creates a Protocol Configuration Options field or appends to the existing Protocol Configuration Options field a S3A_ADDR container set with S3A IP address.
    - Sends a Create PDP context response back to the SGSN with its own TEID and IP address for control plane and GGSN TEID and IP address for user plane[3].

---

[1] Depending on operator's configuration with regards to the user plane path rules (whether the user plane goes through the S3A or not), the user plane may go through the S3A. In this case, the S3A replaces the user plane address[1] of the SGSN or TTG by its own too.

[2] The Protocol Configuration Options (PCO) information element may be included in the request when the UE provides the GGSN with application specific parameters; here it provides the S3A_ADDR. The SGSN or TTG shall copy the content of this IE transparently from the content of the PCO IE in the Create PDP context request message or Create Secondary PDP context request.

[3] If the user plane passes through the S3A then the S3A sends back to the SGSN a Create PDP context response with its own TEID and IP address for control and user planes.

6. The SGSN returns Activate PDP Context Accept to the UE. The UE has to store the IP address of the S3A for the next handover.

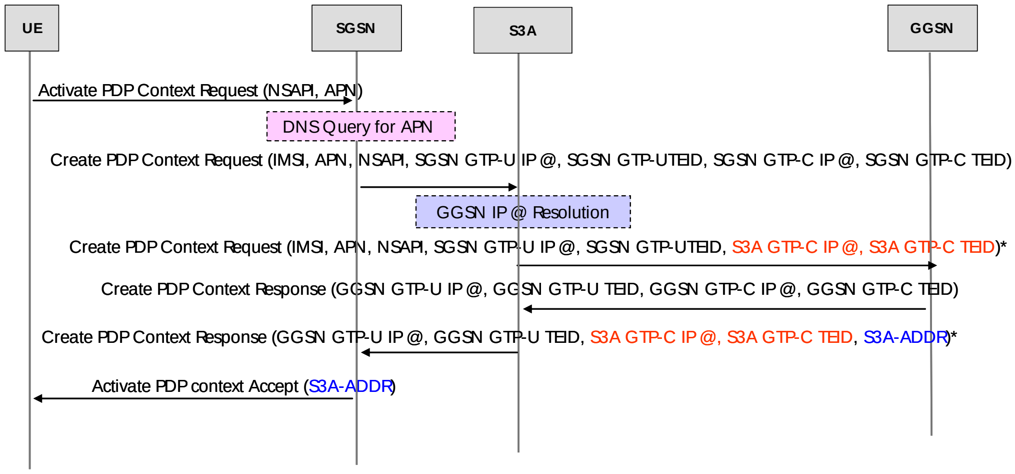


Figure 6.2.10 First PDP context activation on the GERAN/UTRAN side

6.2.2.3.3 First PDP context activation on the I-WLAN side

The current Radio Access in use is WLAN and the UE successfully performed an IPSec Tunnel establishment[4] with the TTG. This scenario below describes the first PDP context activation procedure:

1. The UE sends an Activate PDP Context Request to the TTG. This PDP context has not yet been activated on any access, and so no "S3A_ADDR container" is set in the Protocol Configuration Options (PCO) field. A GRE "key" (tunnel id) is allocated by the UE for user plane downlink traffic and provided within the request.
2. Upon the reception of the Activate PDP Context Request, the serving TTG performs User Authorization for that APN. Then the TTG initiates a Create PDP Context Procedure. The APN resolution provides the TTG with a list of IP addresses of S3As. The TTG sends Create PDP context request to a selected S3A.
3. The S3A receives the PDP Context Creation Request without S3A_ADDR container within the PCO information, then it creates a PDP context and among others:
    - It stores the parameter related to the Gn signalling (IP address of TTG and TEID for signalling);
    - It allocates a TEID for GTP signalling for the Network Termination.

   After, a DNS query may take place to translate FQDN (APN) into a GGSN IP address. Then, the S3A sends Creates PDP context request to the GGSN with the IP address and TEID for GTP-U (user plane) provided by the TTG[5] and its IP address and the TEID for GTP-C (signalling).
4. The GGSN processes Create PDP context request as defined in 3GPP TS 23.060 and 29.060: it returns Create PDP context response to the S3A.
5. The S3A stores the IP address and the TEID for GTP-C (signalling) of the GGSN. The S3A sends back to the TTG, a Create PDP context response but:
    - Replaces the control TEID and IP address of the GGSN by its own control TEID and IP address[6],
    - Creates a Protocol Configuration Options field or appends to the existing Protocol Configuration Options field a S3A_ADDR container set with the S3A IP address.

[4] Upon reception of the Tunnel Establishment Request, the TTG contacts the AAA server for authentication. The AAA server uses service authorization information to start EAP procedures and establish the IPSec tunnel between the UE and the TTG.

[5] If the user plane passes through the S3A then the S3A sends a Create PDP context request with its own TEID and IP addresses for control and user planes.

[6] If the user plane passes through the S3A then the S3A sends back to the TTG a Create PDP context response with its own TEID and IP addresses for control and user planes.

6. At the end of the procedure, the TTG returns an Activate PDP context accept including the new IP address of S3A in the S3A_ADDR container in the PCO field as received as well as the " GRE key" and IP address of its selected GRE tunnel for uplink traffic.

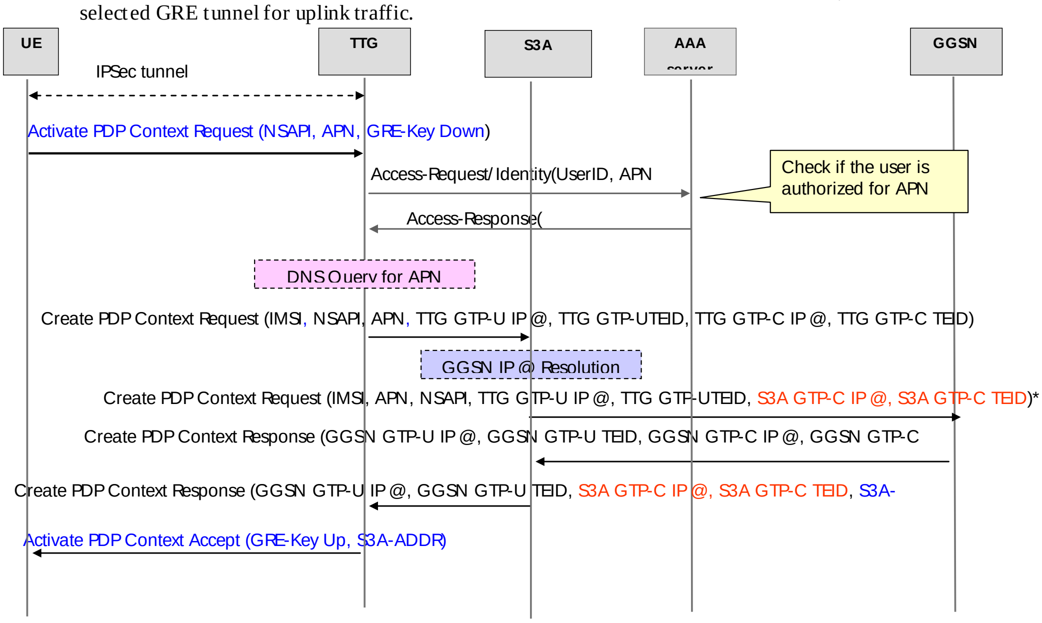


Figure 6.2.11 First PDP context activation on the I-WLAN side

6.2.2.3.4 Handover from WLAN to GERAN/UTRAN

The UE has an active PDP context. A handover procedure is initiated on the UE side due to some radio environment-based trigger. The following flow chart describes how active PDP contexts are maintained in a seamless manner.

1. The UE sends Activate PDP context request to the SGSN. It inserts S3A_ADDR container received at the previous PDP context activate response, in Protocol Configuration Options.
2. The SGSN sends Create PDP context request to S3A. The destination IP address of this request is found thanks to DNS query on the APN. The APN resolution provides the SGSN with a list of IP addresses of S3A. The SGSN may select an "interim" S3A that is in charge of reading the S3A_ADDR and relays the request to the serving S3A specified in the S3A_ADDR.
3. The S3A selected by the SGSN, receives Create PDP context request, gets the IP address of the S3A thanks to the Protocol Configuration Option field that contains the S3A_ADDR; then it forwards[7] the Create PDP context request toward this S3A.
4. The S3A retrieves the PDP context (based on IMSI and NSAPI values), registers the parameters related to the Gn signalling (IP address of SGSN and TEID). The S3A sends Update PDP context request to the GGSN with the S3A IP address and TEID for GTP-C and the IP address and TEID for GTP-U (user plane): depending on operator's configuration (whether the user plane goes through the S3A or not), the IP address and TEID for GTP-U (user plane) remain those provided by the SGSN or they are replaced by S3A IP address and TEID.
5. Then, GGSN processes Update PDP context request as defined in 3GPP TS 23.060 and sends an Update PDP context response. Now, the downlink traffic is sent to the SGSN.
6. The S3A sends Create PDP context response back to the SGSN with its own TEID and IP address for control plane and GGSN TEID and IP address for user plane[8].

---

[7] This behaviour takes on the first request only, the "interim" S3A is not involved in further requests, which are directly routed between SGSN and S3A anchor.

[8] If the user plane passes through the S3A then the S3A sends back to the SGSN a Create PDP context response with its own TEID and IP addresses for control and user planes.

