Wi-Fi Handovers

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
TFT Handling for WiFi Handovers is supported.	2021.01.0
The Wi-Fi to 5GS Handover with EPS Fallback feature is fully qualified in this release.	2020.02.2
The Wi-Fi to 5GS Handover with EPS Fallback feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.1

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF+PGW-C product supports Wi-Fi handovers. The cloud-based architecture supports the following Wi-Fi handovers in 5GS or EPS and non-3GPP untrusted access.

- EPC to non-3GPP untrusted Wi-Fi handover
- Non-3GPP untrusted Wi-Fi to EPC handover
- Non-3GPP untrusted Wi-Fi to 5GS handover with EPS fallback
- Non-3GPP untrusted Wi-Fi to 5GS handover
- 5GS to non-3GPP untrusted Wi-Fi handover

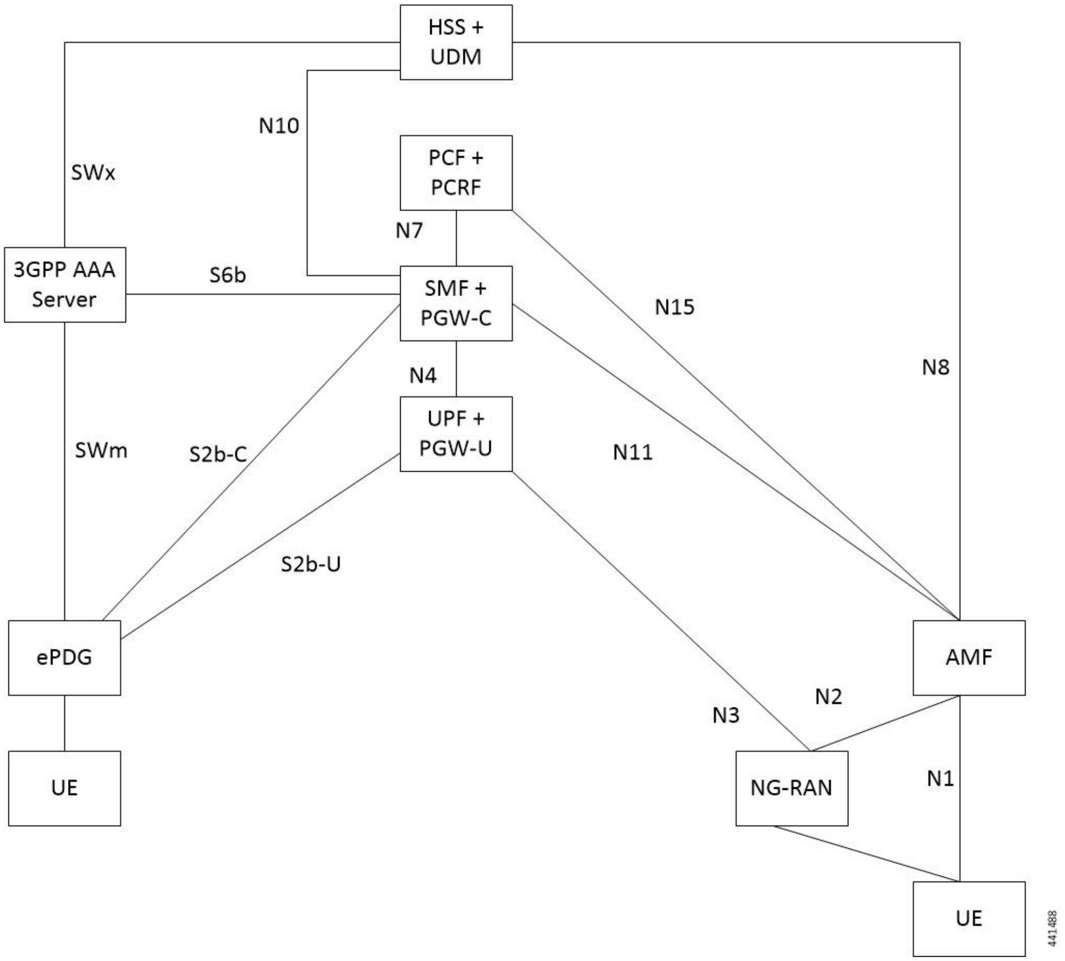
Architecture

The following sections describe the architecture for interworking between the ePDG or EPC and 5GS and the nonroaming architecture within the EPS using S5 and S2b interfaces.

ePDG and 5GS Interworking for Handover

The following figure illustrates the non-roaming architecture for interworking between the ePDG or EPC and 5GS.

