GTP-based S2b Interface Support on the P-GW and SAEGW

This chapter describes the GTP-based S2b interface support feature on the standalone P-GW and the SAEGW.

- Feature Description, on page 1
- How the S2b Architecture Works, on page 3
- How the S2a Architecture Works, on page 25
- Configuring the GTP-based S2b Interface on the P-GW and SAEGW, on page 39
- Monitoring the GTP-based S2b Interface Feature, on page 40
- Monitoring the GTP-based S2a Interface Feature, on page 42

Feature Description

This section describes the GTP-based S2a/S2b interface implementation on the P-GW and SAEGW.

GTP-based S2b Interface Support on the Standalone P-GW and SAEGW

Important GTP-based S2b interface support is a license-controlled feature. Contact your Cisco account or support representative for licensing information.

The S2b interface reference point connects the standalone P-GW with the ePDG and the P-GW of the SAEGW with the ePDG. Communication runs between the non-trusted non-3GPP ePDG (Evolved Packet Data Gateway) and the P-GW uses PMIPv6 (Proxy Mobile IP version 6) for providing access to the EPC. GTPv2-C is the signaling protocol used on the S2b. The S2b interface is based on 3GPP TS 29.274.

The S2b interface uses the PMIPv6 protocol to establish WLAN UE sessions with the P-GW. It also supports the transport of P-CSCF attributes and DNS attributes in PBU (Proxy-MIP Binding Update) and PBA (Proxy-MIP Binding Acknowledgment) messages as part of the P-CSCF discovery performed by the WLAN UEs. When the P-CSCF Address information is missing, P-CSCF Discovery is initiated upon an S4-SGSN-to-LTE (and vice versa) handoff. If the P-CSCF Address information is already available, there is no need to explicitly trigger another P-CSCF Discovery upon S4-SGSN to LTE (and vice versa) handoff.

Example: The UE tries to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports

such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies. So the UE can have independent PDN connections via multiple access types.

The access types supported are 4G and WiFi.

The S2b interface implementation on the P-GW and SAEGW supports the following functionality:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff

GTP-based S2a Interface Support on the Standalone P-GW and SAEGW

Important GTP-Based S2a Interface Support is a licensed-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

GTP-based S2a interface support is available on the P-GW and SAEGW. Operators deployed with the SAEGW are now able to integrate Trusted WiFi network functionality using this feature.

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD. Specifically, the S2a interface supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the standalone P-GW or P-GW of the SAEGW. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

When the WLAN is considered as trusted by the operator, the Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the S2a interface to the P-GW. Support has been extended for WiFi-to-LTE handovers using Make and Break for the SAEGW service. Multi-PDN handovers are also supported as part of this feature.

Supported functionality includes:

- Initial Attach
- WiFi-to-LTE handover
- LTE-to-WiFi handover
- Multi-PDN handovers

Supported protocols include:

- Transport Layer: UDP, TCP
- Tunneling: GRE IPv6
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Relationships to Other Features

This section describes how the GTP-based S2b and S2a interface support feature is related to other features.

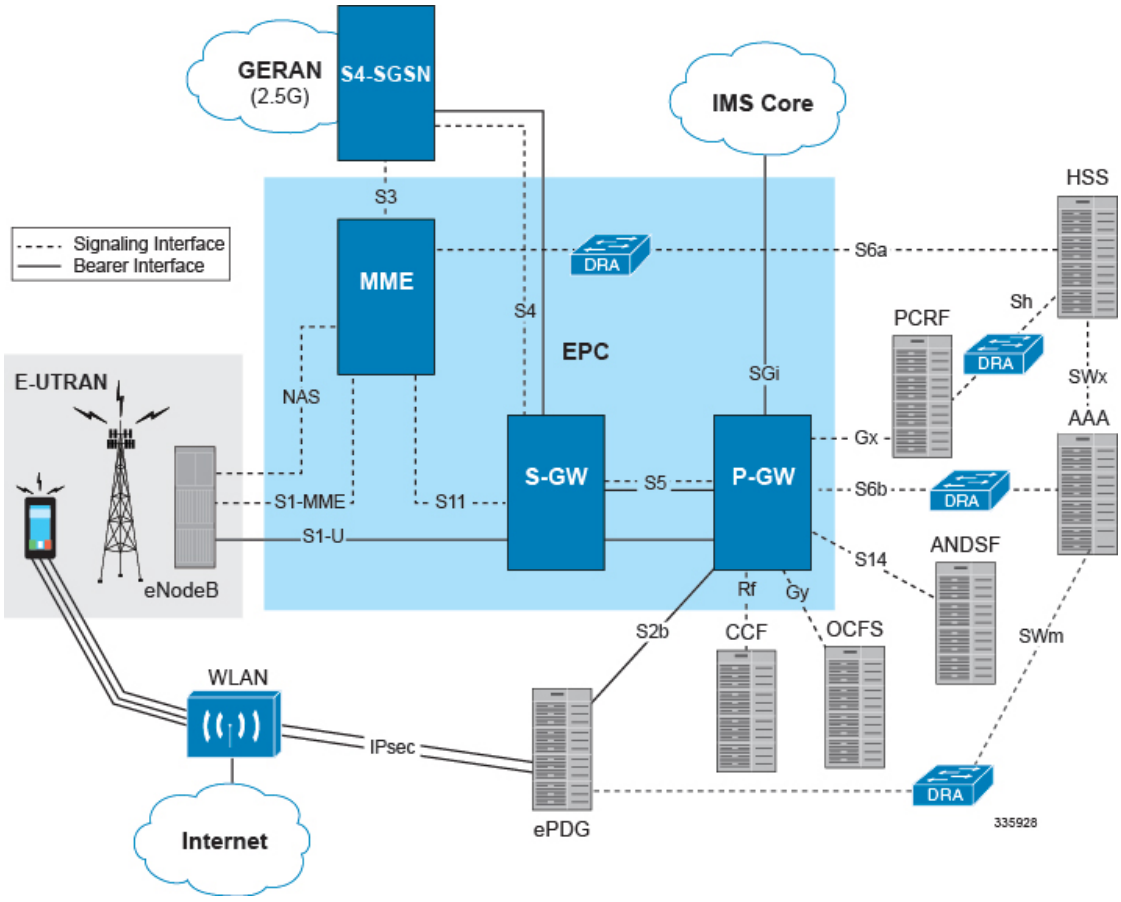
- A P-GW service must be configured and operational before GTP-based s2b interface support can be configured on the standalone P-GW and SAEGW.
- GTP-based S2b interface support must also be configured and operational on the ePDG to support this feature.
- A P-GW service must be configured and operational before GTP-based S2a interface support can be configured on the standalone P-GW and SAEGW.

How the S2b Architecture Works

Standalone P-GW Architecture for S2b Interface Support

The GTP-based S2b interface architecture is part of the P-GW deployment in the E-UTRAN/EPC Network. The P-GW communicates with the ePDG over the S2b interface, and the ePDG connects to the WLAN offload architecture via an IPSec interface.

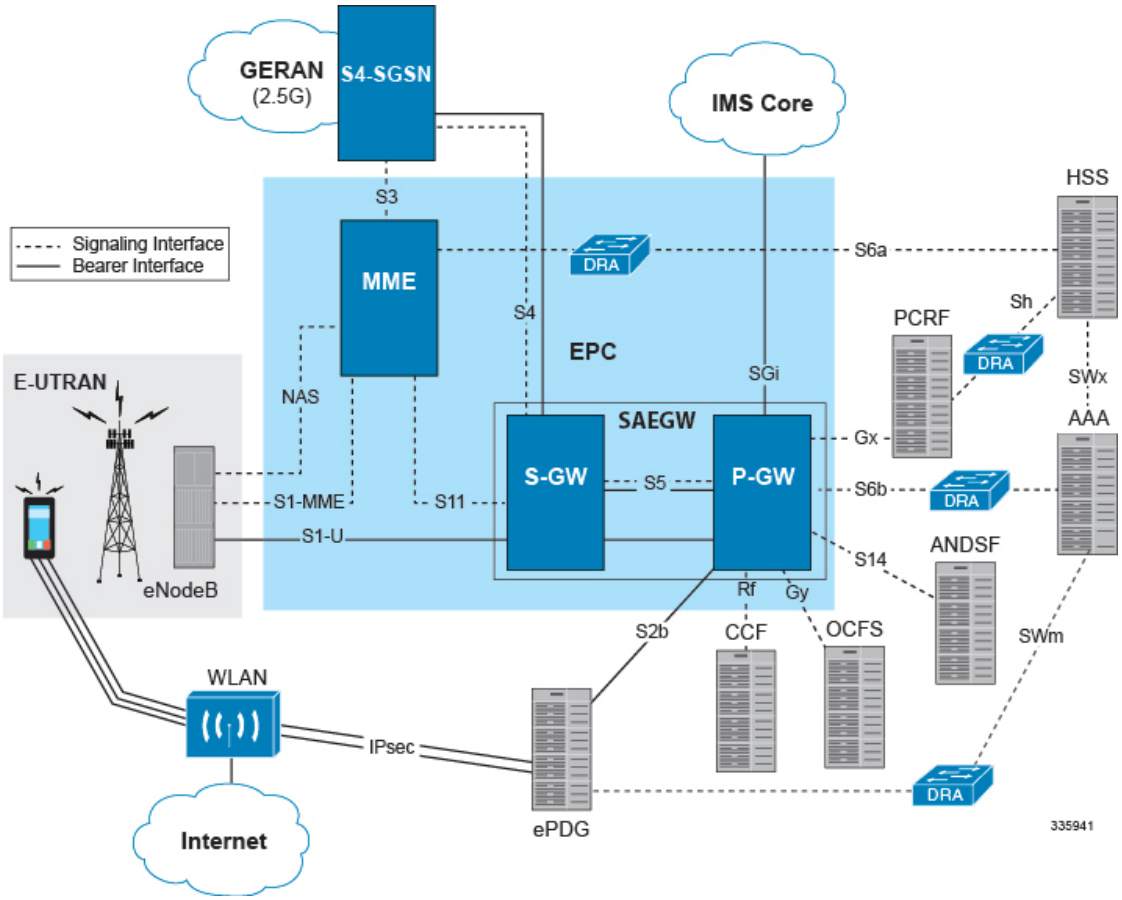
Figure 1: Standalone P-GW: GTP-based S2b Interface Implementation in the E-UTRAN/EPC Network



SAEGW Architecture for S2b Interface Support

The GTP-based S2b interface architecture is part of the SAEGW deployment in the E-UTRAN/EPC Network. The P-GW of the SAEGW communicates with the ePDG over the S2b interface, and the ePDG connects to the WLAN offload architecture via an IPSec interface.

Figure 2: SAEGW: GTP-based S2b Interface Implementation in the E-UTRAN/EPC Network



Limitations on S2b Interface Support for the P-GW and SAEGW

Note the following limitations of the GTP-based S2b interface implementation on the P-GW and SAEGW:

- Only the following interfaces/access types from the WiFi Offload and VLC Flows are supported:
- Access Types:
  - WiFi
  - LTE
- Interfaces:
  - S6b
  - Gy
  - Rf

- Gx
- GTPv2 (S2b)

- Legacy Lawful Intercept is supported on the S2b interface on the standalone P-GW, but is not qualified on the S2b interface on the SAEGW at this time.

Standalone P-GW Call Flows

This section provides call flows that illustrate the basic functionality of the GTP-based S2b interface support on the standalone P-GW.