7. The SGSN returns Activate PDP context accept to the UE.

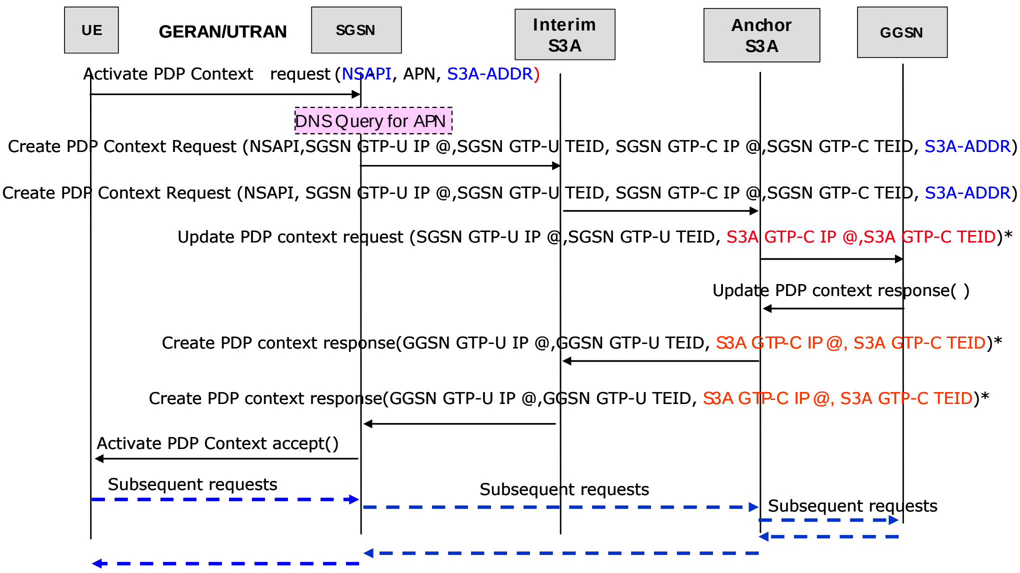


Figure 6.2.12 Handover from WLAN to GERAN/UTRAN

6.2.2.3.5 Handover from GERAN/UTRAN to WLAN

The handover procedure is initiated on the UE side due to some radio environment-based trigger. The following flow chart describes how active PDP contexts are maintained in a seamless manner:

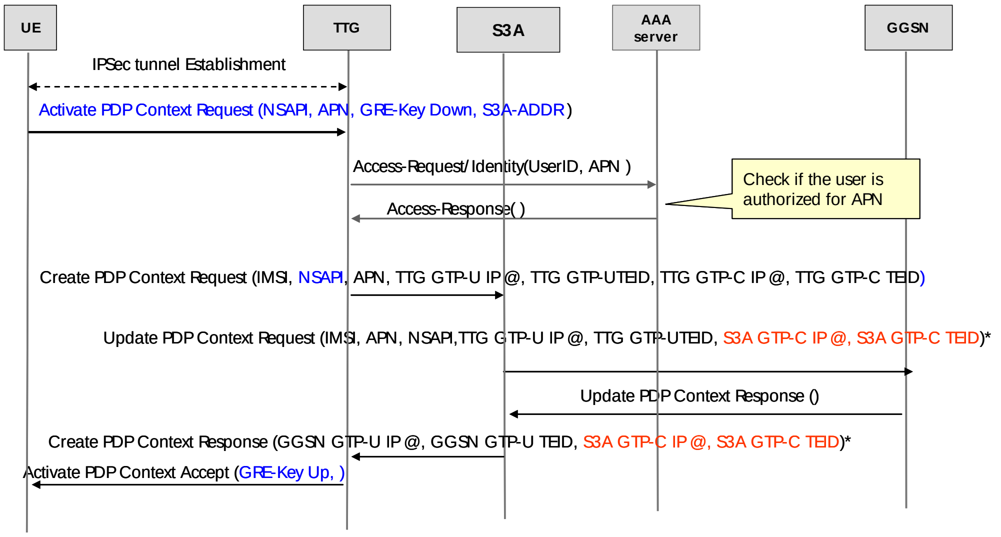
1. At first, the UE performs an IPSec Tunnel establishment[9] with the TTG if it does not exist.
2. The UE sends Activate PDP Context Request to the TTG with the stored IP address of the S3A in "S3A_ADDR container" set in the Protocol Configuration Options (PCO) field. A GRE "key" (tunnel identity) is allocated by the UE for user plane downlink traffic and provided within the request.
3. Upon reception of Activate PDP Context Request, the serving TTG performs User Authorization for that APN. Then, the TTG gets IP address of anchor thanks to S3A_ADDR, and sends Create PDP context request to the S3A.
4. The S3A retrieves the PDP context (based on IMSI and NSAPI), stores the parameters related to the Gn signalling (IP address of TTG and TEID). Then, it sends Update PDP Context Request to the GGSN with the IP address and TEID for GTP-U (user plane)[10] provided by the TTG.
5. The GGSN processes Update PDP Context Request and returns Update PDP Context Response. Now, the downlink traffic is sent to the TTG.
6. The S3A sends Create PDP Context Response back to the TTG with its own TEID and IP address for control plane and the GGSN IP address and TEID[11].
7. The TTG returns Activate PDP Context Accept including the GRE key and IP address of its selected GRE tunnel (uplink traffic), towards the UE.

---

[9] Upon reception of the Tunnel Establishment Request, the TTG contacts the AAA server for authentication. The AAA server uses service authorization information to start EAP procedures and establish the IPSec tunnel between the UE and the TTG.

[10] If the user plane passes through the S3A then the S3A sends an Update PDP context request with its own TEID and IP addresses for control and user planes.

[11] If the user plane passes through the S3A then the S3A sends back to the TTG a Create PDP context response with its own TEID and IP addresses for control and user planes.



*Depending on operator's configuration with regards to the user plane path rules, the user plane may go through the S3A . In this case, the S3A sends an Update PDP context request / Create PDP context response with its own TEID and IP addresses for control and user planes.

Figure 6.2.13 Handover from GERAN/UTRAN to WLAN

6.2.2.3.6 PDP context de-activation on the GERAN/UTRAN side

The UE proceeds with the deletion of the PDP context as defined below:

1. Since the PDP context is active on the GERAN/UTRAN side only, the UE initiates Deactivate PDP context request towards the SGSN as defined in 3GPP TS 24. 008.
2. Since the SGSN is unchanged, it processes the de-activate PDP context request as defined in 3GPP TS 23.060 and 3GPP TS 29.060: it sends Delete PDP context request to the S3A.
3. The S3A receives the Delete PDP context request, retrieves the PDP context parameters and initiates Delete PDP context request towards the GGSN.
4. Since the GGSN is unchanged, it processes Delete PDP context request as defined in 3GPP TS 23.060 and 3GPP TS 29.060: it sends Delete PDPD context response to the S3A.
5. The S3A forwards Delete PDP Context Response towards the SGSN and releases all the resources related to this PDP context.
6. If the WLAN Access Termination is still active, the S3A sends Delete PDP Context Request to the TTG.
7. The SGSN sends De-activate PDP Context Response to the UE.

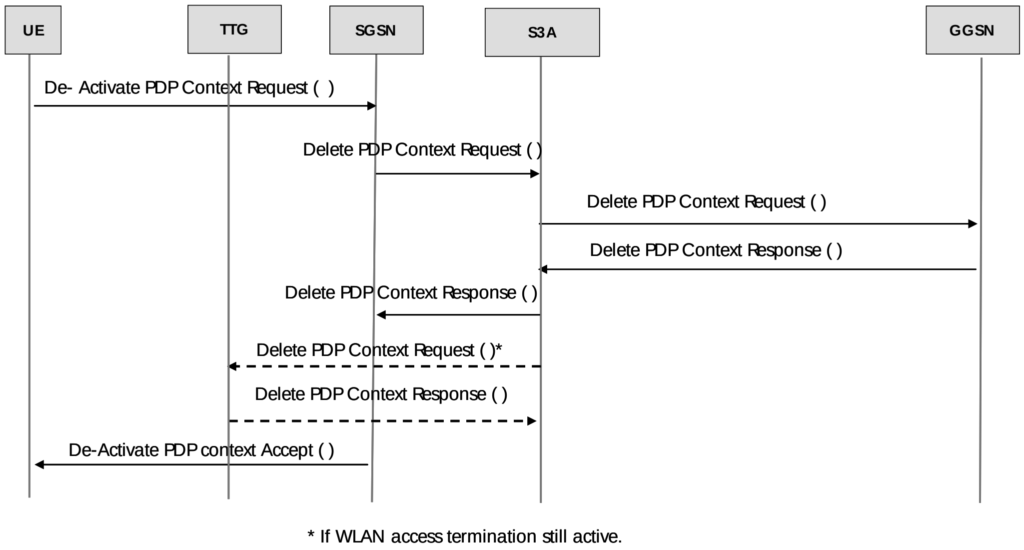


Figure 6.2.14 PDP context de-activation on the GERAN/UTRAN side

6.2.2.3.7 PDP context de-activation on the WLAN side

The UE proceeds with the deletion of the PDP context as defined below:

1. Since the PDP context is active on the WLAN side, the UE sends Deactivate PDP context request to the TTG.
2. The TTG retrieves the PDP context then sends Delete PDP context request to the S3A.
3. The S3A receives the Delete PDP context request and initiates Delete PDP context request towards the GGSN.
4. Since the GGSN is unchanged, it processes Delete PDP context request as defined in 3GPP TS 23.060 and 3GPP TS 29.060: it sends Delete PDP context response.
5. The S3A forwards Delete PDP context response towards the TTG and releases all resources related to this PDP context.
6. The TTG sends De-activate PDP context response to the UE.
7. If the GERAN/UTRAN Access Termination is still active, the S3A sends Delete PDP Context Request to the SGSN.
8. The SGSN returns Delete PDP Context Response to the S3A.