Figure 1: Non-roaming Architecture for Interworking between ePDG or EPC and 5GS



The interworking between the ePDG and 5GS is similar to the interworking between the EPC and 5GS without the N26 interface. In this interworking, the IP address preservation occurs on the UEs on inter-system mobility. Fetching and saving the PGW-C and SMF and the corresponding APN and DNN information through the HSS and UDM makes interworking possible. In such networks, the AMF also supports interworking with UEs without the N26 interface during the initial registration in 5GC. The AMF may support interworking with UEs without N26 in the Attach procedure in 5GS. In case of a non-3GPP untrusted Wi-Fi access, the ePDG does not communicate with the AMF because the N26 interface does not exist.

A 5GS supports network slicing and can interwork with the EPS in its PLMN or in other PLMNs. The SMF+PGW-C performs UDM registration for each UE with PGW-C FQDN and NSSAI values. With this registration, the AMF or ePDG identify the PGW-C IP-address from the UDM or HSS as part of the subscription information after the UE authorization is completed.

The mobility between 5GC to EPC does not ensure that all the active PDU sessions can be transferred to the EPC. During PDN connection establishment in the EPC, the UE allocates the PDU session ID and sends it to the PGW-C+SMF through the PCO.

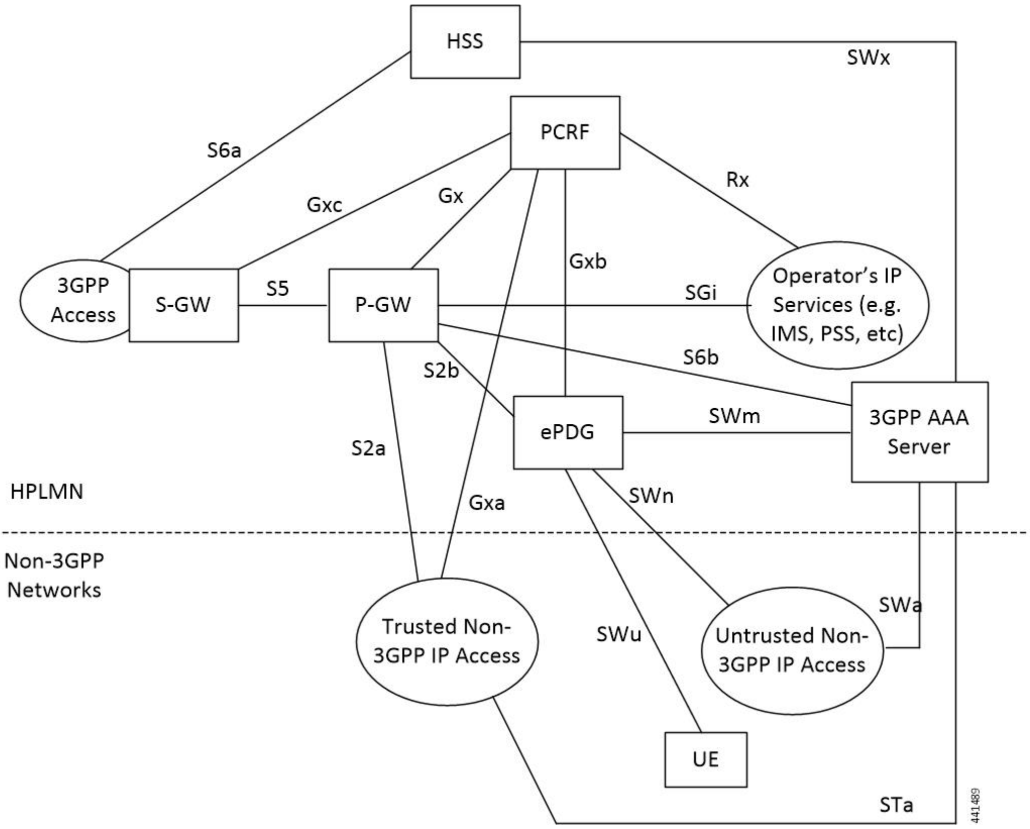
An S-NSSAI that is associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF. For example, the combination of PGW-C+SMF address and APN is sent to the UE in the PCO along with a PLMN ID to which the S-NSSAI relates. If the PGW-C+SMF supports multiple S-NSSAI and the APN is valid for multiple S-NSSAIs, the PGW-C+SMF selects only the S-NSSAI that is mapped to the subscribed S-NSSAIs of the UE.