Figure 3: Initial Attach Call Flow - P-GW

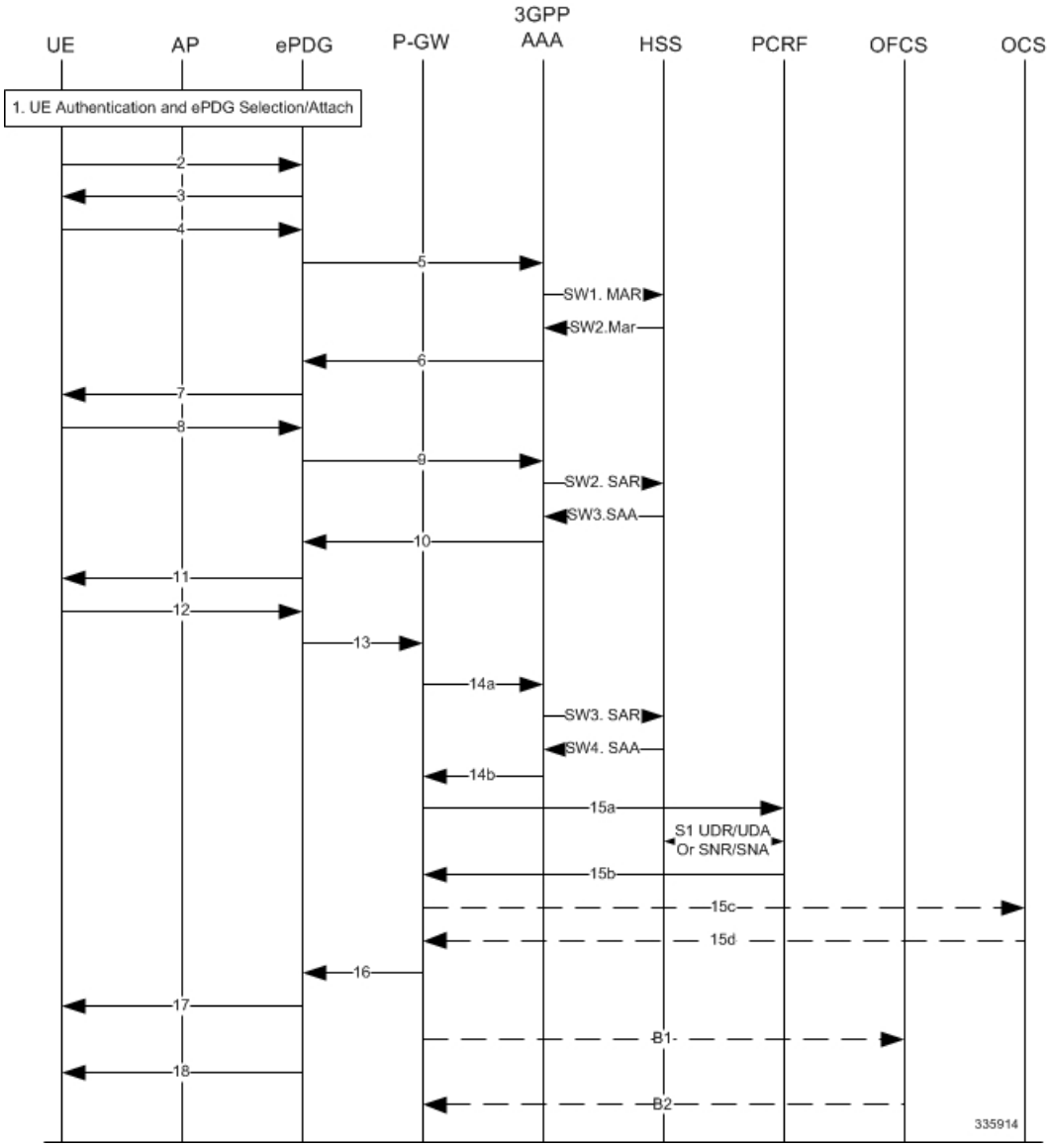


Table 1: Initial Attach - P-GW

Step	Description
1	UE performs initial Access Point association and authentication if necessary.
2 - 11	The UE creates a connection with the ePDG.
12	UE sends IKE_AUTH request (AUTH). The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG selects the P-GW based on Node Selection options. The ePDG sends Create Session Request.
14a	The P-GW sends AAR to the 3GPP AAA to authorize the PDN for the subscriber and to update P-GW address on the HSS for the APN.
SW3	The 3GPP AAA updates the HSS with the P-GW address for the APN and retrieves Subscriber-APN profiles from the HSS.
SW4	The HSS sends Server-Assignment-Answer (Session-Id, Result-Code, Experimental-Result (Vendor-Id, Experimental-Result-Code))
14b	The 3GPP AAA sends AAA.
15a	The P-GW sends an indication of IP-CAN establishment to the PCRF with CCR to indicate establishment of a new IP CAN session.
S1	The PCRF downloads (and caches) user profile (by sending an Sh: UDR (User-Identity, Service-Indication, Data-Reference) and receiving an Sh: UDA (Result-Code, User-Data)).
S2	The PCRF may subscribe to profile update notification.
15b	The PCRF Acknowledges IP CAN Session Establishment with a CCA message.
15c	If the Online AVP is set in the CCA from the PCRF (UC users / CF / RTR), the P-GW shall conditionally send a CCR-Initial.
15d	The OCS responds with a CCA to the P-GW.
16	The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
17	The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
18	ePDG sends Router Advertisement to ensure IP Stack is fully initialized. P-GW disables the Router Advertisement to the UE.
B1	If the Offline AVP is set in the CCA from the PCRF, then after IP-CAN session establishment procedure is complete, the P-GW shall send a ACR-Start to the OFCS.
B2	The OFCS responds with an ACA to the P-GW.

Figure 4: P-GW: LTE to WiFi Handoff Call Flow

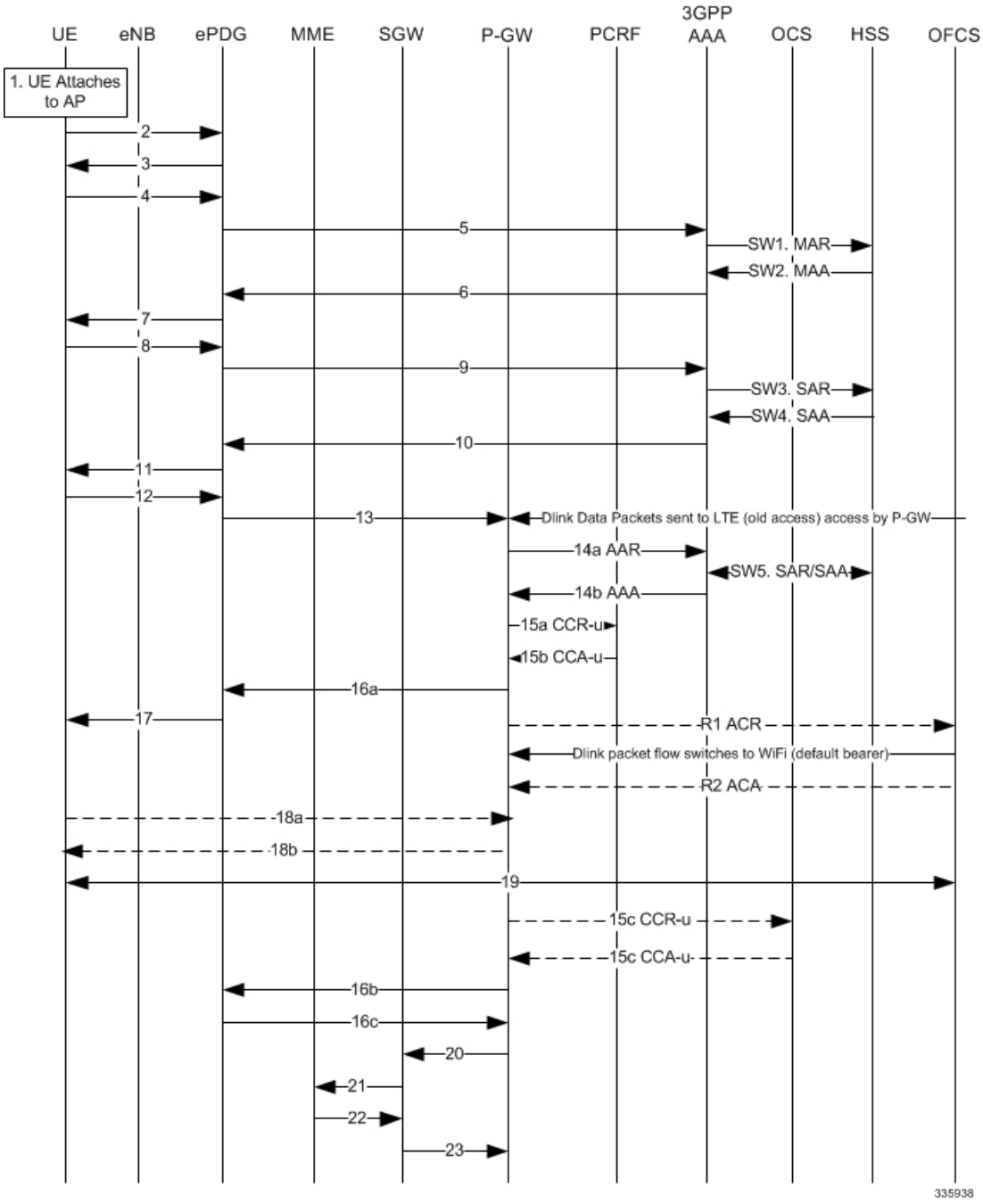


Table 2: P-GW LTE to WiFi Handoff

Step	Description
1	Authentication and ePDG Selection. UE performs initial Access Point association and authentication if necessary.

Step	Description
2	UE to ePDG: IKEv2 SA_INIT. The UE sends IKE_SA_INIT Request.
3	ePDG to UE: INIT Response. The ePDG responds with an IKE_SA_INIT Response. The ePDG will start the IKEv2 setup timer when sending the IKE_SA_INIT Response.
4	UE sends Auth_Request.
5	ePDG to AAA: DER. The ePDG sends the DER message to the 3GPP AAA Server. Note the NAI shall not contain the AP MAC address sent in the username that comes in the IKE message
SW1. MAR	AAA to HSS: MAR. The 3GPP AAA Server fetches the user profile and authentication vectors from HSS over SWx. The 3GPP AAA server look up the IMSI of the authenticated user based on the received user identity and includes the EAP-AKA as requested authentication method in the request sent to the HSS. The AAA sends the Multimedia-Auth-Request MAR, Origin-Host, Origin-Realm, Destination-Realm, Destination-Host, User-Name, RAT-Type, SIP-Auth-Data-Item, SIP-Number-Auth-Items, and Routing-Information).
SW2. MAA	HSS to AAA: MAA. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The HSS sends the Multimedia-Auth-Answer MAA.
6	AAA to ePDG: DEA. The 3GPP AAA Server initiates the authentication challenge and responds with DEA.
7	ePDG to UE: IKE_AUTH. The ePDG responds with IKE_AUTH. The identity is the IP address of the ePDG; the AUTH payload authenticates the first IKE_SA_INIT response. If the UE requested certificates, the CERT is included. The EAP message received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.
8	UE to ePDG: IKE_AUTH Request. The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message IKE_AUTH Request (EAP).
9	ePDG to AAA: DER. The ePDG sends DER (Base AVPs, Auth Request Type, EAP Payload, Auth-Session-State, Service Selection) to the 3GPP AAA Server.
SW3. SAR	AAA to' HSS: SAR. The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the authenticated user. The AAA sends Server-Assignment-Request, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, User-Name (IMSI-NAI), Server-Assignment-Type (REGISTRATION)).
SW4 SAA	HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
10	AAA to ePDG: DEA. The 3GPP AAA Server sends an EAP success. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access before responding with DEA.
11	ePDG to UE: IKE_AUTH_Response. ePDG sends IKE_AUTH_Response (EAP).

Step	Description
12	UE to ePDG: IKE_AUTH_Request. UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG to P-GW: Create Session Request. The ePDG sends Create Session Request to the P-GW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.
14a	P-GW to 3GPP-AAA: AAR. The P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
SW5. SAR/SAA	AAA to HSS: SAR. The 3GPP AAA updates the HSS with the P-GW address for the APN. The AAA sends Server-Assignment-Request.
14b AAA	3GPP AAA to P-GW: AAA. 3GPP AAA sends AAA to the P-GW.
15a CCR-u	P-GW to PCRF: CCR-U. The P-GW sends an indication of IP-CAN modification to the PCRF with CCR to indicate modification of the IP-CAN session.
15b CCA-u	PCRF to P-GW: CCA. The PCRF Acknowledges of IP-CAN Session Modification with a CCA message. This message includes the Policy and Charging rules the P-GW will enforce and triggers for events that must be reported by the P-GW.
16a	P-GW to ePDG: Create Session Response. The P-GW identifies the S5 session and re-allocates the requested IP address session and responds back to the ePDG with a Create Session Response message. The P-CSCF private IE is included if the ePDG had included the P-CSCF request in message 13.
17	ePDG to UE: IKE_AUTH. The ePDG sends IKE_AUTH.
R1 ACR	P-GW to OFCS: ACR. The P-GW sends an ACR-Interim to the OFCS.
R2 ACA	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW.
18a	UE sends a Router Solicitation message.
18b	The P-GW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
19	The UE sends a SIP Re-Register once it successfully identifies it has changed access network to indicate the RAT change to the P-CSCF and assigned IP address is unchanged. UE will include 802.11 a/b/g/n in the PANI header. The SIP re-registration does not impact the way the P-CSCF does charging as charging is not used from the P-CSCF in IMS case.
15c CCR-u	P-GW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
15d CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW.
16b	P-GW to ePDG: Create Bearer Request. The IMS PDN has one or more dedicated bearers established prior to handoff and the P-GW also sends Create Bearer Request to the ePDG. Note that Charging ID is not sent on S2b.