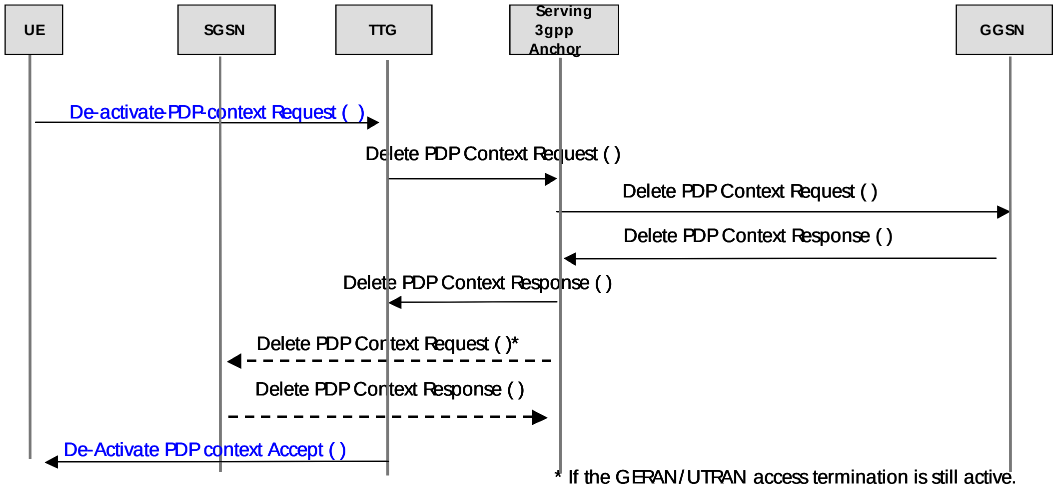


Figure 6.2.15 PDP context de-activation on the WLAN side

6.2.3 Alternative C

6.2.3.1 The Architecture

The proposed architecture for the non-roaming case is shown in the following figure 6.2.16. Within this proposal it is assumed that DSMIPv6 is used to provide mobility between pre-SAE and I-WLAN. A Home Agent is connected to the GGSN and PDG through Gi and Wi interfaces. The Home Agent may be co-located with GGSN or PDG and terminates the DSMIPv6 signalling [3] within the network.

The two involved access networks, the 3GPP access network and the 3GPP-WLAN interworking access network, are kept separately and no direct interworking between them is proposed. Also no changes are needed for the defined initial attach, session set-up, etc. procedures within the two different access systems. The UE has to initiate DSMIPv6 specific signalling towards the Home Agent to create a binding in the HA and to register its care-of-address. This will on one side establish the DSMIPv6 tunnel between the HA and the UE and on the other side ensure that mobile terminated traffic is routed by the HA towards the correct access network.

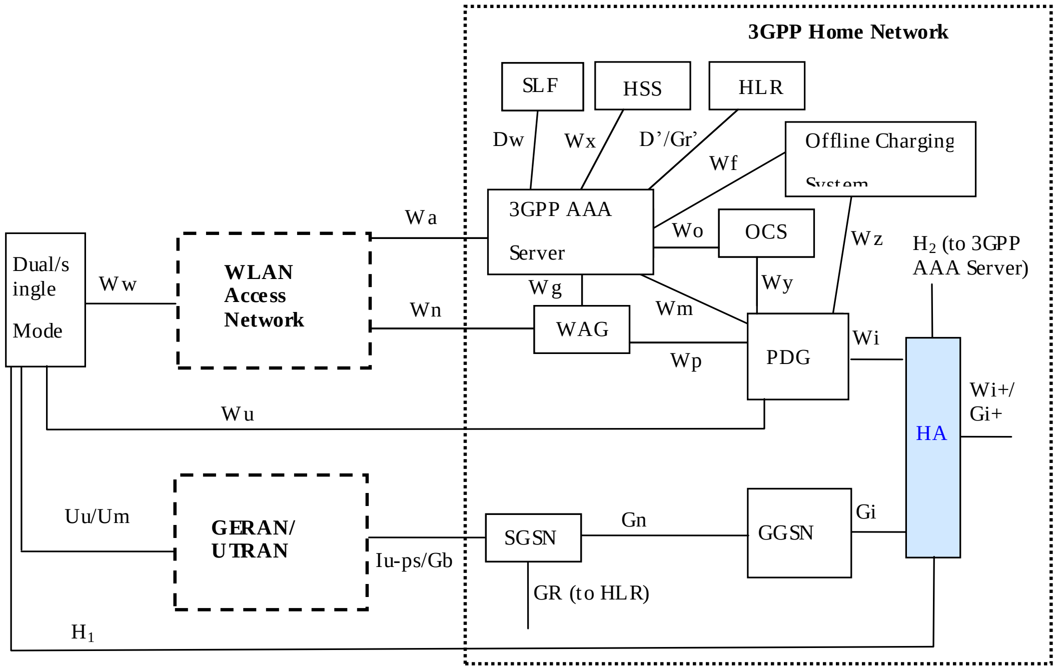


Figure 6.2.16 Alternative Non-Roaming Architecture for I-WLAN Mobility

In the proposed architecture, the following enhancements are needed to enable I-WLAN mobility.

- Home Agent:
  Home Agent functionality has to be added to the 3GPP Home Network. This functionality could be realized in a stand-alone entity, or co-located with either the GGSN or PDG (details of co-location are FFS). The Home Agent will communicate with the UE and exchange DSMIPv6 related signalling to keep track about the access network the UE is recently camping on. This signalling is transparent to GGSN and PDG.

- Dual Mode/Single Mode UE:
  The UE needs to be enhanced by a DSMIPv6 Client to enable the DSMIPv6 based signalling towards the Home Agent. The proposed solution is able to support both types of UE, dual mode and single mode UEs. In case that a single mode UE will be used, seamless service continuity is not possible.

- GGSN, PDG:
  In general (HA not co-located with GGSN and PDG) no changes to GGSN and PDG are required, i.e. all of the existing procedures could be used as already defined for GPRS and I-WLAN. Due to the fact that the DSMIPv6 signalling is transparent for the GGSN as well as for the PDG no specific MIP functionality is needed on both entities.

Wi+/Gi+: this reference point defines the interface from the HA outwards (whereas Gi and Wi are within this mobility architecture).

H_1: this is the reference point for mobility signalling between UE and HA.

H_2: this reference point defines the interface between HA and 3GPP AAA server and is used for authentication of mobility signaling.

The corresponding architecture for the roaming case for home routed traffic is provided within figure 6.2.17.

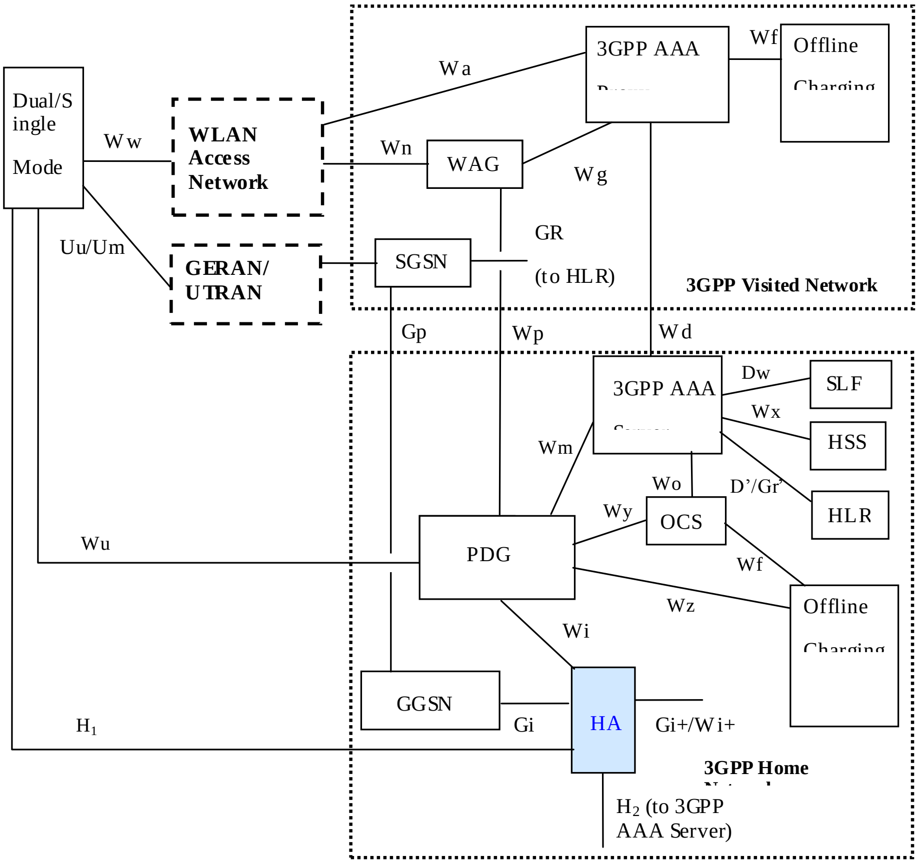


Figure 6.2.17 Alternative Roaming Architecture (with home routed traffic) for I-WLAN Mobility

A roaming scenario with e.g. PDG in VPLMN and GGSN in HPLMN, or vice versa, is theoretically possible but seems impractical and is therefore not considered. It can be excluded by suitable configuration of DNS for (W-)APN resolution.