The UE saves the S-NSSAI and the PLMN ID that is associated with the PDN connection. The UE derives the requested NSSAI through the received PLMN ID. The NAS registration request message includes the requested NSSAI. The RRC carries the registration request when the UE registers in 5GC. This scenario is applicable if the UE is non-roaming or the UE has configured NSSAI for the VPLMN in roaming case.

EPS and ePDG Interworking for Handover

The following figure illustrates the non-roaming architecture within the EPS using S5 and S2b interfaces.

Figure 2: Non-roaming Architecture Within EPS using S5, S2a, and S2b Interfaces



For 3GPP access to non-3GPP access untrusted Wi-Fi handover and for non-3GPP access untrusted Wi-Fi to 3GPP access handover, if a UE has multiple PDN connections to different APNs in the source access and the UE can route different simultaneously active PDN connections through different access networks, the UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them. This transfer can have the restriction that multiple PDN connections to the same APN have one access.

The transfer process can occur in the following scenarios:

- 3GPP access to non-3GPP access untrusted Wi-Fi handover
- Non-3GPP access untrusted Wi-Fi to 3GPP access handover

The UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them if the following conditions are met:

- The UE has multiple PDN connections to different APNs in the source access
- The UE can route different, but simultaneously active, PDN connections through different access networks."

The SMF supports untrusted Wi-Fi access for end-users over S2b interface with ePDG after establishment of IPSec connection between the end-user and ePDG.

For untrusted Wi-Fi to EPC handover, the SMF provides a PGW-C FQDN during UDM registration and fetches the subscription information.

During UE handover, the MME fetches PGW-C FQDN from the HSS. After authentication, the MME initiates GTPv2 create session request indicating handover. The SMF+PGW-C does not perform the UDM registration and subscription procedures while processing handover request. SMF+PGW-C ensures that GTPv2 MB request indicating handover is sent to perform data path switching from untrusted Wi-Fi to EPC.

For EPC to untrusted Wi-Fi handover, the HSS provides SMF+PGW-C FQDN after the subscriber authentication. When UE performs handover, after authentication HSS provides SMF+PGW-C FQDN. The ePDG initiates GTPv2 create session request indicating handover toward PGW after IPSec tunnel establishment. SMF+PGW-C performs the UDM registration and no subscription procedures exist while processing the handover request.

TFT Handling for WiFi Handovers

In 4G and 5G deployment, the three-way audio or video multiparty call conference, and RCS message use cases, PGW-C ends up having more than four filters (it can go upto max 16 filters) for both UL and DL direction. SMF includes “EPS Bearer Level Traffic Flow Template (Bearer TFT)” is included in the GTPv2 CBReq/UBReq of BearerContextList. CBReq/UBReq carry maximum of 4 TFTs per bearer.

In case of three-way Audio/Video and multiparty call-conference, PCF tries to push the pccRules by adding different subscriber TFTs in multiple “N7 Policy Notify Req” messages. PGW-C handles the received “N7 Update Notify Req” in dedicated bearer establishment or update towards WiFi or LTE by initiating GTPv2 CBReq or UBReq messages. SMF accommodates the received SDF Filters in TFT as it never crosses more than 256 Bytes (4 TFTs).

Note PGW-C don’t support more than 4TFTs received from PCF “N7 Policy Notify Req”.

PCF keeps pushing multiple pccRules for same bearer by sending “N7 Policy Notify Req” and over the period SMF ends up having 12-16 filters for case of multiparty call.

When subscriber moves from LTE to WiFi or WiFi to LTE or NR to WiFi Handover call-model cases, SMF first establishes default bearer creation as part of HO. SMF then tries to send out CBReq for Dedicated bearer establishment by accommodating all 16 filters in “EPS Bearer Level Traffic Flow Template (Bearer TFT)” of bearer context list of the subscriber and if it fails to encode because of these restrictions. The SMF sends out CBReq without “EPS Bearer Level Traffic Flow Template (Bearer TFT)” IE based on HO type, SGW/MME/ePDG rejects GTPv2 CBResp with Mandatory IE Incorrect with “TFT Semantic Errors”.

After receiving CBResp from SGW/ePDG, SMF doesn’t free up policy/charging resources for respective failed bearers and that leads to further stale entries on SMF and UPF which leads to system inconsistency for that subscriber with “EBI Mismatch – 408 Error Voice Call Failure WiFi HOs”.