Step	Description
16c	ePDG to P-GW: Create Bearer Response. The ePDG sends Create Bearer Response message
20	P-GW to S-GW: Delete Bearer Request. The P-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the S-GW. This message may be sent any time after message 13, the create session request.
21	S-GW to MME: Delete Bearer Request. The S-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the MME. The MME releases the E-UTRAN bearers if not already released. The MME does not send Notify Request to HSS at this point, as the cause IE is RAT change to Non-3GPP. MME does not page the UE either or initiate any NAS signaling and remove the locally stored PDN state and does S1 context release to the eNodeB if it has not already been triggered by the eNodeB. For last PDN MME removes all locally stored UE state.
22	MME to S-GW: Delete Bearer Response. The MME sends Delete Bearer Response to the S-GW.
23	S-GW to P-GW: Delete Bearer Response. The S-GW sends Delete Bearer Response to the P-GW.

Figure 5: P-GW: WiFi to LTE Handoff

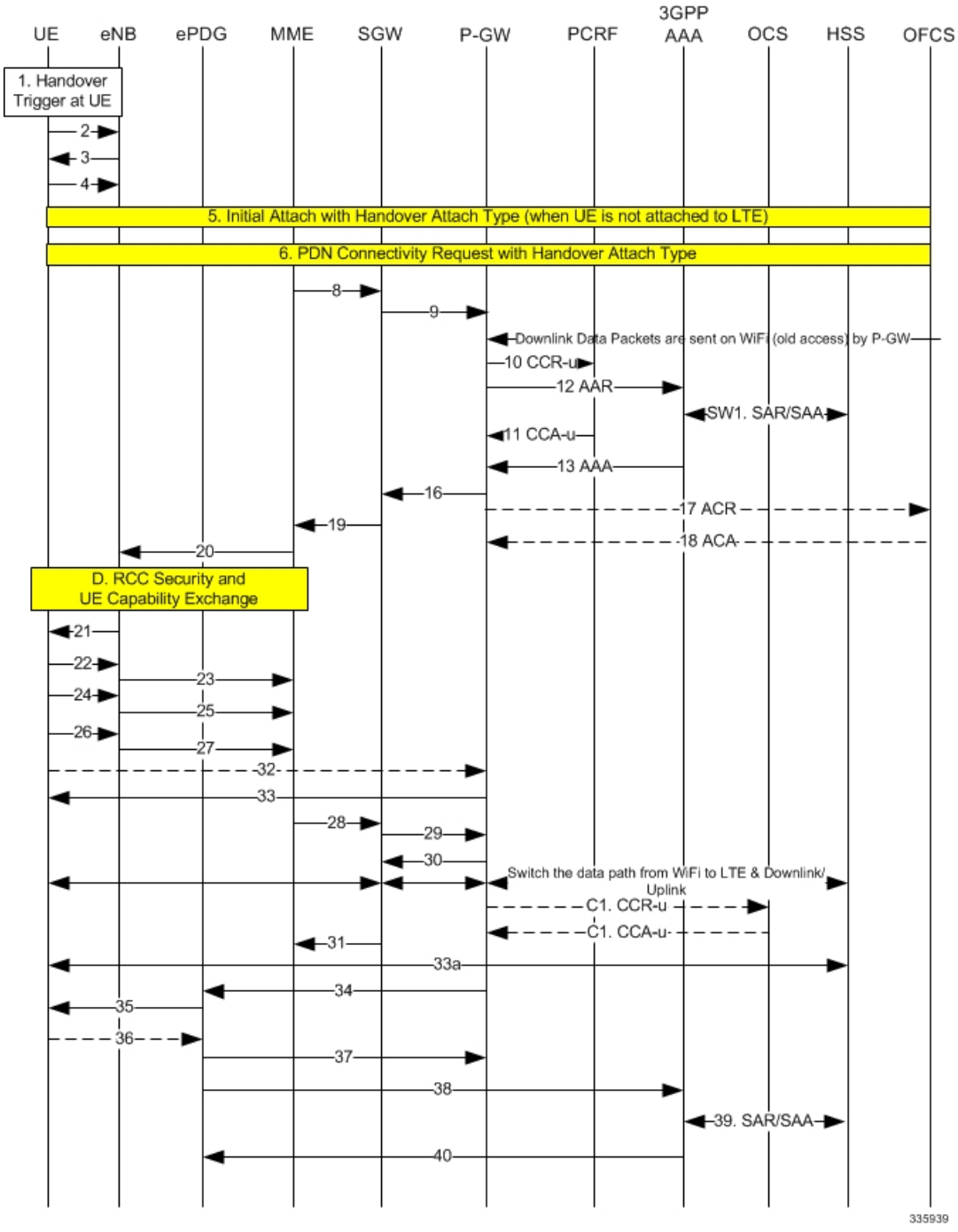


Table 3: P-GW WiFi to LTE Handoff Procedure

Step	Description
1	A handover trigger occurs at the UE.

Step	Description
2, 3	RRC Connection Request/Connection Setup. The UE and eNodeB exchange signaling to set up an RRC connection (5.3.3, TS 36.331).
4	RRC Connection Setup Complete [Attach Request]. The UE sends RRC Connection Setup Complete message to the eNodeB.
5	Attach Request from eNB to MME. The UE indicates in the Attach Request to LTE that this is a Handover Attach. The eNodeB selects the MME. The eNodeB forwards the Attach Request message in an Initial UE Message to the MME.
6	MME selects the same P-GW based on HSS provided PGW FQDN and sends the Create Session request.
8	The MME selects the PGW/SGW. The MME sends a Create Session Request to the SGW with RAT as EUTRAN and the handoff indicator set to TRUE.
9	The SGW sends a Create Session Request to the PDN GW in order to establish the handoff (handoffindicator is set to true). RAT type is E-UTRAN.
10	P-GW to PCRF CCR IP-CAN Session Modification Procedure. The PCEF sends a CC-Request (CCR) Command with CC-Request-Type set to UPDATE_REQUEST. The APN-AMBR is included in the QoS-information AVP.
12	The P-GW sends AAR to 3GPP-AAA and includes the RAT type of the new connection.
SW1. SAR/SAA	The 3GPP-AAA sends SAR to HSS to retrieve the user profile, the HSS returns an SAA. The P-GW-FQDN is not updated as the 3GPP-AAA is not registered for this user.
11	PCRF ' P-GW: CCA IP-CAN Session modification Procedure. On receiving the CCR the PCRF shall send a CC-Answer (CCA) Command to install the PCC rules and event triggers for all configured and established bearers. The QoS-Information AVP contains APN-AMBR-UL and APN-AMBR-DL.
13	The 3GPP-AAA responds with AAA.
16	P-GW to S-GW: Create Session Response + Create Bearer Request. The P-GW responds with a Create Session Response message to the S-GW. The P-GW provides IPv6 Prefix. Subject to operator configuration the P-GW can begin to forward downlink data and the S-GW shall buffer any downlink data packets.
17	P-GW to OFCS: ACR. After the P-GW sends the PBA, the P-GW shall send an ACR-Interim to the OFCS.
18	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW.
19	Create Session Response. The S-GW sends Create Session Response to the MME.
20	Initial Context Setup Request/Attach Accept. The Attach Accept is sent as NAS PDU in the Initial Context Setup Request from MME to eNodeB. Attach Accept message contains new GUTI.

Step	Description
D	These procedures occur independently of the location procedures. These procedures only apply to initial attach scenarios.
21	RRC Connection Re-configuration. The eNodeB sends the RRC Connection Reconfiguration message including the EPS Radio Bearer Identity to the UE, and the Attach Accept message to the UE. The APN is provided to the UE to notify it of the APN for which the activated default bearer is associated.
22	RRC Connection Re-configuration Complete. The UE sends the RRC Connection Reconfiguration Complete message to the eNodeB.
23	Initial Context Setup Response. The eNodeB sends Initial Context Setup Response to the MME.
24	Uplink Information Transfer. The UE sends an Uplink Information Transfer message.
25	Attach Complete. The eNodeB forwards the received Attach Complete message in an Uplink NAS Transport as part of NAS PDU.
26	Uplink Information Transfer. When the UE has received Activate dedicated EPS Bearer Context Request message in the Attach Accept message, the UE sends Activate Dedicated EPS Bearer Context Accept message in a Uplink Information Transfer message.
27	UL NAS Transport. The eNB passes the Activate Dedicated EPS Bearer Context Accept message received in Step 14.b, to the MME in a UL NAS Transport message. At this time, the uplink data can be sent on the dedicated bearer.
32	Router Solicitation. This step may happen any time after step 26. For IPv6 PDN, the UE may send a Router Solicitation to the P-GW.
33	Router Advertisement. This step may happen any time after step 29 if the UE requested IPv4v6 or IPv6 PDN type. On receipt of the RS or prior the P-GW shall send a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
28	Modify Bearer Request / Create Bearer Response. On receiving both Initial Context Setup Response and Attach Complete, the MME sends a Modify Bearer Request message to the S-GW. The MME piggybacks the Modify Bearer Request message on the Create Bearer Response message.
29	The S-GW processes each message independently. The S-GW forwards the Create Bearer Response to the P-GW. At this time, the P-GW can send downlink data on the dedicated bearer for the IMS traffic. Since Handover Indication is set to TRUE in the Modify Bearer Request, the S-GW sends Modify Bearer Request to the P-GW separately. Based on TS 23.401, the P-GW switches the downlink traffic to S5 upon receiving this message. However, subject to operator configuration, this switching occurs at Create Session Request above (C3).
30	The P-GW sends Modify Bearer Response (Cause) message to the S-GW.

Step	Description
C1. CCR-u	P-GW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
C1. CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW.
31	The S-GW sends Modify Bearer Response to the MME. The S1 S-GW F-TEID is the same as the S1-U S-GW F-TEID sent in Create Session Response from the S-GW to the MME. The S-GW can now start sending downlink packets to eNB and the switching of the data path from WiFi to LTE occurs after the Modify Bearer Response.
33a	SIP Re-registration RAT Change. The UE sends a SIP Re-Register to the P-CSCF to indicate that it detected a RAT change and assigned IP address remained unchanged.
34	P-GW to ePDG: Delete Bearer Request. The P-GW sends Delete Bearer Request to ePDG to disconnect the session.
35	ePDG to UE: IKEv2 Information Delete Request. The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
34	UE to ePDG: IKEv2 Informational Delete Response. UE responds with IKEv2 Information Delete Response () and initiates air interface resource release. This step is conditional and UE may not send this response.
37	ePDG to P-GW: Delete Bearer Response. The ePDG sends Delete Bearer Response to the P-GW.
38	ePDG to AAA: Session Termination Request. The ePDG sends STR to the 3GPP AAA.
39	AAA to HSS: Server Assignment Request. The AAA sends Server-Assignment-Request to de-register. HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
40	AAA to ePDG: Session Termination Answer. The AAA sends STA to the ePDG.

SAEGW GTP-based S2b Call Flows

This section provides call flows that illustrate the basic functionality of the GTP-based S2b interface support on the SAEGW.