The proposed architecture provides an easy migration to the SAE architecture for mobility and session continuity, as it is inline with solutions to be described in TS 23.402[9].

6.2.3.2 Initial Attachment in I-WLAN and Subsequent Handover to GPRS

The information flow for initial attachment in I-WLAN and subsequent handover to GPRS is shown in figure 6.2.18 for the non-roaming case (HSS and 3GPP AAA server are left out for simplicity).

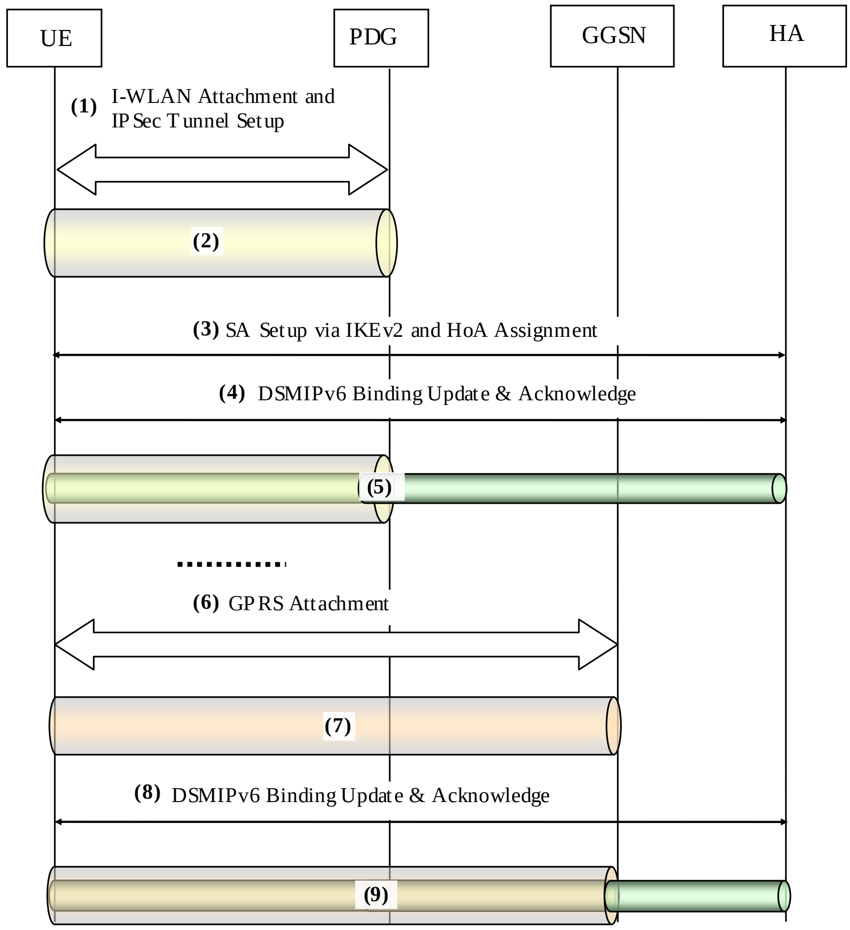


Figure 6.2.18 Information Flow for Initial Attach in I-WLAN and Subsequent Handover to GPRS (non-roaming case)

The following steps are performed:

(1) I-WLAN attachment and IPSec tunnel setup is executed according to TS 23.234 and TS 33.234. As a prerequisite a local IP address has been assigned by the WLAN access network to the UE. This step includes selection of a PDG via resolution of the W-APN.

(2) The result is an established IPSec tunnel between UE and PDG, and an IP address from the PDG's range is assigned to the UE (Remote IP address). Dynamic IP address assignment shall be used.

(3) A security association is setup between MN and the HA, based on IKEv2. The HA assigns a HoA to the UE and delivers it in the configuration payload of the corresponding IKEv2 signalling. The method by which HA is known to the UE is left FFS.

(4) A DSMIPv6 [3] Binding Update (BU) message is sent to the HA, where the Remote IP address is used as the CoA. The HA authenticates the BU message, creates an entry in its binding cache and sends a Binding Acknowledgement (BA) back to the UE.

Editor's note: The use of IETF RFC 4285 [4] is FFS. When it is used the procedure will be different.

(5) The result is a DSMIPv6 tunnel between UE and HA (inside the IPSec tunnel between UE and PDG), and UE is now able to transfer data.

(6) The dual mode UE when having GPRS coverage, may then decide to attach to the GPRS network using standard GPRS procedures according TS 23.060, and to establish a PDP context. It includes selection of a GGSN and assignment of an IP address to the UE (another Remote IP address for the GPRS domain). The GGSN allocates a suitable Remote IP address from its own range. Dynamic IP address assignment shall be used.

(7) GPRS connectivity (GTP tunnel and GERAN/UTRAN radio connection) is finally established and the UE may transfer data in uplink direction via this access.

(8) Another DSMIPv6 BU message for the previously assigned HoA is sent to the HA, where the Remote IP address from the GPRS access is used as the CoA. The HA authenticates the BU message, modifies the entry in its binding cache and sends a BA back to the UE.

(9) As a result the DSMIPv6 tunnel is modified, and it is inside the GPRS tunnel and GERAN/UTRAN radio connection between UE and GGSN.

Note: On this level of detail the roaming cases (both PDG and GGSN in VPLMN or both in HPLMN) show no difference and are thus not shown. A roaming scenario with PDG in VPLMN and GGSN in HPLMN, or vice versa, is theoretically possible but seems impractical and is therefore not considered.

6.2.3.3 Initial Attachment in GPRS and Subsequent Handover to I-WLAN

The information flow for this case is shown in figure 6.2.19. It is quite similar (or rather mirrored) to the above case, as some symmetry is observed between I-WLAN and GPRS access. The steps thus do not need further textual explanation.

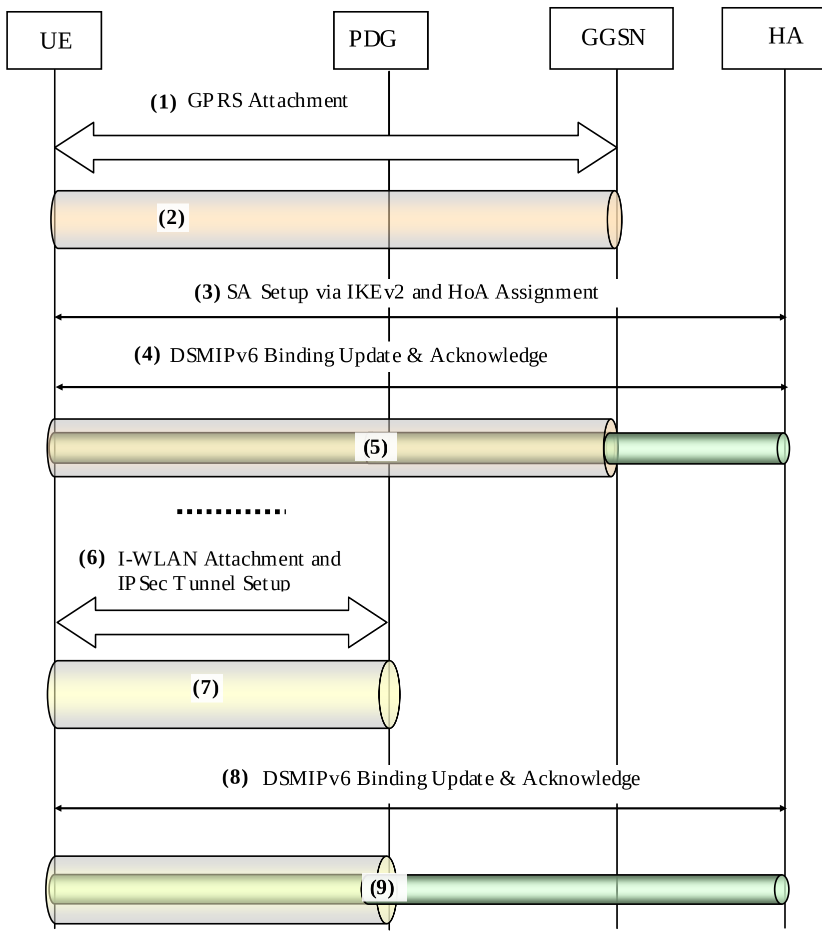


Figure 6.2.19 Information Flow for Initial Attach in GPRS and subsequent Handover to I-WLAN (non-roaming case)

6.2.3.4 Characteristics of this Solution

The selection procedures for GGSN and PDG are unchanged. Specific configuration of APNs may optimize the procedures.

Note that both the IPSec tunnel in I-WLAN and the GPRS PDP context serve as a "virtual" layer 2 between UE and PDG, ores. UE and GGSN. In both cases dedicated signalling is performed, which obsoletes any Router Solicitation/Advertisement messages.

In I-WLAN the UE has to handle three IP addresses (local, remote and home address) and store the HA address.

The procedure can easily be extended for multiple tunnels. If in I-WLAN multiple IPSec tunnels were established prior to handover to GPRS (corresponding to multiple HoA's) they shall be mapped one by one to primary PDP contexts. If several secondary PDP contexts in the GPRS access were established prior to handover to I-WLAN in the simplest case they may be mapped to one IPSec tunnel, but it would then not allow to continue with differentiated QoS handling in the I-WLAN case. Alternative solutions are FFS.