Standards Compliance

The Wi-Fi handovers feature complies with the following standards:

- *3GPP TS 23.502 V15.2.0 (2018-09)*
- *3GPP TS 23.402 V15.3.0 (2018-03)*
- *3GPP TS 29.214 V15.5.0 (2018-03)*

How it Works

This section describes the Wi-Fi to LTE handover, Wi-Fi handover with EPS fallback, and Wi-Fi to 5GS handover.

EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the EPC to non-3GPP untrusted Wi-Fi handover call flow.

Figure 3: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

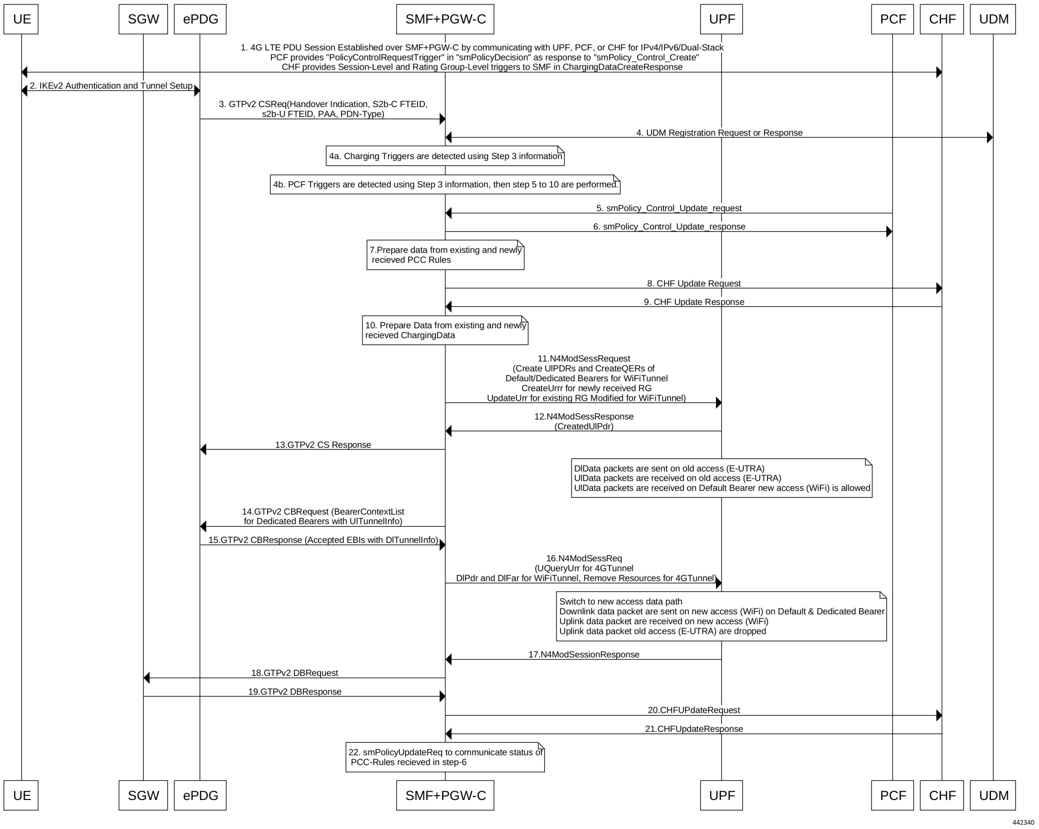

UE
SGW
ePDG
SMF+PGW-C
UPF
PCF
CHF
UDM
1. 4G LTE PDU Session Established over SMF+PGW-C by communicating with UPF, PCF, or CHF for IPv4/IPv6/Dual-Stack
PCF provides "PolicyControlRequestTrigger" in "smPolicyDecision" as response to "smPolicy_Control_Create"
CHF provides Session-Level and Rating Group-Level triggers to SMF in ChargingDataCreateResponse
2. IKEv2 Authentication and Tunnel Setup
3. GTPv2 CSReq(Handover Indication, S2b-C FTEID,
s2b-U FTEID, PAA, PDN-Type)
4. UDM Registration Request or Response
4a. Charging Triggers are detected using Step 3 information
4b. PCF Triggers are detected using Step 3 information, then step 5 to 10 are performed.
5. smPolicy_Control_Update_request
6. smPolicy_Control_Update_response
7.Prepare data from existing and newly
recieved PCC Rules
8. CHF Update Request
9. CHF Update Response
10. Prepare Data from existing and newly
recieved ChargingData
11.N4ModSessRequest
(Create UlPDRs and CreateQERs of
Default/Dedicated Bearers for WiFiTunnel
CreateUrrr for newly received RG
UpdateUrr for existing RG Modified for WiFiTunnel)
12.N4ModSessResponse
(CreatedUlPdr)
13.GTPv2 CS Response
DlData packets are sent on old access (E-UTRA)
UlData packets are received on old access (E-UTRA)
UlData packets are received on Default Bearer new access (WiFi) is allowed
14.GTPv2 CBRequest (BearerContextList
for Dedicated Bearers with UlTunnelInfo)
15.GTPv2 CBResponse (Accepted EBIs with DlTunnelInfo)
16.N4ModSessReq
(UQueryUrr for 4GTunnel
DlPdr and DlFar for WiFiTunnel, Remove Resources for 4GTunnel)
Switch to new access data path
Downlink data packet are sent on new access (WiFi) on Default & Dedicated Bearer
Uplink data packet are received on new access (WiFi)
Uplink data packet old access (E-UTRA) are dropped
17.N4ModSessionResponse
18.GTPv2 DBRequest
19.GTPv2 DBResponse
20.CHFUPdateRequest
21.CHFUpdateResponse
22. smPolicyUpdateReq to communicate status of
PCC-Rules recieved in step-6
UE
SGW
ePDG
SMF+PGW-C
UPF
PCF
CHF
UDM
442340