Figure 6: Initial Attach Call Flow - SAEGW

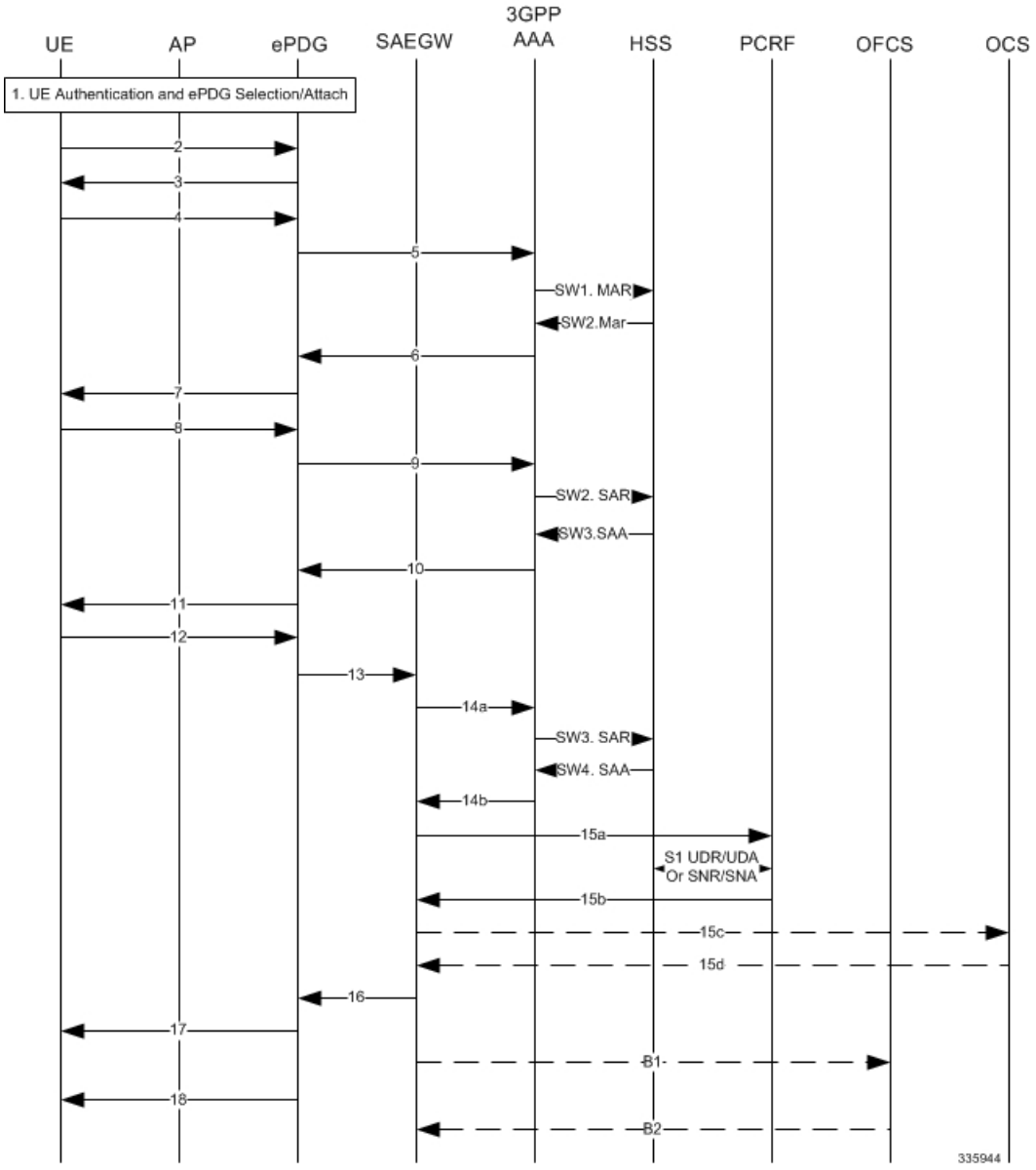


Table 4: Initial Attach - SAEGW

Step	Description
1	UE performs initial Access Point association and authentication if necessary.
2 - 11	The UE creates a connection with the ePDG.
12	UE sends IKE_AUTH request (AUTH). The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.

Step	Description
13	ePDG selects the P-GW of the SAEGW based on Node Selection options. The ePDG sends Create Session Request.
14a	The P-GW of the SAEGW sends AAR to the 3GPP AAA to authorize the PDN for the subscriber and to update P-GW address on the HSS for the APN.
SW3	The 3GPP AAA updates the HSS with the P-GW address of the SAEGW for the APN and retrieves Subscriber-APN profiles from the HSS.
SW4	The HSS sends Server-Assignment-Answer (Session-Id, Result-Code, Experimental-Result (Vendor-Id, Experimental-Result-Code))
14b	The 3GPP AAA sends AAA.
15a	The P-GW of the SAEGW sends an indication of IP-CAN establishment to the PCRF with CCR to indicate establishment of a new IP CAN session.
S1	The PCRF downloads (and caches) user profile (by sending an Sh: UDR (User-Identity, Service-Indication, Data-Reference) and receiving an Sh: UDA (Result-Code, User-Data)).
S2	The PCRF may subscribe to profile update notification.
15b	The PCRF Acknowledges IP CAN Session Establishment with a CCA message.
15c	If the Online AVP is set in the CCA from the PCRF (UC users / CF / RTR), the P-GW shall conditionally send a CCR-Initial.
15d	The OCS responds with a CCA to the P-GW.
16	The P-GW of the SAEGW allocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
17	The ePDG sends the assigned IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
18	ePDG sends Router Advertisement to ensure IP Stack is fully initialized. The P-GW of the SAEGW disables the Router Advertisement to the UE.
B1	If the Offline AVP is set in the CCA from the PCRF, then after IP-CAN session establishment procedure is complete, the P-GW of the SAEGW shall send a ACR-Start to the OFCS.
B2	The OFCS responds with an ACA to the P-GW of the SAEGW.

Figure 7: SAEGW: LTE to WiFi Handoff Call Flow

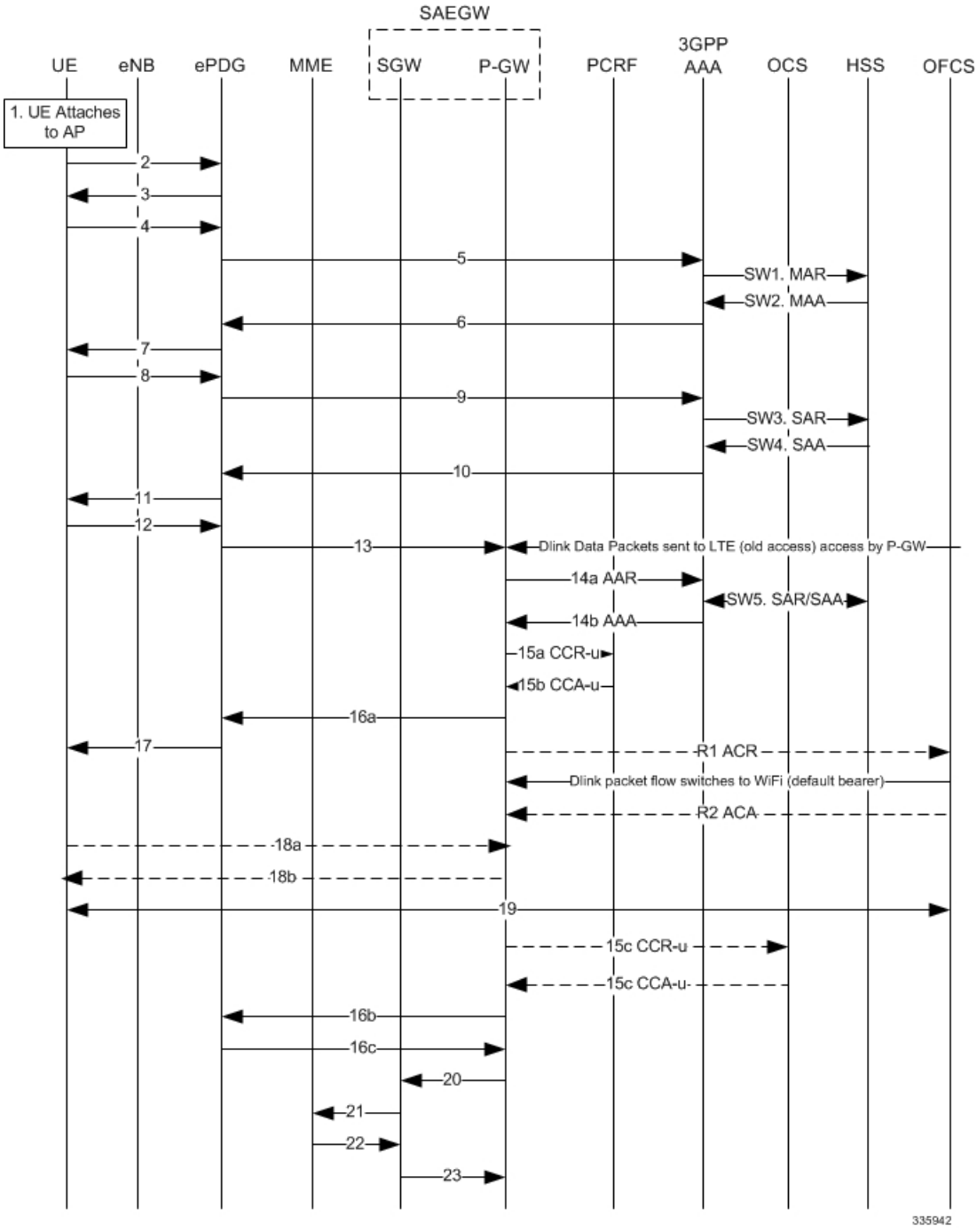


Table 5: SAEGW LTE to WiFi Handoff

Step	Description
1	Authentication and ePDG Selection. UE performs initial Access Point association and authentication if necessary.

Step	Description
2	UE to ePDG: IKEv2 SA_INIT. The UE sends IKE_SA_INIT Request.
3	ePDG to UE: INIT Response. The ePDG responds with an IKE_SA_INIT Response. The ePDG will start the IKEv2 setup timer when sending the IKE_SA_INIT Response.
4	UE sends Auth_Request.
5	ePDG to AAA: DER. The ePDG sends the DER message to the 3GPP AAA Server. Note the NAI shall not contain the AP MAC address sent in the username that comes in the IKE message
SW1. MAR	AAA to HSS: MAR. The 3GPP AAA Server fetches the user profile and authentication vectors from HSS over SWx. The 3GPP AAA server look up the IMSI of the authenticated user based on the received user identity and includes the EAP-AKA as requested authentication method in the request sent to the HSS. The AAA sends the Multimedia-Auth-Request MAR, Origin-Host, Origin-Realm, Destination-Realm, Destination-Host, User-Name, RAT-Type, SIP-Auth-Data-Item, SIP-Number-Auth-Items, and Routing-Information).
SW2. MAA	HSS to AAA: MAA. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The HSS sends the Multimedia-Auth-Answer MAA.
6	AAA to ePDG: DEA. The 3GPP AAA Server initiates the authentication challenge and responds with DEA.
7	ePDG to UE: IKE_AUTH. The ePDG responds with IKE_AUTH. The identity is the IP address of the ePDG; the AUTH payload authenticates the first IKE_SA_INIT response. If the UE requested certificates, the CERT is included. The EAP message received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.
8	UE to ePDG: IKE_AUTH Request. The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message IKE_AUTH Request (EAP).
9	ePDG to AAA: DER. The ePDG sends DER (Base AVPs, Auth Request Type, EAP Payload, Auth-Session-State, Service Selection) to the 3GPP AAA Server.
SW3. SAR	AAA to' HSS: SAR. The 3GPP AAA updates the HSS with the 3GPP AAA Server Address information for the authenticated user. The AAA sends Server-Assignment-Request, Origin-Host, Origin-Realm, Destination-Host, Destination-Realm, User-Name (IMSI-NAI), Server-Assignment-Type (REGISTRATION)).
SW4 SAA	HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
10	AAA to ePDG: DEA. The 3GPP AAA Server sends an EAP success. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access before responding with DEA.
11	ePDG to UE: IKE_AUTH_Response. ePDG sends IKE_AUTH_Response (EAP).

Step	Description
12	UE to ePDG: IKE_AUTH_Request. UE sends IKE_AUTH request (AUTH) The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message.
13	ePDG to P-GW of SAEGW: Create Session Request. The ePDG sends Create Session Request to the P-GW of SAEGW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.
14a	P-GW to 3GPP-AAA: AAR. The P-GW of SAEGW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
SW5. SAR/SAA	AAA to HSS: SAR. The 3GPP AAA updates the HSS with the P-GW address for the APN. The AAA sends Server-Assignment-Request.
14b AAA	3GPP AAA to P-GW: AAA. 3GPP AAA sends AAA to the P-GW of SAEGW.
15a CCR-u	P-GW of SAEGW to PCRF: CCR-U. The P-GW sends an indication of IP-CAN modification to the PCRF with CCR to indicate modification of the IP-CAN session.
15b CCA-u	PCRF to P-GW of SA: CCA. The PCRF Acknowledges of IP-CAN Session Modification with a CCA message. This message includes the Policy and Charging rules the P-GW will enforce and triggers for events that must be reported by the P-GW.
16a	P-GW of SAEGW to ePDG: Create Session Response. The P-GW of SAEGW identifies the S5 session and re-allocates the requested IP address session and responds back to the ePDG with a Create Session Response message. The P-CSCF private IE is included if the ePDG had included the P-CSCF request in message 13.
17	ePDG to UE: IKE_AUTH. The ePDG sends IKE_AUTH.
R1 ACR	P-GW to OFCS: ACR. The P-GW sends an ACR-Interim to the OFCS.
R2 ACA	OFCS to P-GW: ACA. The OFCS responds with an ACA to the P-GW of SAEGW.
18a	UE sends a Router Solicitation message.
18b	The P-GW of SAEGW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
19	The UE sends a SIP Re-Register once it successfully identifies it has changed access network to indicate the RAT change to the P-CSCF and assigned IP address is unchanged. UE will include 802.11 a/b/g/n in the PANI header. The SIP re-registration does not impact the way the P-CSCF does charging as charging is not used from the P-CSCF in IMS case.
15c CCR-u	P-GW of SAEGW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW shall conditionally send a CCR-Update to the OCS to request online charging quota for the PDN session.
15d CCA-u	OCS to P-GW: CCA. The OCS responds with a CCA to the P-GW of SAEGW.