This solution works for IPv4 only and IPv6 only networks, if the HA is DS capable and I-WLAN and GPRS IP connectivity access networks (IPCAN) support the corresponding IP version. MIP signalling and tunnelling is then performed according to [5] or [6]. It works also in case an IPCAN supports only IPv4 addressing and an IPv6 HoA is required; MIP signalling and tunnelling is then performed according to [3].

The solution has minimal impact on UEs: UE's need only a DSMIP client, and the logic for initiating and finalizing the handover.

This solution does not have any impact the existing PDG and GGSN functionality and the existing procedures within I-WLAN and GPRS, i.e., legacy GGSN and PDG implementations can be used.

6.2.4 Alternative D

6.2.4.1 The Architecture

Figure 6.2.20 shows the architecture for a pre-SAE GPRS-IWLAN mobility solution based on the MIPv4 FA protocol. The new or modified reference points with respect to REL-7 baseline architecture are shown in blue ink. The GGSN and the PDG contain a Foreign Agent (FA) functionality.

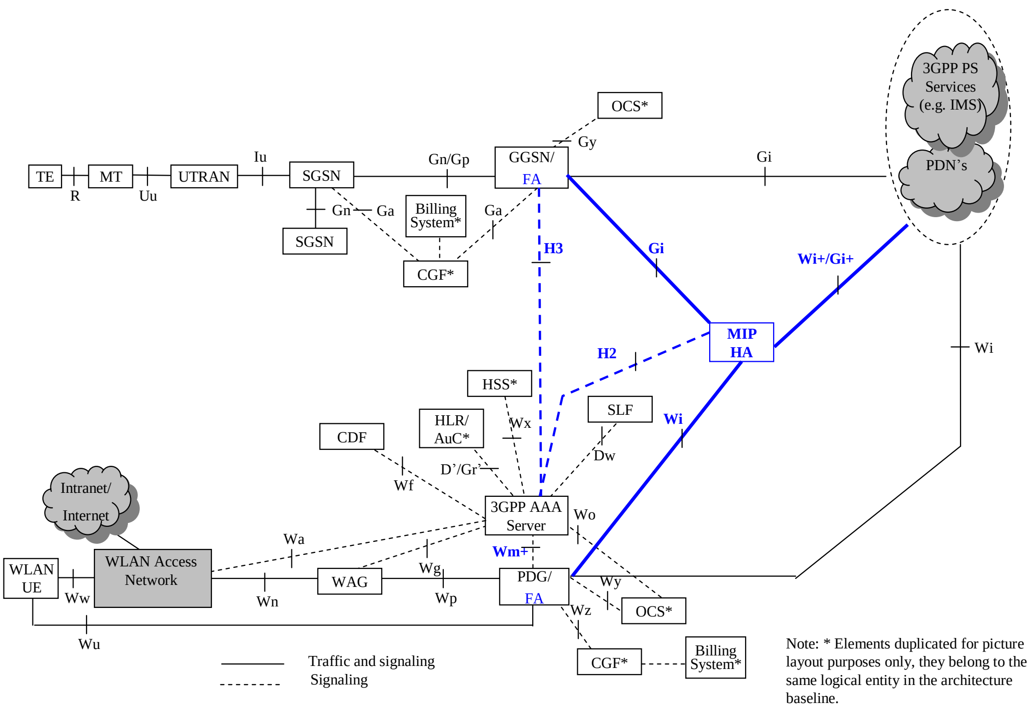


Figure 6.2.20 Solution for GPRS-IWLAN mobility based on the MIPv4 FA protocol

Listed below are all new or modified reference points with respect to the baseline architecture:

- **H2**: this is the reference point between the MIP HA and the 3GPP AAA server. It is used during setup of security associations and for authentication of mobility signalling.
- **H3**: this is the reference point between the GGSN and the 3GPP AAA server. It is used by the Diameter Mobile IP application, RFC 4004 [x], for dynamic assignment of a MIP HA, as well as during setup of security associations (MN-HA, MN-FA, FA-HA);

- **Wm+**: this is an enhancement to the existing Wm reference point. The additional functionality is similar to the H3 functionality described above.

For further details on this solution the reader may refer to Annex A, noting that some of the reference points have different names as follows: H2, H3, Gi, Wi and Gi+/Wi+ in this section correspond to Rha-aaa, Gi-aaa, Gi+, Wi+ and Gi/Wi in Annex A, respectively.

Formatted: B1

6.3 6.3 Comparisons

Formatted: Bullets and Numbering

6.3.1 Evaluated solutions

Formatted: Heading3;H3;H31;H32;H33;H34;H35;h3;Underrubrik2;E3;no break, No bullets or numbering

Solution A

In the solution A proposal: the TTG' is the 2G/3G and I-WLAN anchor point for both control and user plane. It is based on GTP tunneling and proposes to use simple mobility mechanisms that are possible because of two simultaneous radios and of IPsec tunneling between UE and network: there is no need for GPRS/UMTS Mobility Management, in particular no need for neither LA/RA nor context transfers. This solution allows the support of multiple PDP contexts (primary and secondary) for a given APN, and also supports multiple APN, but via multiple IPsec tunnels and via triggering PDP context activations. When the UE is in GPRS network, the TTG' either works as a GGSN or a proxy GSN. When the UE is in the WLAN, the TTG' terminates the IPsec tunnel. The TTG' maintains the session information and carries out the handover.

Solution B

In the Solution B proposal: the GGSN is the 2G/3G and I-WLAN user plane anchor point while a new node S3A entity which could be collocated with the TTG is the control plane anchor point. It is based on GTP tunneling and proposes to use simple mobility mechanisms that are possible because of two simultaneous radios and of IPsec tunneling between UE and network. There is no need for GPRS/UMTS Mobility Management (no need for neither LA/RA nor context transfers). This solution allows the support of multiple PDP contexts (primary and secondary) for a given APN, and also supports multiple APN, via a single IPsec tunnel and via triggering PDP context activations thanks to a simple UE-TTG Session Management protocol. This proposal introduces a NAS Session Management protocol (W-SM) between the UE and the TTG to replace multiple IPsec tunnels by one single IPsec tunnel established at authentication. This solution avoids multiple IPsec tunnel and would allow the maintain of original QoS profile for running sessions when the UE moves between WLAN and GPRS

Solution C

In the solution C proposal the mobility management solution is based on the Dual Stack MIPv6 and the innovation of this proposal resides in the capability of the UE is to use either IPv4 or IPv6 addresses as home addresses. This solution does not include the description of any roaming solution with the associated charging mechanisms. The solution does not specify any access authentication and authorization procedure, which, if was specified would necessarily bring modification to the network architecture. There are some other drawbacks of this solution, the UE and the HA need to have a DSMIPv6 stack. The systematic MIP tunnel in the WLAN adds a significant overhead to the already existing IPsec tunnel. The drawback associated with this solution is the lack of commercial implementations available today.

Solution D

In the solution D proposal: session continuity is handled by MIP (v4/v6) as the UE is moving between GPRS and WLAN AN. The new architecture which introduces a HA requires no change to the legacy PDG and GGSN entities. The drawbacks of this solution include the incapacity for a UE to move between IPv4 and IPv6 networks. Access authentication procedures for the UE have not been specified either. Moreover QoS differentiation has not been addressed for WLAN access. The other one is the overhead of MIPv4 in the WLAN domain when the FA is not an element of the architecture. The HA is a new node introduced in the core network. This has strong impact on provisioning and packet forwarding delay.

6.3.2 Technical assessment

The following table attempts to provide comparison among those solutions based on the proposed comparison criteria as presented previously in a separate contribution. It is important to note that these comparisons are the results of initial analysis on the solutions instead of approved operational experiences in existing networks.

	Alternatives	A	B	C	D
1	- Support continuity of 3GPP and Internet services including multiple simultaneous sessions across different access networks [yes, no]	Yes • It supports Gi and Wi interfaces. • Multiple simultaneous sessions (included primary/secondary PDP context) supported thanks to multiple IPSec tunnel implementation.	Yes • Only Gi interface being support. • Multiple simultaneous sessions (included primary/secondary PDP context) supported thanks to the introduction W-SM (NAS session protocol in WLAN)	Yes • Support both Gi and Wi interface. • Multiple simultaneous sessions (included primary/secondary PDP context) not supported (due to one MIP instance + one IPsec tunnel)	Yes • Support both Gi and Wi interface. Multiple simultaneous sessions (included primary/secondary PDP context) not supported (due to one MIP instance + one IPsec tunnel)
2	- Migration complexity from R6/R7 I-WLAN and PS networks to R8 (with I-WLAN Mobility enabled)	• Configuration DNS+HSS for APN list (The operator's DNS entry and subscribed APN needs to be modified). • Upgrade of TTG	• Configuration DNS+HSS for APN list (The operator's DNS entry and subscribed APN needs to be modified). • Upgrade of TTG	• Upgrade of 3GPP AAA server for mobility security • Add HA node	• Upgrade of 3GPP AAA server for mobility security • Upgrade of GGSN & PDG for MIPv4 and mobility security function • Add HA node
3	- Migration complexity from Rel. 8 (with I-WLAN Mobility enabled) to SAE	• TTG' would evolve to ePDG with PMIPv6 interface to the PDN GW instead of existing Gn interface to GGSN.	• Compliant with SAE solution: S3A function could be integrated in S-GW • The NAS layer will not be reused in SAE, i.e. It is specific to this solution	• Compliant with SAE solution: DSMIPv6	• Compliant with SAE solution: MIPv4, MIPv6.