Table 3: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE is attached to the 3GPP access network. The SMF+PGW-C communicates with UPF, PCF, and CHF for IPv4, IPv6, or dual-stack to establish 4G LTE PDU session. The PCF sends the Policy Control Request trigger, which is the SM policy decision, in response to SM policy control create. The CHF provides session-level or rating-group-level triggers to the SMF in Charging Data Create response.
2	The UE connects to an untrusted non-3GPP access and an ePDG is selected through the ePDG selection process. Then, the UE initiates the handover attach procedure as defined in *3GPP TS 23.402, section 8.6.2.1*. After the IKE tunnel is established between the UE and ePDG and after the UE is authenticated over SWm interface with AAA server, the UE initiates IKE authentication (IKE_AUTH). The IKE_AUTH includes configuration parameters of the earlier assigned IPv4 or IPv6 addresses in the EPC and P-CSCF and the DNS options.
3	The ePDG sends a Create Session Request to the P-GW. This request includes the following details: • IMSI • APN • Handover indication • RAT type • ePDG TEID of the Control Plane • ePDG address for the User Plane • ePDG TEID of the User Plane • EPS bearer identity • User location The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and is included in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session Request to allow the PDN gateway to reallocate the same IP address or the prefix assigned to the UE. This IP address or prefix is assigned while UE is connected to the 3GPP IP access and initiates the policy modification procedure with PCF.
4a	The SMF performs UDM registration by updating the PGW-C FQDN with UDM. The UDM registration does not occur during the session establishment with EPC.
4b	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4c	The SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to the PCF.

Step	Description
6	The PCF includes new or updated PCC rules and sends the SM Policy Control Update response. The Update response includes information on the SM policy decision.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If new PCC rules are received in Step 6 with new Rating Group that requires quota information, SMF sends the Charging Update request to CHF. SMF also includes new access parameters for the PDU session information.
9	CHF sends the Charging Update Response with multi-unit information that contains quota information for the requested rating-group in Step 8 to SMF. CHF may also send the new quota information for the existing rating-group of EPC session.
10	SMF processes the information that is received as Charging Update response from CHF.
11	SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, and update on URR for modified quota information.
12	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SMF sends the GTPv2 Create Bearer request to S-GW. This request includes information on bearer context list, which contains DL tunnel information to end-user, to be created.
15	S-GW sends the GTPv2 Create Bearer response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
16	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to create the DL PDR and DL FAR with DL tunnel information for each bearer, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
17	UPF sends the usage report as N4 Session Modification response to SMF.
18	SMF+PGW-C sends the GTPv2 DB request to S-GW. This request includes EBI or list of EBIs.
19	S-GW sends the GTPv2 DB response to SMF+PGW-C.
20	SMF sends the Charging Update request to CHF. This request includes the PDU session information with the new access params and multi-usage report containing details on the access params and usage report that is received in Step 8
21	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information may include new quota information for the existing rating-groups.

Step	Description
22	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in *3GPP 23.502, section 4.3.3.2*.

Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to EPC handover call flow.