Step	Description
16b	P-GW of SAEGW to ePDG: Create Bearer Request. The IMS PDN has one or more dedicated bearers established prior to handoff and the P-GW of SAEGW also sends Create Bearer Request to the ePDG. Note that Charging ID is not sent on S2b. **Note** If there is a collision and already one transaction is pending and handoff request is received, then handoff is rejected with message "Rejecting S2b/LTE Handoff as only one pending transaction is supported".
16c	ePDG to P-GW: Create Bearer Response. The ePDG sends Create Bearer Response message
20	P-GW of SAEGW to S-GW of SAEGW: Delete Bearer Request. The P-GW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the S-GW. This message may be sent any time after message 13, the create session request.
21	S-GW of SAEGW to MME: Delete Bearer Request. The S-GW of SAEGW sends the Delete Bearer Request (Linked EPS Bearer ID (if last bearer) or EPS Bearer ID, Cause (RAT changed from 3GPP to Non-3GPP)) to the MME. The MME releases the E-UTRAN bearers if not already released. The MME does not send Notify Request to HSS at this point, as the cause IE is RAT change to Non-3GPP. MME does not page the UE either or initiate any NAS signaling and remove the locally stored PDN state and does S1 context release to the eNodeB if it has not already been triggered by the eNodeB. For last PDN MME removes all locally stored UE state.
22	MME to S-GW of SAEGW: Delete Bearer Response. The MME sends Delete Bearer Response to the S-GW of SAEGW.
23	S-GW of SAEGW to P-GW of SAEGW: Delete Bearer Response. The S-GW of SAEGW sends Delete Bearer Response to the P-GW of SAEGW.

Figure 8: SAEGW WiFi to LTE Handoff

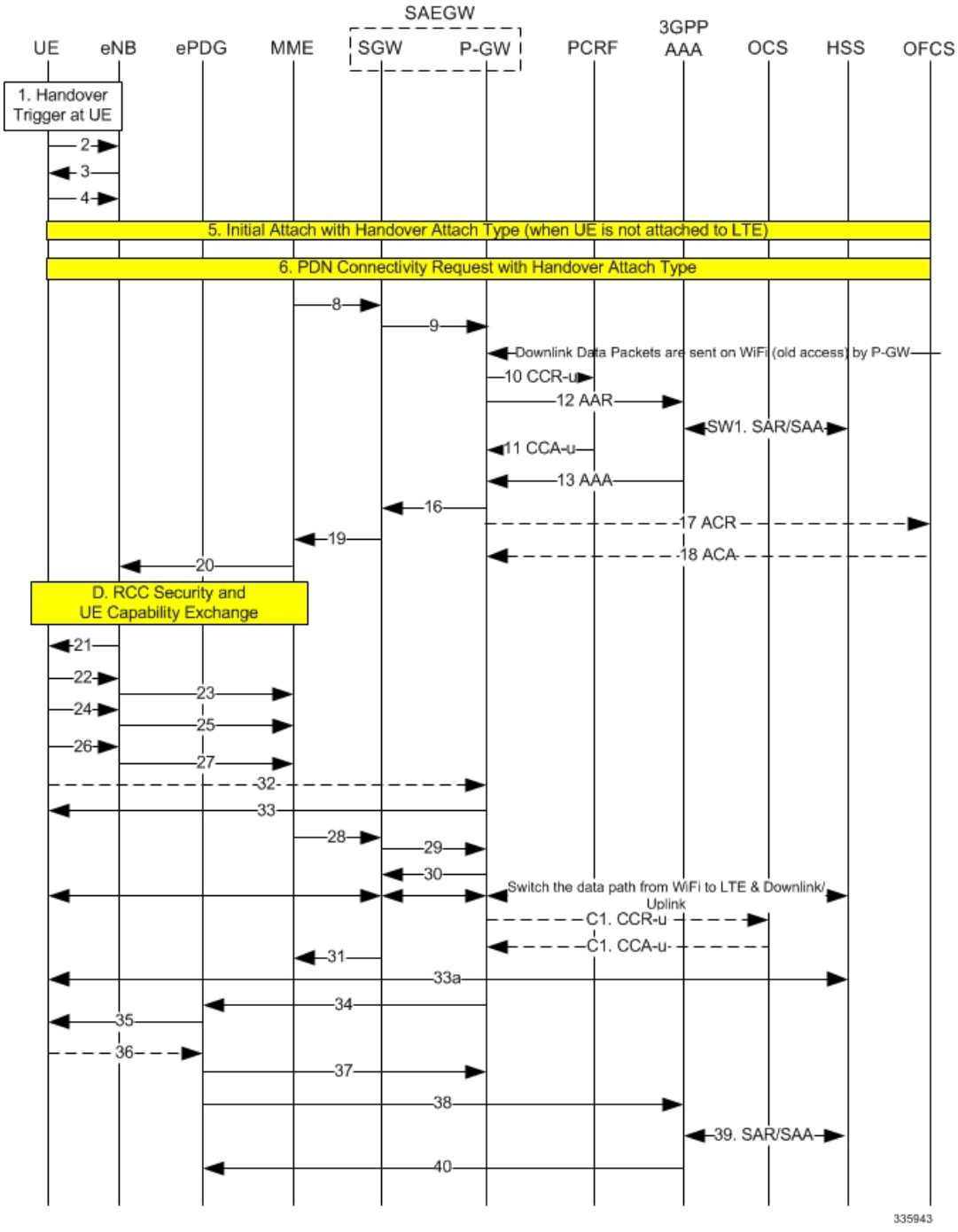


Table 6: SAEGW WiFi to LTE Handoff Procedure

Step	Description
1	A handover trigger occurs at the UE.

Step	Description
2, 3	RRC Connection Request/Connection Setup. The UE and eNodeB exchange signaling to set up an RRC connection (5.3.3, TS 36.331).
4	RRC Connection Setup Complete [Attach Request]. The UE sends RRC Connection Setup Complete message to the eNodeB.
5	Attach Request from eNB to MME. The UE indicates in the Attach Request to LTE that this is a Handover Attach. The eNodeB selects the MME. The eNodeB forwards the Attach Request message in an Initial UE Message to the MME.
6	MME selects the same P-GW of SAEGW based on HSS provided PGW FQDN and sends the Create Session request.
8	The MME selects the PGW/SGW of SAEGW. The MME sends a Create Session Request to the SGW of SAEGW with RAT as EUTRAN and the handoff indicator set to TRUE.
9	The SGW of SAEGW sends a Create Session Request to the PDN GW in order to establish the handoff (handoffindicator is set to true). RAT type is E-UTRAN.
10	P-GW of SAEGW to PCRF CCR IP-CAN Session Modification Procedure. The PCEF sends a CC-Request (CCR) Command with CC-Request-Type set to UPDATE_REQUEST. The APN-AMBR is included in the QoS-information AVP.
12	The P-GW of SAEGW sends AAR to 3GPP-AAA and includes the RAT type of the new connection.
SW1. SAR/SAA	The 3GPP-AAA sends SAR to HSS to retrieve the user profile, the HSS returns an SAA. The P-GW-FQDN is not updated as the 3GPP-AAA is not registered for this user.
11	PCRF to P-GW of SAEGW: CCA IP-CAN Session modification Procedure. On receiving the CCR the PCRF shall send a CC-Answer (CCA) Command to install the PCC rules and event triggers for all configured and established bearers. The QoS-Information AVP contains APN-AMBR-UL and APN-AMBR-DL.
13	The 3GPP-AAA responds with AAA.
16	P-GW of SAEGW to S-GW of SAEGW: Create Session Response + Create Bearer Request. The P-GW of SAEGW responds with a Create Session Response message to the S-GW of SAEGW. The P-GW of SAEGW provides IPv6 Prefix. Subject to operator configuration the P-GW of SAEGW can begin to forward downlink data and the S-GW of SAEGW buffers any downlink data packets.
17	P-GW of SAEGW to OFCS: ACR. After the P-GW of SAEGW sends the PBA, the P-GW of SAEGW sends an ACR-Interim to the OFCS.
18	OFCS to P-GW of SAEGW: ACA. The OFCS responds with an ACA to the P-GW.
19	Create Session Response. The S-GW of SAEGW sends Create Session Response to the MME.

Step	Description
20	Initial Context Setup Request/Attach Accept. The Attach Accept is sent as NAS PDU in the Initial Context Setup Request from MME to eNodeB. Attach Accept message contains new GUTI.
D	These procedures occur independently of the location procedures. These procedures only apply to initial attach scenarios.
21	RRC Connection Re-configuration. The eNodeB sends the RRC Connection Reconfiguration message including the EPS Radio Bearer Identity to the UE, and the Attach Accept message to the UE. The APN is provided to the UE to notify it of the APN for which the activated default bearer is associated.
22	RRC Connection Re-configuration Complete. The UE sends the RRC Connection Reconfiguration Complete message to the eNodeB.
23	Initial Context Setup Response. The eNodeB sends Initial Context Setup Response to the MME.
24	Uplink Information Transfer. The UE sends an Uplink Information Transfer message.
25	Attach Complete. The eNodeB forwards the received Attach Complete message in an Uplink NAS Transport as part of NAS PDU.
26	Uplink Information Transfer. When the UE has received Activate dedicated EPS Bearer Context Request message in the Attach Accept message, the UE sends Activate Dedicated EPS Bearer Context Accept message in a Uplink Information Transfer message.
27	UL NAS Transport. The eNB passes the Activate Dedicated EPS Bearer Context Accept message received in Step 14.b, to the MME in a UL NAS Transport message. At this time, the uplink data can be sent on the dedicated bearer.
32	Router Solicitation. This step may happen any time after step 26. For IPv6 PDN, the UE may send a Router Solicitation to the P-GW.
33	Router Advertisement. This step may happen any time after step 29 if the UE requested IPv4v6 or IPv6 PDN type. On receipt of the RS or prior the P-GW of SAEGW sends a Router Advertisement and include the globally unique /64 IPv6 prefix previously assigned.
28	Modify Bearer Request / Create Bearer Response. On receiving both Initial Context Setup Response and Attach Complete, the MME sends a Modify Bearer Request message to the S-GW of SAEGW. The MME piggybacks the Modify Bearer Request message on the Create Bearer Response message.

Step	Description
29	The S-GW of SAEGW processes each message independently. The S-GW of SAEGW forwards the Create Bearer Response to the P-GW. At this time, the P-GW of SAEGW can send downlink data on the dedicated bearer for the IMS traffic. Since Handover Indication is set to TRUE in the Modify Bearer Request, the S-GW of SAEGW sends Modify Bearer Request to the P-GW of SAEGW separately. Based on TS 23.401, the P-GW of SAEGW switches the downlink traffic to S5 upon receiving this message. However, subject to operator configuration, this switching occurs at Create Session Request above (C3).
30	The P-GW of SAEGW sends Modify Bearer Response (Cause) message to the S-GW.
C1. CCR-u	P-GW of SAEGW to OCS: CCR-U. If the Online AVP is set in the CCA from the PCRF, the P-GW of SAEGW conditionally sends a CCR-Update to the OCS to request online charging quota for the PDN session.
C1. CCA-u	OCS to P-GW of SAEGW: CCA. The OCS responds with a CCA to the P-GW of SAEGW.
31	The S-GW of SAEGW sends Modify Bearer Response to the MME. The S1 S-GW F-TEID is the same as the S1-U S-GW F-TEID sent in Create Session Response from the S-GW of SAEGW to the MME. The S-GW of SAEGW can now start sending downlink packets to eNB and the switching of the data path from WiFi to LTE occurs after the Modify Bearer Response.
33a	SIP Re-registration RAT Change. The UE sends a SIP Re-Register to the P-CSCF to indicate that it detected a RAT change and assigned IP address remained unchanged.
34	P-GW of SAEGW to ePDG: Delete Bearer Request. The P-GW of SAEGW sends Delete Bearer Request to ePDG to disconnect the session.
35	ePDG to UE: IKEv2 Information Delete Request. The ePDG sends IKEv2 Informational Delete Request () to UE to disconnect the session.
34	UE to ePDG: IKEv2 Informational Delete Response. UE responds with IKEv2 Information Delete Response () and initiates air interface resource release. This step is conditional and UE may not send this response.
37	ePDG to P-GW of SAEGW: Delete Bearer Response. The ePDG sends Delete Bearer Response to the P-GW.
38	ePDG to AAA: Session Termination Request. The ePDG sends STR to the 3GPP AAA.
39	AAA to HSS: Server Assignment Request. The AAA sends Server-Assignment-Request to de-register. HSS to AAA: SAA. The HSS sends Server-Assignment-Answer.
40	AAA to ePDG: Session Termination Answer. The AAA sends STA to the ePDG.

Standards Compliance

This section lists the industry-standards and references that were used in developing the GTP-based S2b interface implementation on the P-GW and SAEGW:

The following standards and references were used in developing the GTP-based S2b interface support feature.