Formatted: Heading3;H3;H31;H32;H33;H34;H35;h3;Underrubrik2;E3;no break

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

4	- **3GPP procedures consistency (e.g. Authentication, charging & billing and Lawful interception)**	• 3GPP authentication, charging & billing and LI procedures are fully complied with. • GTP, IKEv2, EAP-SIM, AAA protocols are widely used *Note: Network triggered PDP context support is FFS.*	• 3GPP authentication, charging & billing and LI procedures are fully complied with. • GTP, IKEv2, EAP-SIM , AAA protocols are widely used *Note: Network triggered PDP context is supported to thanks to NAS session management*	• 3GPP procedures need to be evolved to provide authentication, charging & billing functions for the MIP based solution. • L.I. in separated nodes or in additional node (impacts FFS). • Impact on the PCRF is FFS *Note: Network triggered PDP context support is FFS.*	• 3GPP procedures need to be evolved to provide authentication , charging & billing and LI functions for the MIP based solution. • Impact on the PCRF is FFS *Note: Network triggered PDP context support is FFS.*
5	- **Minimal impact and upgrade on the dual mode UE**	• The UE needs to be capable of using the same address across GPRS and I-WLAN.	• The UE has to support specific layers for I-WLAN mode: W-SM and TCP layers for signalling plane, IETF GRE tunnelling for user plane.	• The UE needs to support a Dual stack MIP client.	• MIP client required on the UE.
6	- **Transmission efficiency, in terms of overhead, on radio link and the last mile network links**	• No overhead on GRPS radio link	• No overhead on GRPS radio link	• DSMIPv6 works in collocated mode thus, the MIPv6 tunnel between the UE and the HA introduces an overhead over the GPRS radio link. (MIP overhead disappears if the GPRS core network is considered as the Home network) & IWLAN	• MIP introduces overhead on both GPRS and IWLAN radio link in collocated mode. • MIP overhead disappears when the FA is implemented.

Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering

7	- **Minimal Impact to the GPRS Core and I-WLAN network (modifications or additional nodes)**	• No impact to GGSNs • New node TTG' based on evolved TTG) • Additional support of Gn/Gp interface between SGSN and TTG' NOTE: Insertion of a new node in the GPRS GTP-C (and potentially GTP-U) path. *Note: mechanism to retrieve the TGG' by the SGSN during HO is FFS.*	• No impact to SGSNs • No impact to GGSNs • New function S3A in TTG • New interface Wu' (evolved Wu to support the W-SM protocol and GRE tunnel management for user plane downlink traffic) • Additional support of Gn/Gp interface between TTG'-SGSN	• No impact on GPRS infrastructure. • Interfaces between various nodes (e.g. GGSN, PDG, HA and AAA server, etc) need to be specified and implemented. • DS-MIPv6 requires availability of a dual stack HA which is not a requirement in R6 Note: The DSMIPv6 is only a draft and not yet any available implementation	• No impact on GPRS infrastructure except if HA or FA is co-located to GGSN/PDG. • The interface between HA and PDG, needs to be standardised • New interfaces Wm+ (evolved Wm), H2, H3
8	- **Support for dual radio operation** **[yes, no]**	Yes • The path on the new access system is established before the deletion of the old path. • The handover can be performed without any service disruption from user perspective	Yes • The mobility mechanism consists in a make-before-break handover by establishing a second leg in the target RAT, switching the leg by the GGSN then releasing the first leg in the old RAT	Yes • Minimizing the MIP handover latency is enabled by capability to send and receive data on one interface while the UE is registering on the new interface. This reduces packet loss during I-WLAN handover. • Simultaneous binding is available neither in MIPv6 nor in DS-MIPv6. DS-MIPv6 does not guarantee zero packet loss.	Yes • Minimizing the MIP handover latency is enabled by sending and receiving data on one interface while the UE is registering on the new interface. This reduces packet loss during I-WLAN handover. • Eliminating packet loss can further be achieved by the creation of simultaneous bindings at the HA and duplication of packets. This

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

					is enabled in MIPv4 with the Simultaneous Bit (S bit) in the Registration Request
9	- Mobility support in the roaming situation, with the re-use of operator's current roaming architecture, interfaces and protocols [yes, no]	Yes • Roaming interface Gp is reutilised.	Yes • Roaming interface Gp is reutilised.	Yes • I-WLAN roaming agreement can be re-used • New roaming agreement needed if the PDG/GGSN and HA are in different PLMN. •	Yes • I-WLAN roaming agreement can be re-used • New roaming agreement needed if the PDG/GGSN and HA are in different PLMN. •
10	- Support for both IPv4 and Ipv6 sessions [yes, no]	Yes	Yes.	Yes • The UE is able to use an IPv4 and IPv6 home or care-of address simultaneously. Capable to maintain a session when handing over between IPv4 and IPv6 networks.	Yes • Two different architectures depending on whether MIPv4 or MIPv6 is supported
11	- Possible operator control of I-WLAN Mobility (commanded by the network) [yes, no] Note: refers to the possibility for the network to request to the UE to attach to another RAT according to operator policies	No	FFS • Possibly controlled by S3A (anchor point of signalling) thanks to enhancements of the protocol	No • Controlled by terminal only	No • Controlled by terminal only

Formatted: Bullets and Numbering

Formatted: Normal

7 Conclusion

Editor's note: depending on the progress and status of the SAE WI, the output of the SI may be considered to be either incorporated into SAE TS 's or TS23.234.

- The WI concludes that a TS should be formed with one of the solutions.
- The standard specification work is to be completed by end of 2007.

Formatted: Bullets and Numbering

Annex A: Mobility between pre-SAE/LTE 3GPP and non 3GPP access systems

A.1 General

The intent of this Annex is to study architectural solutions for session continuity and seamless mobility for 3GPP-WLAN Interworking in parallel to the study of the evolved system. The goal is to develop a feasible architectural solution for session continuity and seamless mobility for 3GPP-WLAN Interworking, which allows evolution towards the SAE architecture for mobility between access systems using 3GPP and non-3GPP radio.

A.2 Description of mobility between pre-SAE/LTE 3GPP and non 3GPP access systems

The term Access System is used here to designate one of the following:

- The GPRS IP access (including both the PS core network and the RAN),
- The WLAN 3GPP IP Access, or
- The WLAN Direct IP Access.

Currently there is no standard means for ensuring session continuity or seamless mobility between these two systems. Whenever the UE moves between the two, any established session will fail and will have to be tunnelled. The purpose of this clause is to study mobility solutions.

A.3 Solutions for mobility between pre-SAE/LTE 3GPP and non 3GPP access systems

This clause assumes that Mobile IP is used as mobility protocol for GPRS-WLAN mobility, whereas MOBIKE [8] is used for UE-PDG IPsec tunnel relocation within the WLAN 3GPP IP Access. It is assumed that the same solution applies for both session continuity (a.k.a. Scenario 4) and seamless mobility (a.k.a. Scenario 5), depending on the mobile's capability for simultaneous connections.

Note that in the subsequent text we use the traditional MIP terminology i.e. Mobile Node (MN), Foreign Agent (FA) and Home Agent (HA).

It is assumed that Home AAA in HPLMN is in charge of user authentication and authorization.

Figure A.1 is a simplified figure describing how the Diameter application for Mobile Ipv4, RFC 4004 [7], works in conjunction with the Mobile Ipv4 protocol. Depicted is the case where Mobile Ipv4 is used with Foreign Agent Care-of Address (FA-CoA). This requires a FA functionality within the Gateway (PDG or GGSN). The names associated with some interfaces (e.g. Wm+, Wd+, Gi-aaa, Rha-aaa, Gi+, Wi+) are clarified later in the text.

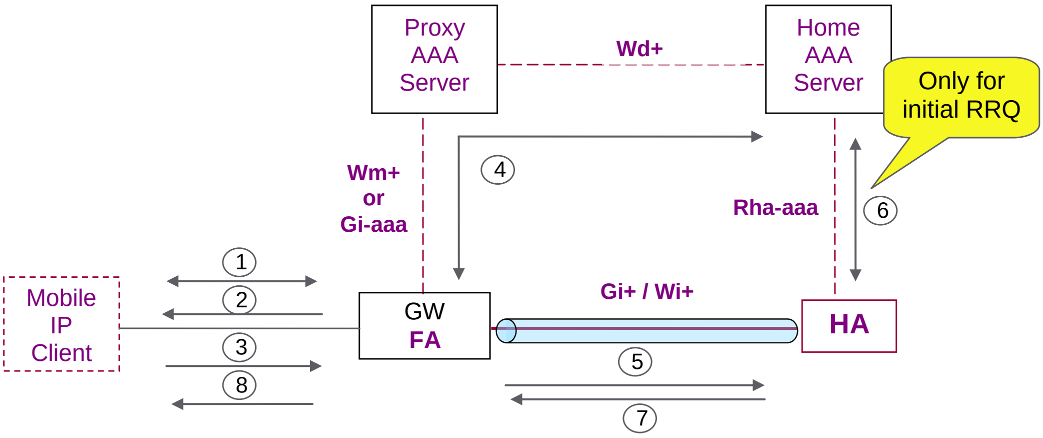


Figure A.1: Use of MIPv4 FA care-of address mode with Diameter application

The following are the subsequent steps described in Figure A.1 (for more details the reader may refer to RFC 4004 [7]):

1) The MN establishes a connection with the GW (i.e. GGSN or PDG);

2) The MIP Foreign Agent (MIP FA) function in the GW sends a FA advertisement;

3) The MN sends a MIP v4 Registration Request (RRQ);

4) The GW interrogates the user's Home AAA server in order to authenticate and authorise the user. In the roaming case, the GW uses the Proxy AAA to contact the user's Home AAA server. The Home AAA server assigns a Home Agent (HA) and provides the address of the assigned HA to the GW.