Figure 4: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

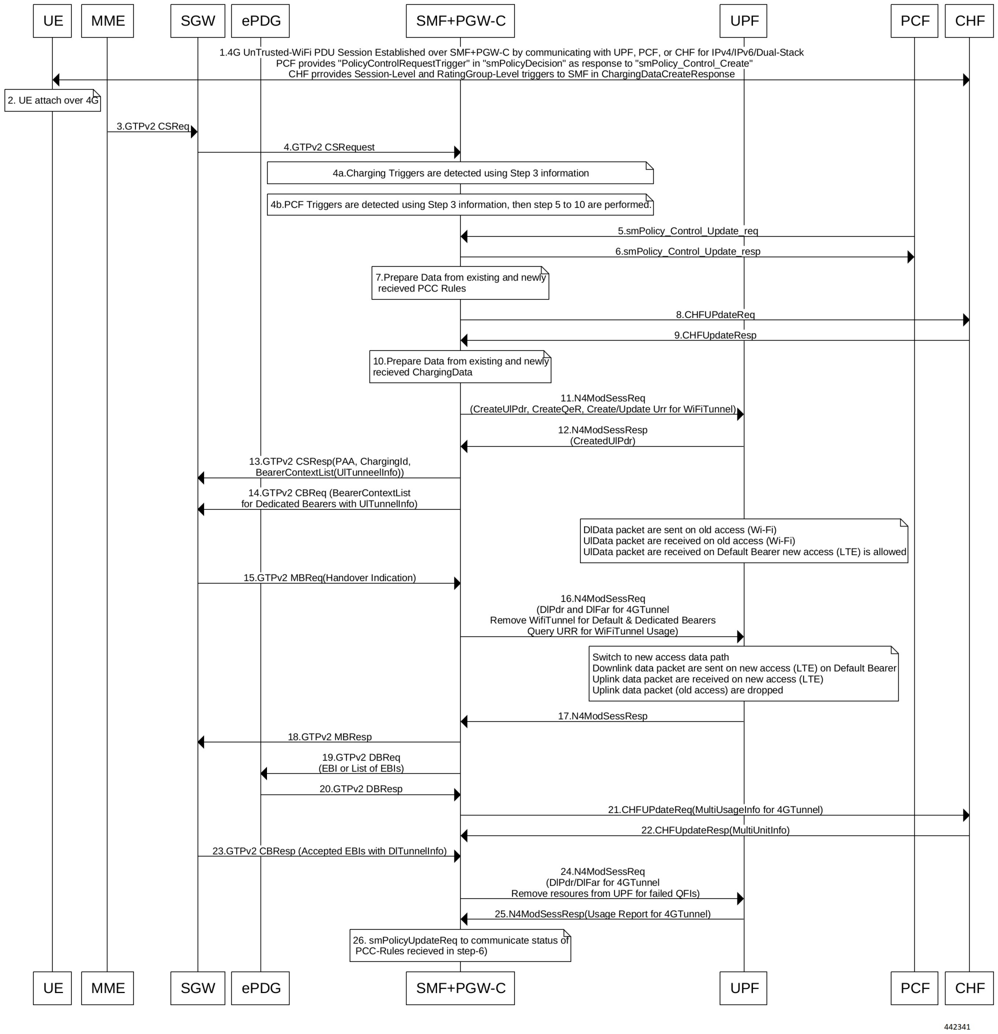

UE
MME
SGW
ePDG
SMF+PGW-C
UPF
PCF
CHF
1.4G UnTrusted-WiFi PDU Session Established over SMF+PGW-C by communicating with UPF, PCF, or CHF for IPv4/IPv6/Dual-Stack
PCF provides "PolicyControlRequestTrigger" in "smPolicyDecision" as response to "smPolicy_Control_Create"
CHF prrovides Session-Level and RatingGroup-Level triggers to SMF in ChargingDataCreateResponse
2. UE attach over 4G
3.GTPv2 CSReq
4.GTPv2 CSRequest
4a.Charging Triggers are detected using Step 3 information
4b.PCF Triggers are detected using Step 3 information, then step 5 to 10 are performed.
5.smPolicy_Control_Update_req
6.smPolicy_Control_Update_resp
7.Prepare Data from existing and newly recieved PCC Rules
8.CHFUPdateReq
9.CHFUpdateResp
10.Prepare Data from existing and newly recieved ChargingData
11.N4ModSessReq (CreateUlPdr, CreateQeR, Create/Update Urr for WiFiTunnel)
12.N4ModSessResp (CreatedUlPdr)
13.GTPv2 CSResp(PAA, ChargingId, BearerContextList(UlTunneelInfo))
14.GTPv2 CBReq (BearerContextList for Dedicated Bearers with UlTunnelInfo)
DlData packet are sent on old access (Wi-Fi)
UlData packet are received on old access (Wi-Fi)
UlData packet are received on Default Bearer new access (LTE) is allowed
15.GTPv2 MBReq(Handover Indication)
16.N4ModSessReq (DlPdr and DlFar for 4GTunnel Remove WifiTunnel for Default & Dedicated Bearers Query URR for WiFiTunnel Usage)
Switch to new access data path
Downlink data packet are sent on new access (LTE) on Default Bearer
Uplink data packet are received on new access (LTE)
Uplink data packet (old access) are dropped
17.N4ModSessResp
18.GTPv2 MBResp
19.GTPv2 DBReq (EBI or List of EBIs)
20.GTPv2 DBResp
21.CHFUPdateReq(MultiUsageInfo for 4GTunnel)
22.CHFUpdateResp(MultiUnitInfo)
23.GTPv2 CBResp (Accepted EBIs with DlTunnelInfo)
24.N4ModSessReq (DlPdr/DlFar for 4GTunnel Remove resoures from UPF for failed QFIs)
25.N4ModSessResp(Usage Report for 4GTunnel)
26. smPolicyUpdateReq to communicate status of PCC-Rules recieved in step-6)
442341