- 3GPP TS 23.003-a.1.0 Numbering, addressing and identification
- 3GPP TS 23.234-a.0.0, 3GPP system to Wireless Local Area Network (WLAN) Interworking
- 3GPP TS 23.261-a.1.0, IP flow mobility and seamless Wireless Local Area Network (WLAN) Offload
- 3GPP TS 23.401: GPRS Enhancement for E-UTRAN Access
- 3GPP TS 23.402-a.4.0 Architecture Enhancements for non-3GPP Accesses
- 3GPP TS 24.302-a.4.0: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks.
- 3GPP TS 24.312-a.3.0 Access Network Discovery and Selection Function (ANDSF) Management Object (MO)
- 3GPP TS 29.273-a.3.0 Evolved Packet System (EPS); 3GPP EPS AAA interfaces
- 3GPP TS 29.274- Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 33.234-a.0.0 Wireless Local Area Network (WLAN) interworking security
- 3GPP TS 33.402-a.0.0 Security aspects of non-3GPP accesses
- IETF RFC 3588: Diameter Base Protocol.
- IETF RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPSec
- IETF RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- IETF RFC 3748: Extensible Authentication Protocol (EAP)
- IETF RFC 3948: UDP Encapsulation of IPSec ESP Packets.
- IETF RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- IETF RFC 4303: IP Encapsulating Security Payload (ESP).
- IETF RFC 4306: Internet Key Exchange Protocol Version 2
- IETF RFC 4739: Multiple Authentication Exchange in IKEv2 protocol
- IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)

How the S2a Architecture Works

This section provides information that describes the S2a interface architecture on the standalone P-GW and SAEGW.

Standalone P-GW and SAEGW Architecture for S2a Interface Support

Diagrams for the S2a interface architecture for the standalone P-GW and SAEGW appear below.

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD. Specifically, the S2a interface supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the standalone P-GW or P-GW of the SAEGW. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

Figure 9: S2a Interface Architecture for the Standalone P-GW

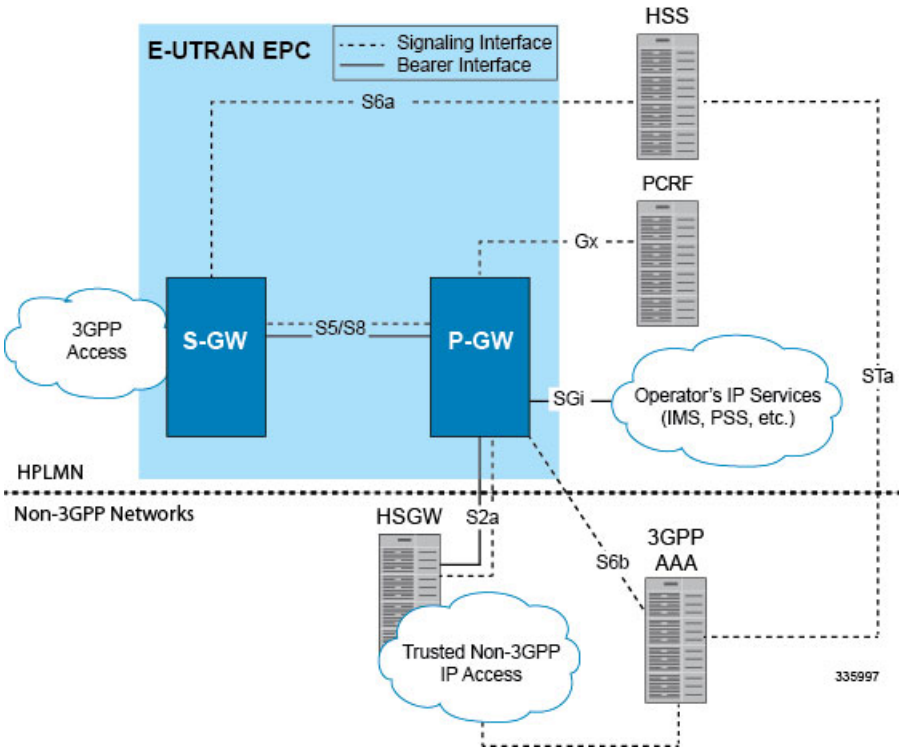
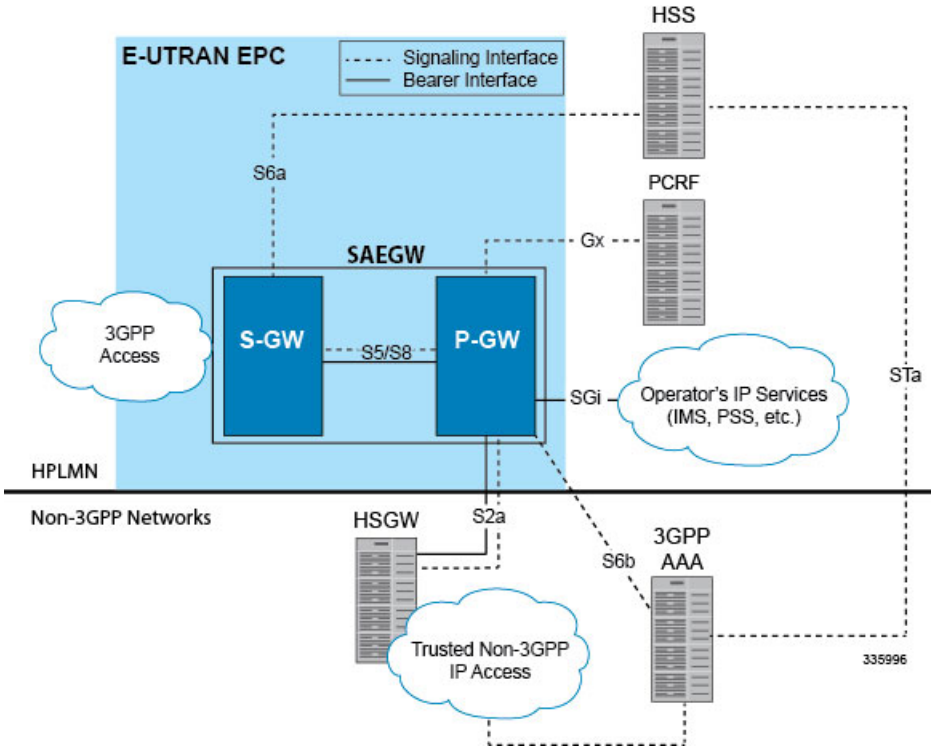


Figure 10: S2a Interface Architecture for the SAEGW



Limitations on S2a Interface Support on the P-GW and SAEGW

Note the following limitations of the GTP-based S2a interface implementation on the P-GW and SAEGW:

- Access Type technologies supported are WiFi and LTE.
- Interfaces supported include:
  - S6b
  - Gy
  - Rf
  - Gx
  - GTPv2

Standalone P-GW S2a Call Flows

The following call flow diagrams describe the basic functionality of the S2a interface when deployed in a standalone P-GW architecture.

Figure 11: S2a Initial Attach on Standalone P-GW

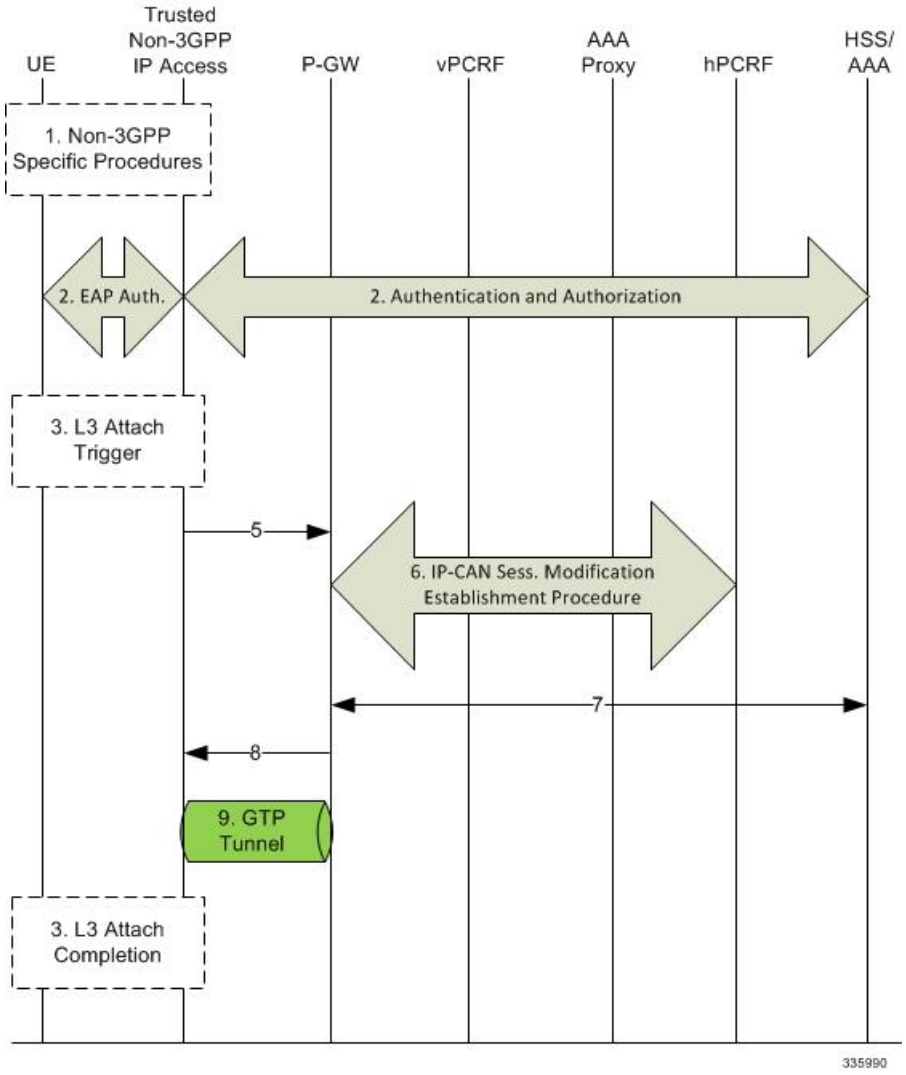


Table 7: S2a Initial Attach on Standalone P-GW

Step	Description
1	
2	
3	
4	

Step	Description
5	The Trusted non-3GPP IP Access sends a Create Session Request message to the P-GW. The RAT type indicates the non-3GPP IP access technology type. The PDN type shall be set based on the requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach.
6	The P-GW initiates the IP-CAN Session Establishment Procedure with the PCRF.
7	The selected P-GW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS.
8	The P-GW returns a Create Session Response message to the TWAN, including the IP address(es) allocated for the UE.
9	The GTP tunnel is set up between the TWAN and the P-GW.
10	Initial Attach is complete.

Figure 12: S2a LTE-to-WiFi Handover on Standalone P-GW

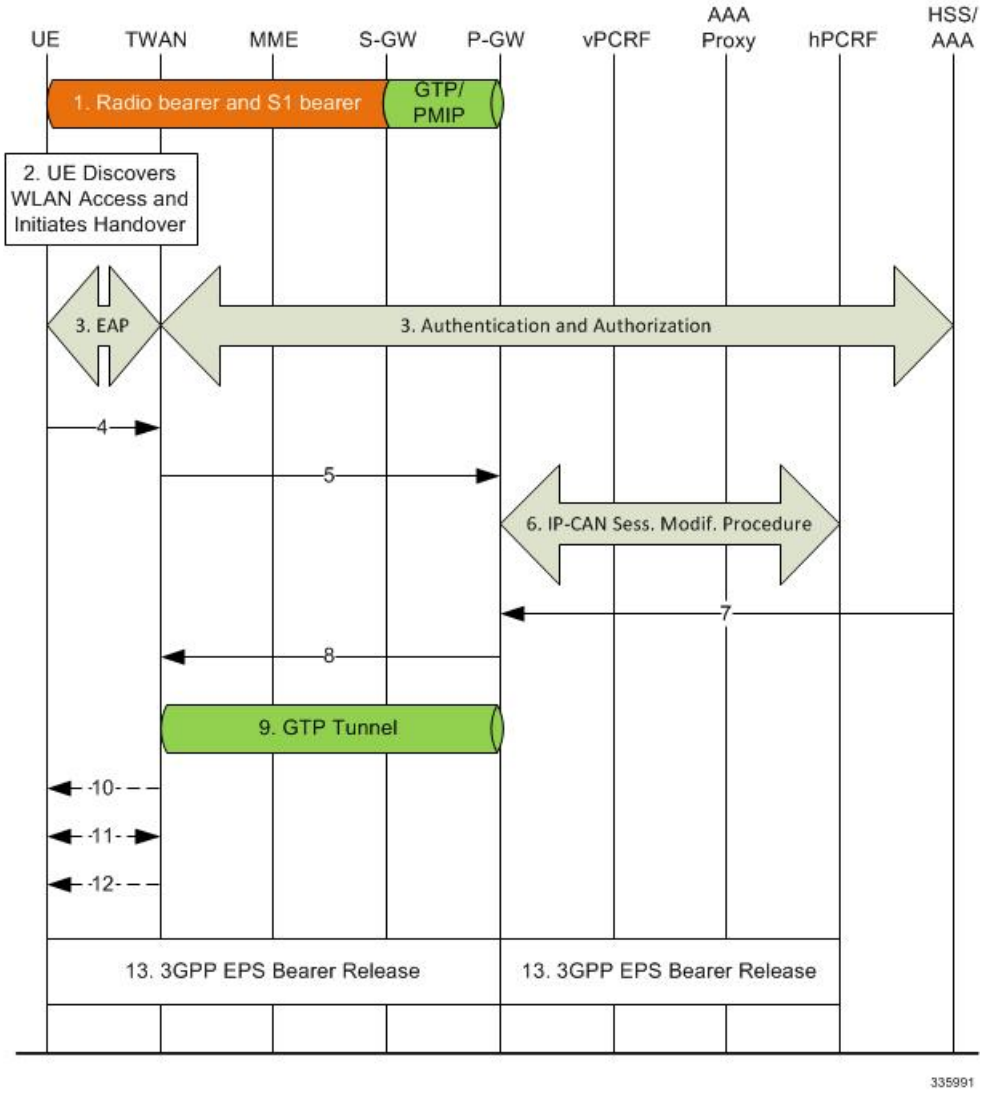


Table 8: S2a WiFi-to-LTE Handover on Standalone P-GW

Step	Description
1	
2 - 4	The UE discovers WLAN access and initiates a handover. The TWAN takes authorization from the AAA server.