5) The FA forwards the MIPv4 RRQ to the MIP HA.

6) The HA fetches a pre-shared key for MN-HA authentication. This step is required only at session establishment. Specifically, it is not required for MN-HA authentication when the UE subsequently connects to other Fas.

7-8) The HA accepts the mobile registration by replying with a MIP v4 Registration Response (RRP).

Figure A.2 is a simplified figure describing how the Diameter application for Mobile Ipv4, RFC 4004 [7], works in conjunction with the Mobile Ipv4 protocol when no FA present (co-located care-of address mode). The names associated with some interfaces (e.g. Rha-aaa) are clarified later in the text.

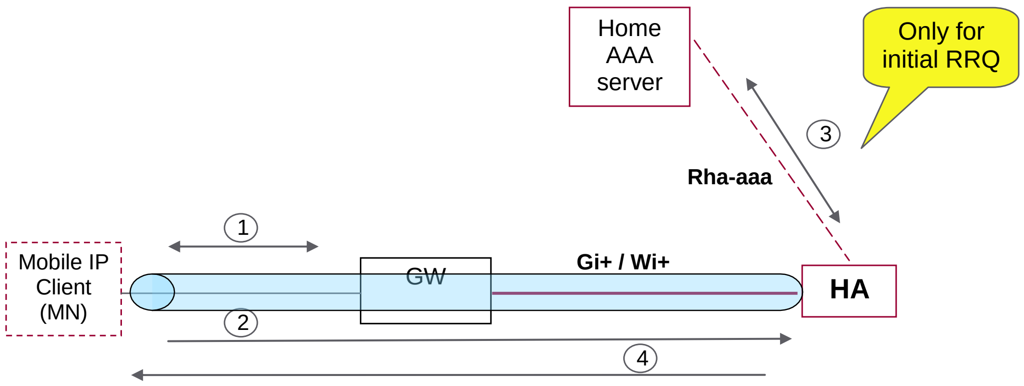


Figure A.2: Use of MIPv4 collocated care-of address mode with Diameter application when no FA is present

The following are the subsequent steps described in Figure A.2 (for more details the reader may refer to RFC 4004 [7]):

1) The MN establishes a connection with a GW (e.g. GGSN or PDG) or is otherwise assigned an IP address from an access network.

2) The MN sends a MIP v4 Registration Request (RRQ) to its HA transparently through the GW. The HA IP address may be discovered e.g. using DNS resolution of a HA FQDN, or through an agent advertisement, if the Home Agent is in the same link as the MN.

3) The HA contacts the AAA server to fetch authentication and keying information for the MN. This step is required at session establishment. Specifically, it is not required for MN-HA authentication when the UE makes subsequent registrations while the lifetime of the MN-HA keys is not due to expire.

4) The HA accepts the mobile registration by replying with a MIP v4 Registration Response (RRP).

Depicted in Figure A.3 is a simplified view on how a Diameter application may work in conjunction with MIPv6. The main difference wrt Ipv4 is the absence of Foreign Agent in the GW.

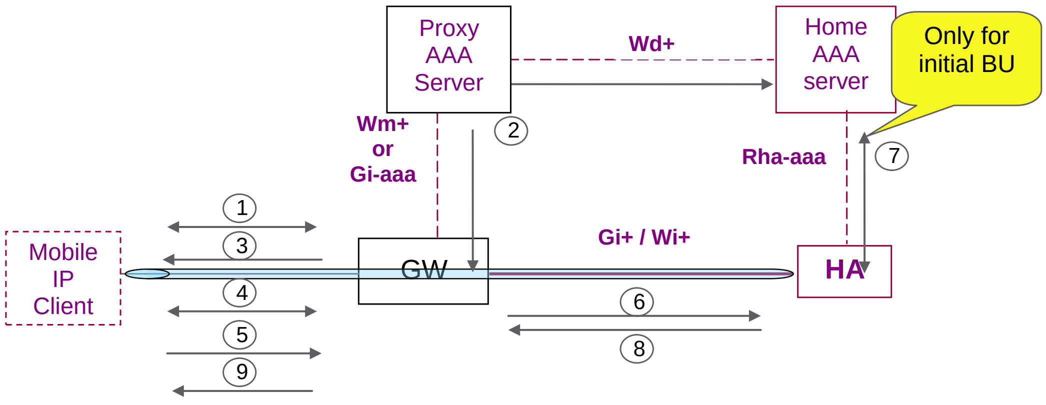


Figure A.3: Use of MIPv6 with Diameter application

The following are the subsequent steps described in Figure A.3:

1) The MN establishes a connection with the GW and begins authentication;

2) The GW interrogates the user's Home AAA server in order to authenticate and authorise the user. In the roaming case, the GW uses the Proxy AAA to contact the user's Home AAA server. In addition, the Home AAA server provides "MIPv6 bootstrap" information i.e. information allowing the Mobile IP client in the UE to configure itself for MIPv6 service and identify the assigned HA;

3) The GW completes the user authentication;

4) The MN carries out a DHCPv6 procedure for MIPv6 bootstrap;

5-6) The MN sends a Binding Update (BU) to the MIPv6 HA (this is the equivalent of the MIPv4 RRQ);

7) The HA authenticates the user and fetches keying material for subsequent Binding Updates;

8-9) The HA accepts the mobile registration by replying with a Binding Acknowledgement (BA).

The next two figures provide examples on how the MIPv4 and MIPv6 concepts described above can be mapped to scenarios for GPRS-WLAN mobility. The red pipes stand for Ipsec tunnels, whereas the blue pipes represent Mobile IP tunnels.

Depicted in Figure A.4 is the application of Mobile Ipv4 as a solution for GPRS-WLAN mobility. A FA functionality is incorporated in both the GGSN and the PDG, meaning that in this case MIPv4 is used with Foreign Agent Care-of-Address (FA-CoA). The Foreign Agent is not necessary for co-located mode operation of Mobile IP (see Figure A.5).

The "Home AAA" functions which are required for the Diameter MIPv4 application are assumed to be provided by the 3GPP AAA server.

The MIPv4 tunnelling is used only on the Gi+ and Wi+ interfaces i.e. between the HA and the FA located in the GGSN and the PDG, respectively.

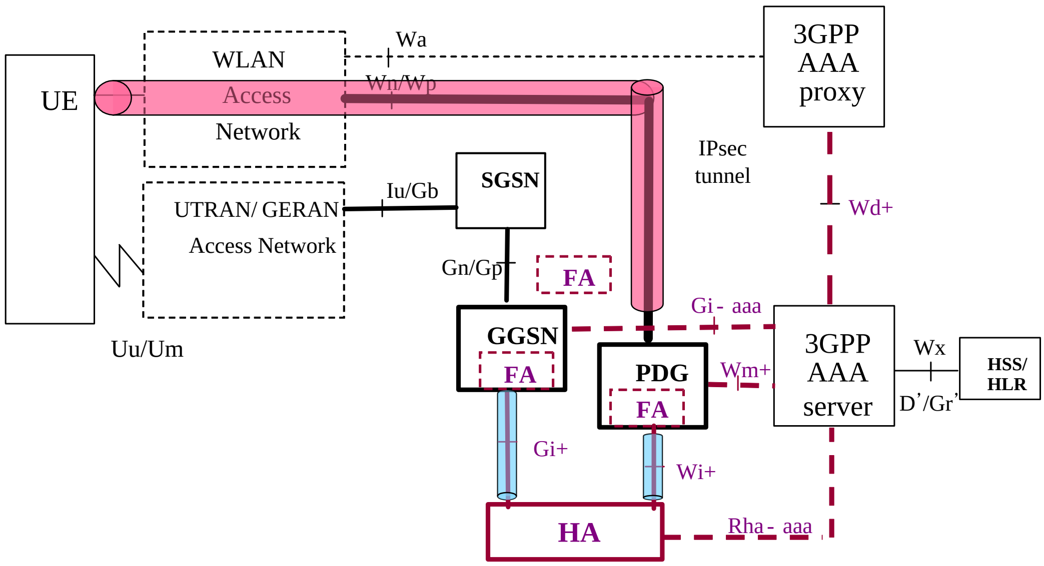


Figure A.4: Use of MIPv4 with FA-CoA for GPRS-WLAN mobility

NOTE 1: In case the HA functionality is collocated with the GGSN, the terminal can be considered to be at home in Mobile IP sense when using the GPRS IP access. The FA functionality in the GGSN becomes redundant in this case.

NOTE 2: In case the GGSN and the PDG are attached to the same IP subnet, the use of MIP is FFS.

NOTE 3: Whether the FA functionality has to be collocated with the GGSN/PDG or whether it can exist as a stand-alone element is FFS.

The same architecture applies to both Scenario 4 and Scenario 5, the only difference being that in Scenario 5 the UE is assumed to maintain simultaneous connections across the source and target Access System during the transition period.

Depicted in Figure A.5 is the application of Mobile Ipv6 as a solution for inter-system mobility. The same figure also applies to the use of MIPv4 with collocated Care-of-Addresses (co-CoA).