Table 4: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE discovers the E-UTRAN access and hands over the sessions from the currently used non-3GPP access system to E-UTRAN. For details on UE discovery of the 3GPP access system, see *3GPP TS 23.401*, section 4.8. UE sends an Attach request to MME for the Handover Attach request type. E-UTRAN routes the messages received from UE to MME as defined in *3GPP TS 23.401*. UE includes the one of the APNs which are corresponding to the PDN connections in the source non-3GPP access. The APN is provided as defined in *3GPP TS 23.401*.
3	MME and HSS perform authentication, which is followed by location update procedure and subscriber data retrieval to receive the APN information. The MME selects an APN, an SGW and PDN gateway as defined in *3GPP TS 23.401*. MME sends a Create Session Request message to SGW. This request includes information on IMSI, MME context ID, PDN-GW address, handover indication for the “handover” request type, and APN.
4	SGW sends a Create Session Request, which is handover indication, message to PDN-GW in the HPLMN as described in *3GPP TS 23.401*. As the MME includes the handover indication information in the Create Session Request message, the SGW sends the GTPv2 Create Session Request message to PDN GW. This message includes details on IMSI, APN, handover indication, RAT type, S5-C TEID, S5-U TEID of the user plane, EBI, and user location information. The RAT type indicates the 3GPP IP access E-UTRAN technology type. If the UE supports IP address preservation and is included in PAA, the SGW configures the handover indication in the Creation Session Request. With this configuration, the PDN GW re-allocates the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access. With this configuration, SGW initiates the Policy Modification Procedure to the PCF. As the handover indication is includes, the PDN GW does not switch the tunnel from non-3GPP IP access to 3GPP access system at this point. SMF does not perform the UDM Registration as the registration happens during the Wi-Fi session establishment.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4b	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
6	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.

Step	Description
8	If SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request, with the new rating-group having quota information, to CHF. This request includes the PDU session information with the new access params.
9	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the rating-group and the existing rating-group of EPC session, if any.
10	SMF prepares the charging data of the received Charging Update Response that CHF sent.
11	SMF sends the N4 Session Modification Request to UPF. This request includes the details on creation of UL and DL PDR, creation of QER, creation of URR for received new rating-group quota information, updated URR for modified quota information, and creation of FAR.
12	UPF sends the UL tunnel information in the created PDR as N4 Session Modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SGW sends the Modification Bearer request with handover indication to PGW for data path switching from Wi-Fi tunnel to 4G tunnel.
15	PGW sends the N4 Session Modification request to delete the Wi-Fi tunnel and to configure DL tunnel information that is received in GTPv2 Create Session request for 4G tunnel in Step 4.
16	UPF sends the N4 Session Modification response to SMF.
17	SMF sends the GTPv2 Create Session request, which includes the bearer context list, to SGW. This list includes the DL Tunnel information for the end-user.
18	SGW sends the GTPv2 Create Session response to SMF. This response includes details on request accepted or request accepted partially and bearer contexts.
19	ePDG sends the GTPv2 Create Bearer resp (accepted EBIs with DL tunnel info to SMF
20	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to update the DL FAR with the DL tunnel information, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
21	UPF sends the N4 Session Modification Response with usage report to SMF.
22	SMF sends the Charging Update request to CHF. This request includes the PDU session information with new access params and multi-usage report consisting of access-params and usage report that is received in Step 8.
23	CHF sends the Charging Update Response with multi-unit information that contains quota information for the existing rating-groups to SMF.
24	SMF+PGW-C initiates the GTPv2 DB Request toward SGW by including EBI or EBI list.
25	SGW sends the GTPv2 DB Response toward SMF+PGW-C.