Step	Description
5	The TWAN sends a Create Session Request (IMSI, APN, RAT type) message to the the P-GW. The RAT type WLAN indicates the non-3GPP IP access technology type. The TWAN does not set the 'Handover Indication' bit. Instead, based on the IMSI, APN and RAT type the P-GW determines that it is potential handover from the TWAN. The P-GW re-allocates the same IPv4 address and/or IPv6 address that was assigned to the UE while it was connected to 3GPP IP access.
6	The P-GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF with the RAT type as WLAN.
7	The P-GW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN and obtains authorization information from the 3GPP AAA Server. The 3GPP AAA Server decides whether or not to update the P-GW identification according to the UE capability, which has been provided at the authentication phase.
8	The P-GW responds with a Create Session Response to the TWAN. The Create Session Response contains the IPv4 address and/or the IPv6 address assigned to the UE while it was connected to the 3GPP IP access.
9	The GTP tunnel is setup between TWAN and the P-GW.
10	
11	
12	
13	The P-GW initiates the P-GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1 for GTP-S5/S8.

Figure 13: S2a WiFi-to-LTE Handover on Standalone P-GW

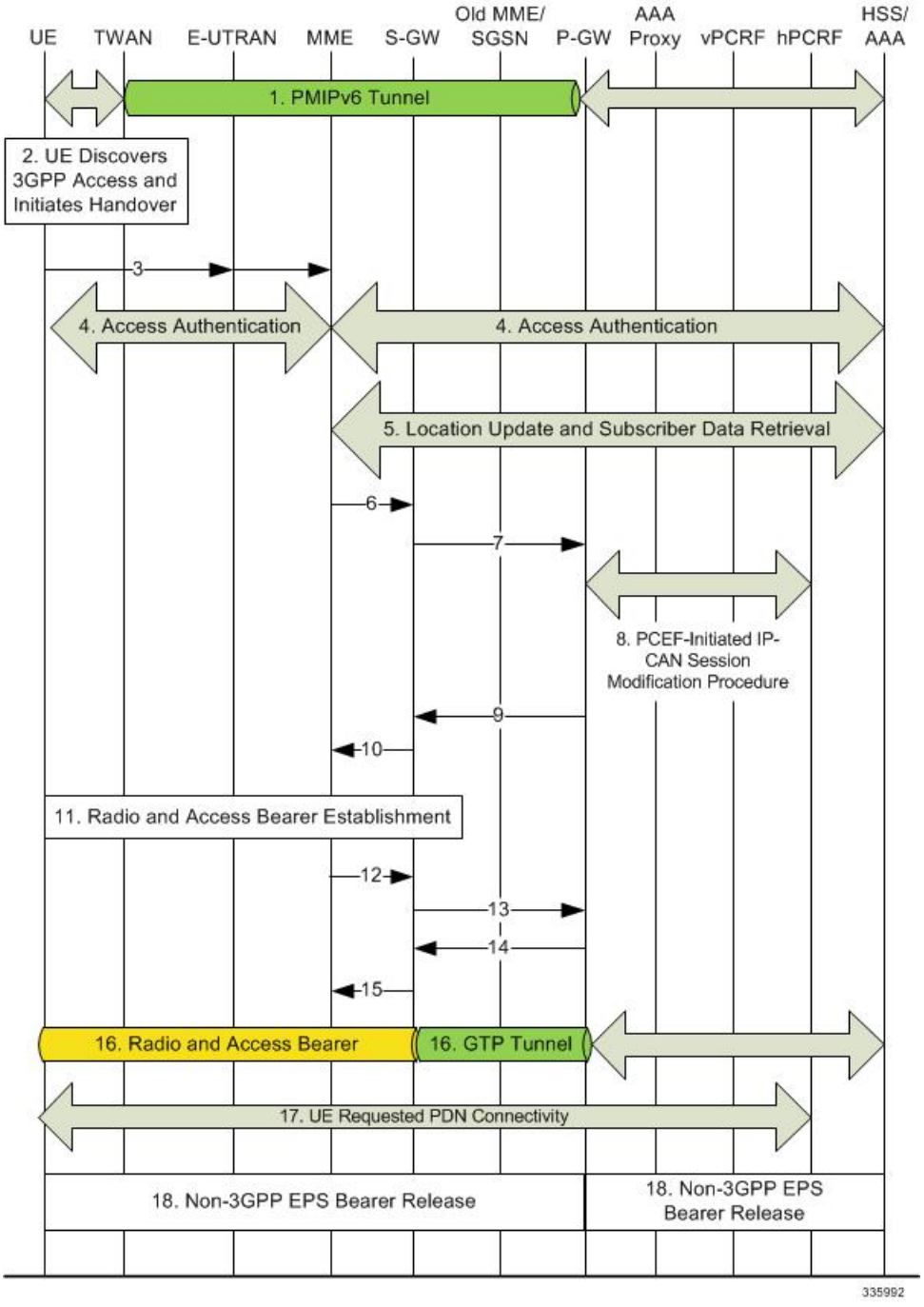


Table 9: S2a WiFi-to-LTE Handover on Standalone P-GW

Step	Description
1	

Step	Description
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

SAEGW S2a Call Flows

The call flow diagrams in this section describe the basic functionality of S2a interface support on the SAEGW, including:

- Initial Attach
- LTE-to-WiFi Handover
- WiFi-to-LTE Handover

Figure 14: S2a Initial Attach on the SAEGW

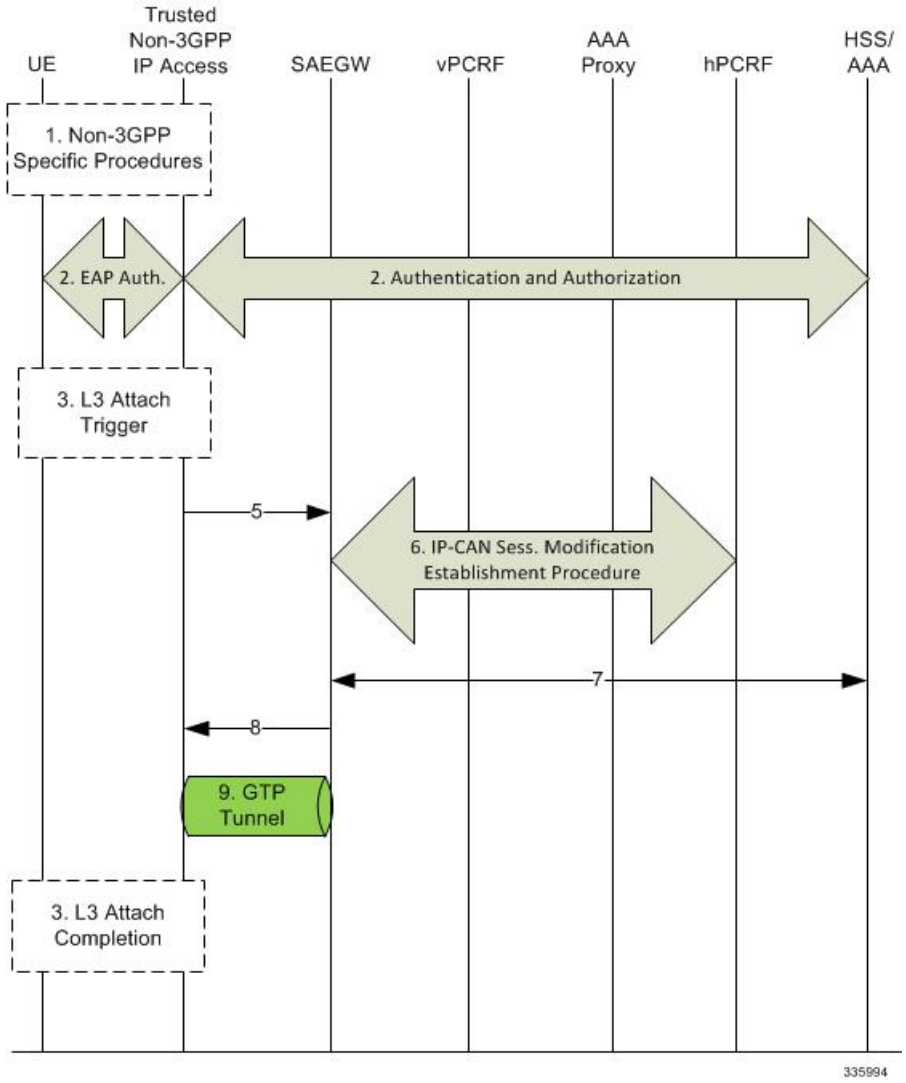


Table 10: S2a Initial Attach on the SAEGW

Step	Description
1	
2	
3	
4	

Step	Description
5	The Trusted non-3GPP IP Access sends a Create Session Request (CSReq) message to the P-GW of the SAEGW. The RAT type indicates the non-3GPP IP access technology type. The PDN type shall be set based on the requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach. The P-GW of the SAEGW creates a new entry in its bearer context table and generates a Charging Id. The new entry allows the P-GW of the SAEGW to route user plane PDUs between the Trusted non-3GPP IP Access Network and the packet data network and to start the charging process.
6	The P-GW initiates the IP-CAN Session Establishment Procedure with the PCRF.
7	The selected P-GW of the SAEGW informs the 3GPP AAA Server of its P-GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the P-GW is located. This information is registered in the HSS.
8	The P-GW returns a Create Session Response (CSResp) message to the TWAN, including the IP address(es) allocated for the UE.
9	The GTP tunnel is set up between the TWAN and the P-GW. Initial Attach is completed.