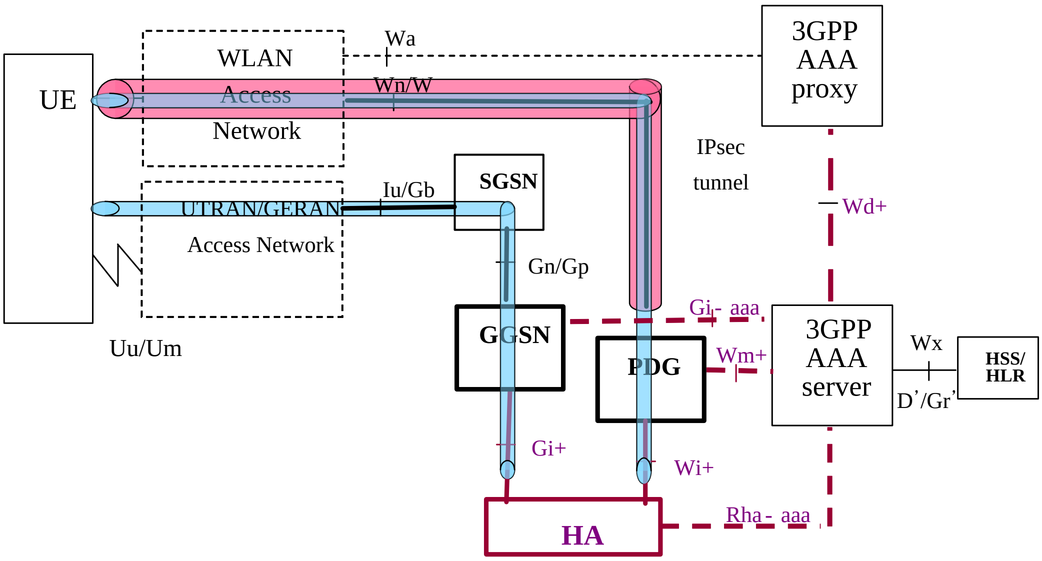


Figure A.5: Use of MIPv6 or MIPv4 with co-CoA for GPRS-WLAN mobility

In either case there is no notion of Foreign Agent in the GGSN or the PDG. MIP tunnelling is used from the HA all the way down to the UE. In case of MIPv6, the MIPv6 "route optimisation" mechanism is used to avoid tunnelling over the radio.

Regarding inter-WLAN mobility, relying on Mobile IP alone may not be sufficient for achieving Scenario 5-like seamless mobility. A possible issue here is the time required for setting up a new Ipsec tunnel when changing the point of WLAN attachment, because, contrary to the inter-system handover, the UE may not be able to initiate a new Ipsec tunnel setup before breaking the previous one. The IETF MOBIKE group is currently working on mechanisms for speeding up this kind of Ipsec tunnel relocation. Figure A.6 clearly shows that Mobile IP does not intervene during the relocation of the Ipsec tunnel. MOBIKE would be used instead.

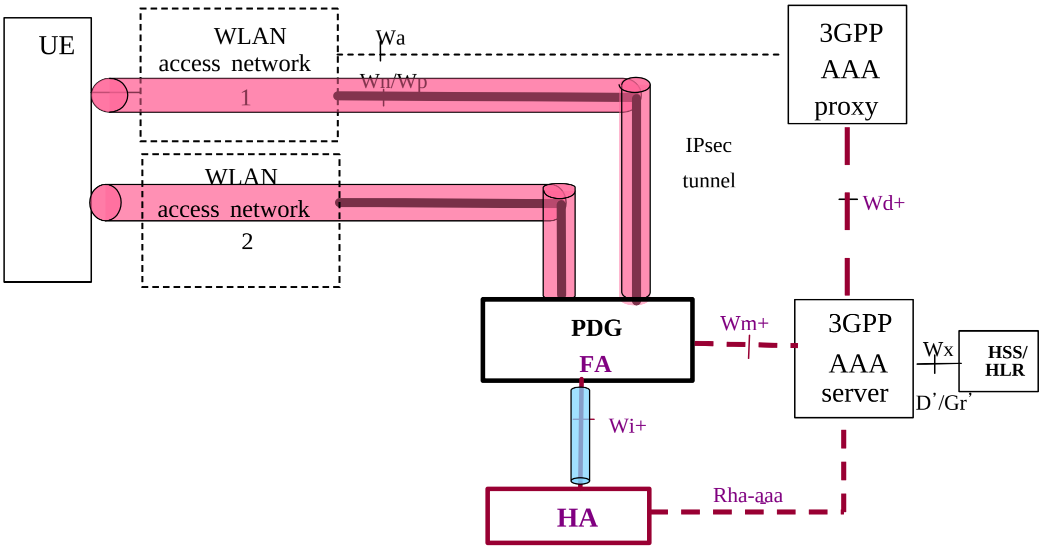


Figure A.6: MOBIKE use for inter-WLAN mobility

A.4 Impact on the baseline CN architecture

Depicted in Figure A.7 is the baseline architecture taken from TR 23.882, from which all IMS specific elements have been removed for simplicity. In addition, a Mobile IP Home Agent (MIP HA) has been added to the figure, as well as a couple of reference points. Listed below are all new or modified reference points, with a description of their role:

- **Gi+/Wi+**: this is the Mobile IP signalling and bearer plane between the Gateway (i.e. GGSN or PDG) and the MIP HA;
- **Wj**; this is the Mobile IP signalling and bearer plane (tunnel) between the UE and the MIP HA, which is used in case of MIPv4 co-located care-of address and MIPv6;
- **Gi-aaa**: this is the AAA part of the Gi interface, which traditionally connects the GGSN to a AAA server which itself is not part of the 3GPP system architecture. Here it is assumed that the Gi-aaa interface connects to the 3GPP AAA server. It is used by the Diameter Mobile IP application, RFC 4004 [7], for dynamic assignment of a MIP HA, as well as during setup of security associations (MN-HA, MN-FA, FA-HA);
- **Wm+/Wd+**: this is respectively an enhancement to the existing Wm and Wd reference points. The additional functionality is similar to the Gi-aaa functionality described above;
- **Rha-aaa**: this is the reference point between the MIP HA and the 3GPP AAA server. Similar to the previous, it is used for dynamic assignment of a MIP HA and during setup of security associations.

The impact on the PCRF is left FFS.

The applicability to WLAN Direct IP Access is FFS.

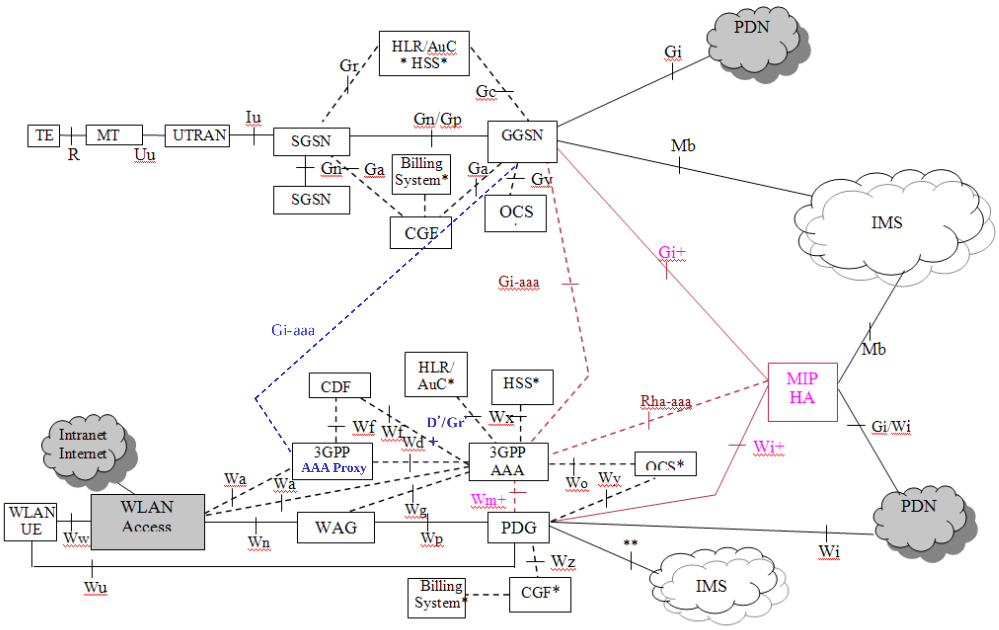


Figure A.7: Impact of Mobile IP on the baseline architecture

A.5 Impact on the baseline RAN architecture

None.

A.6 Impact on terminals used in the existing architecture

In order to support GPRS-WLAN mobility with session continuity (i.e. Scenario 4), the terminal must have a Mobile IP client and a MOBIKE client. In order to support seamless mobility (i.e. Scenario 5), the terminal must in addition be capable of simultaneous connections.

Other impacts on the terminal are FFS.

Annex B: Change History

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2007-3	SA2 ad-hoc C				TR skeleton (S2-071558) includes the approved documents: S2-071627, S2-071560, S2-071628, S2-071629.	0.0.1	0.0.2
2007-4	SA2#57				TR number is changed to 23.827. The version number is revised to 0.2.0	0.0.2	0.2.0
2007-5	SA2#57				The approved documents (including email approval) are included:s2-072209, s2-072210, s2-072211, s2-072212, s2-072213.	0.2.0	0.3.0
2007-8	SA2#587				Corrections are made on figure numbering, word spacing.. A reference is added. The level of content tables is increased.	0.3.0	0.3.1
2007-9	SA2#59				The approved documens, s2-073818, s2-073856, are included.	0.3.1	0.4.0