Figure 15: S2a LTE-to-WiFi Handover on the SAEGW

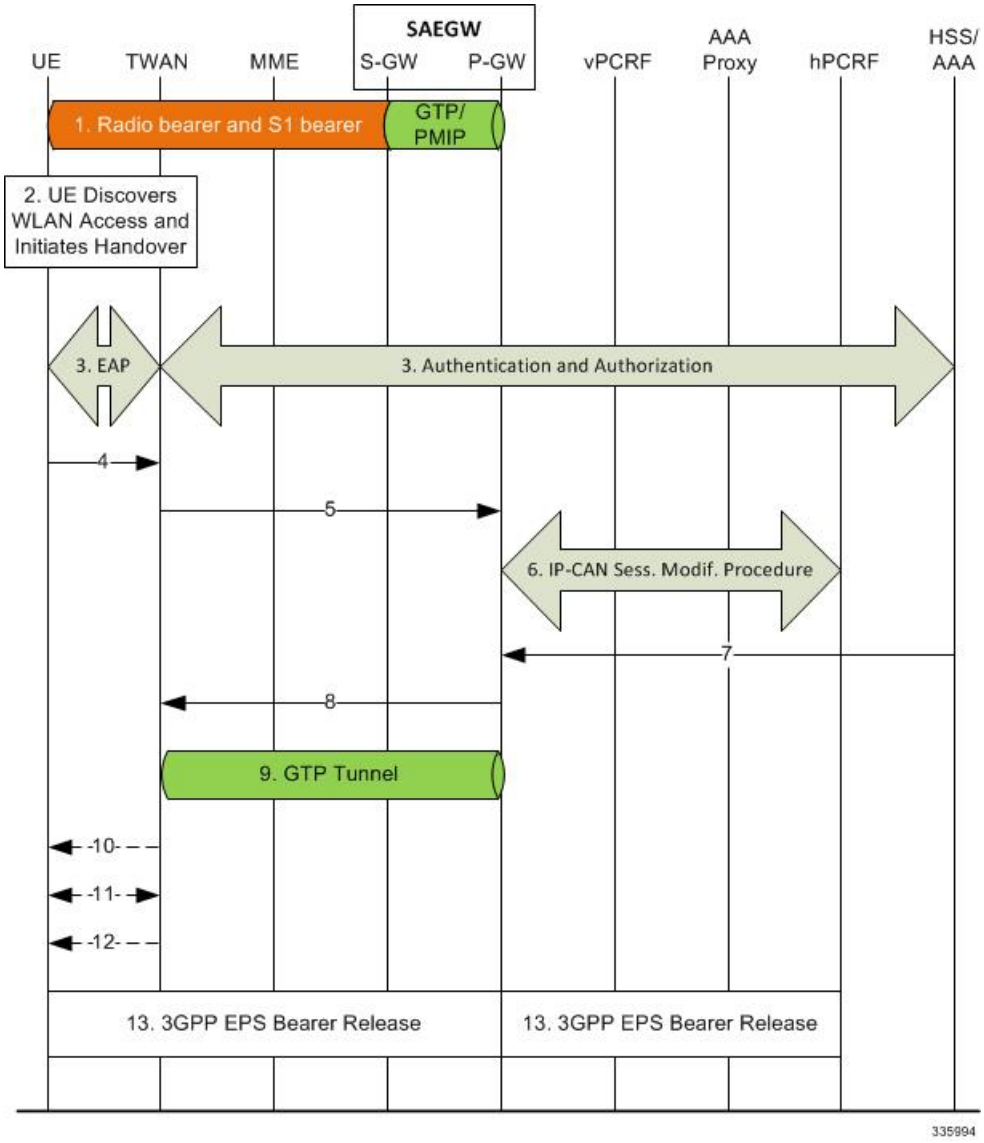


Table 11: S2a LTE-to-WiFi Handover on the SAEGW

Step	Description
1	
2 - 4	In Steps 2-4, the UE discovers WLAN access and initiates a handover. The TWAN takes authorization from the AAA server.

Step	Description
5	The TWAN sends a Create Session Request (including IMSI, APN, RAT type) message to the P-GW of the SAEGW The RAT type WLAN indicates the non-3GPP IP access technology type. The TWAN does not set the 'Handover Indication' bit. Instead, based on the IMSI, APN and RAT type the P-GW of the SAEGW determines that it is a potential handover from the TWAN. The P-GW of the SAEGW re-allocates the same IPv4 address and/or IPv6 address assigned to the UE while it was connected to 3GPP IP access.
6	The P-GW of the SAEGW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF with RAT type as WLAN.
7	The P-GW of the SAEGW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN and obtains authorization information from the 3GPP AAA Server. The 3GPP AAA Server decides whether or not to update PDN GW identification according to the UE capability, which was provided at the authentication phase.
8	The P-GW of the SAEGW responds with a Create Session Response to the TWAN. The Create Session Response contains the IPv4 address and/or the IPv6 address assigned to the UE while it was connected to the 3GPP IP access.
9	A GTP tunnel is setup between TWAN and the P-GW of the SAEGW.
10	
11	
12	
13	The P-GW of the SAEGW begins the P-GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [6], clause 5.4.4.1 for GTP-S5/S8 interfaces.

Figure 16: S2a WiFi-to-LTE Handover on the SAEGW

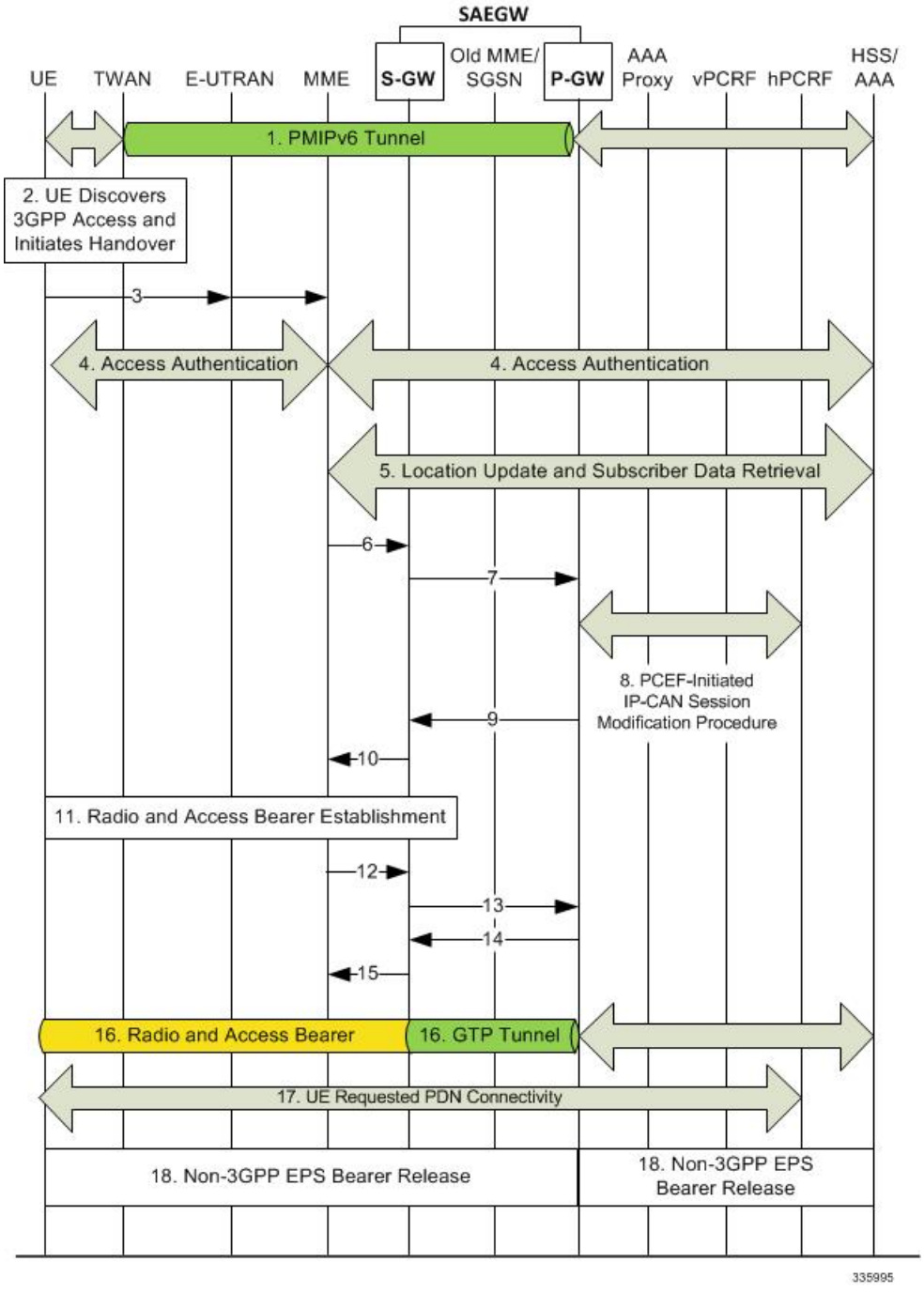


Table 12: S2a WiFi-to-LTE Handover on the SAEGW

Step	Description
1	

Step	Description
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

Configuring the GTP-based S2b Interface on the P-GW and SAEGW

This section describes how to configure the GTP-based S2b interface support feature.

Configuring GTP-based S2b Interface Support

Use the following example to configure GTP-based S2b interface support on the P-GW and SAEGW.

Important GTP-based S2a/S2b interface support on the P-GW and SAEGW is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress s2b
         end
```

Disable S2b interface support by entering the following commands:

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress
         end
```

Verifying the Configuration

This section describes how to verify the GTP-based S2a/S2b interface configuration on the P-GW and SAEGW.

Use the **show configuration** command from Exec Mode to verify that the configuration is active. Look for the eGTP service configuration section in the output:

```
egtp-service EGTP
   interface-type interface-pgw-ingress s2a s2b
```

Once the S2b license is installed and active, run a WiFi Initial Attach Call to check that a successful call is setup. From Exec Mode, use the **show subscribers all** command to verify that the call was successful.

Monitoring the GTP-based S2b Interface Feature

This section provides commands that operators can use to monitor the GTP-based S2b interface feature on the P-GW and SAEGW.

GTP-based S2b Interface Show Commands

This section provides information regarding show commands and/or their outputs for GTP-based S2b interface support.

show pgw-service statistics all

For S2b interface support on the standalone P-GW: This command provides statistics on the number of attempts, failures, and successes for the following S2b interface functions:

- S2bGTP-to-LTE handovers
- LTE-to-S2bGTP handovers

show subscribers epdg-address

This command provides information on the S2b P-GW subscribers connected to the ePDG over the S2b interface.

show subscribers saegw-only epdg-address

This command shows information related to subscribers of the P-GW of the SAEGW connected to a specific ePDG over the S2b interface.

show subscribers saegw-only interface-type S2bGTP

This command shows information related to GTP P-GW subscribers of the SAEGW connected via the S2b interface.

show subscribers summary pgw-address

This command provides information on the number of Active and Dormant GTP S2b IPv4 and IPv6 subscribers.

show subscribers pgw-only full all

For S2b interface support on the standalone P-GW: Use this command to view S2b call related information for P-GW subscribers. The output will provide the following S2b specific information:

- Interface Type (S2b PGW GTP-C interface)
- MAC Address
- ePDG c-teid (ePDG control tunnel endpoint identifier)
- ePDG u-teid (ePDG bearer tunnel endpoint identifier)
- ePDG c-addr (ePDG control IP address)
- ePDG u-addr (ePDG bearer IP address)

show subscribers pgw-only epdg-address

For S2b interface support on the standalone P-GW: Use this command to view all S2b information for all the subscribers' sessions that exist on the P-GW for a specific ePDG. The ePDG is specified by the epdg-address (in IPv4 or IPv6 address format).

show subscribers summary epdg-address

For S2b interface support on the standalone P-GW: Use this command to view statistics for all the subscribers' sessions that exists on the P-GW that belong to the S2b interface on a specific ePDG. The ePDG is specified by the epdg-address.

show subscribers summary interface-type S2bGTP

For S2b interface support on the standalone P-GW: View the number of active and dormant subscriber sessions on the P-GW that belong to the S2b interface.

show subscribers saegw-only full all

For S2b interface support on the SAEGW: This command provides S2b call-related information for P-GW subscribers, including:

- Access Tech
- Interface Type
- Access Point MAC Address
- sgw c-teid
- ePDG c-teid
- sgw c-addr
- ePDG c-addr
- sgw u-teid
- ePDG u-teid
- sgw u-addr
- ePDG u-addr

show saegw-service statistics all function pgw

For S2b interface support on the SAEGW: This command provides statistics related to successes, failures and attempts for various S2bGTP handovers for all P-GW SAEGW services, including:

- S2bGTP-to-LTE handover
  - Attempted
  - Succeeded
  - Failed
- LTE-to-S2bGTP handover
  - Attempted
  - Succeeded
  - Failed

Monitoring the GTP-based S2a Interface Feature

This section provides information on how to monitor the GTP-based S2a interface feature.

GTP-based S2a Interface Show Commands

This section provides information regarding show commands and/or their outputs for GTP-based S2a interface support.

show pgw-service statistics all

The output of this command has been enhanced to provide statistics on S2aGTP-to-LTE and LTE-to-S2aGTP handovers. It records the total number of handover attempts, and the number of attempts that succeeded and failed.

show saegw-service statistics all

The output of this command provides information related to subscribers, bearers, and PDNs on the S2a interface.

show saegw-service statistics all function-pgw

The output of this command provides subscriber, PDN and handover statistics for the P-GW function of the SAEGW on the S2a interface.

show session-subsystem facility sessmgr service-type pgw-ingress

The output of this command has been enhanced to provide S2a interface session information to troubleshoot subscriber session problems and for general monitoring for orphaned sessions. If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

show subscribers pgw-only full all

The output of this command has been enhanced to show S2a call-related information, including access technology, TWAN, and TEID information.

show subscribers saegw-only full all

The output of this command contains subscriber information related to the S2a interface, including subscriber ID information, TEID and address information, and input/output packets recorded and dropped.

show subscribers saegw-only interface-type S2aGTP

The **S2aGTP** keyword has been added to this command to enable operators to view detailed information for S2a subscriber sessions, including call code, CALLID, IMSI/IMEI, APN and Time-Idle.

show subscribers summary interface-type S2aGTP

The output provides interface type details on subscribers connected via the S2a interface. The output provides interface type details on subscribers connected via the S2a interface. Information is given for both IPv4, IPv6, and IPv4v6 interfaces.

show subscribers summary pgw-address

The output of this command contains S2a subscriber information for the specified P-GW. Interface information is included for IPv4, IPv6 and IPv4v6 interfaces.