Step	Description
26	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to 5GS handover call flow.

Figure 5: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

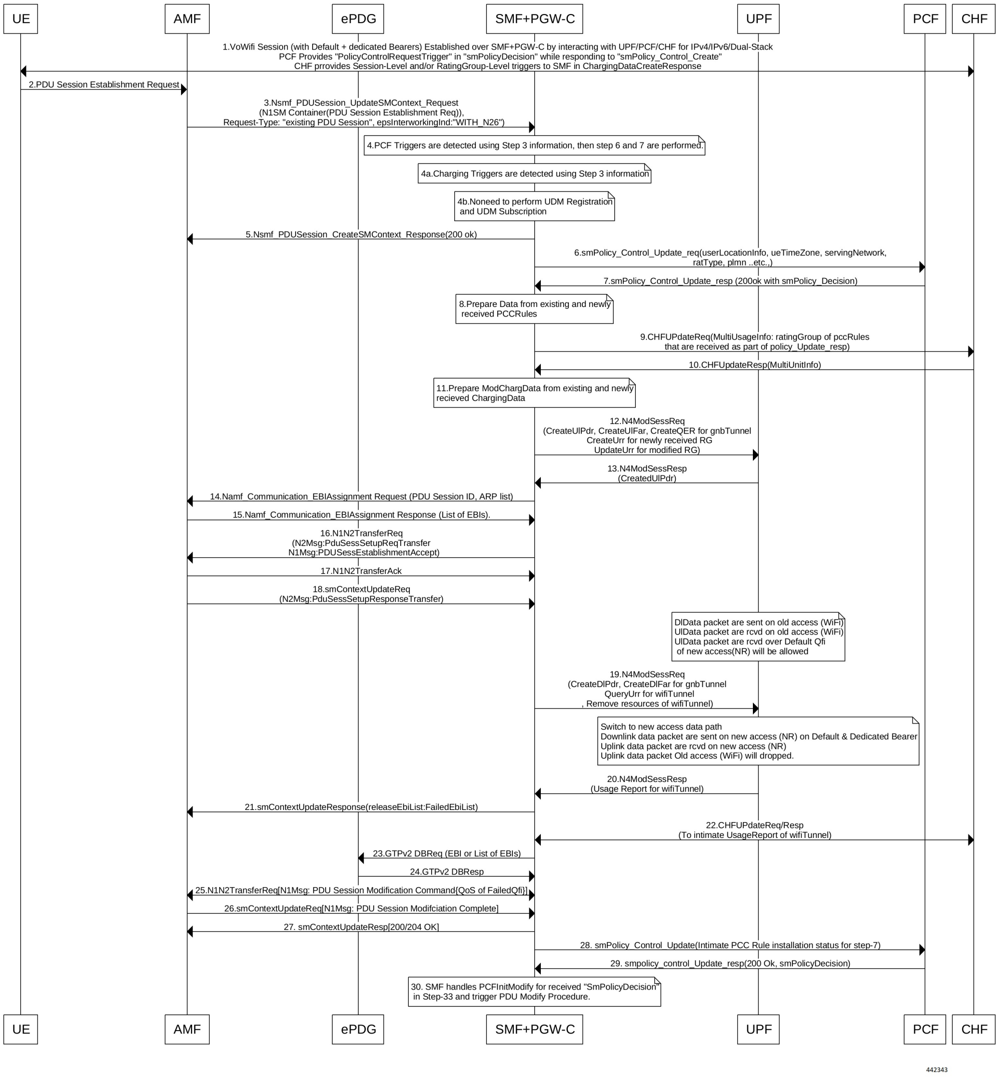

UE
AMF
ePDG
SMF+PGW-C
UPF
PCF
CHF
1.VoWifi Session (with Default + dedicated Bearers) Established over SMF+PGW-C by interacting with UPF/PCF/CHF for IPv4/IPv6/Dual-Stack
PCF Provides "PolicyControlRequestTrigger" in "smPolicyDecision" while responding to "smPolicy_Control_Create"
CHF prrovides Session-Level and/or RatingGroup-Level triggers to SMF in ChargingDataCreateResponse
2.PDU Session Establishment Request
3.Nsmf_PDUSession_UpdateSMContext_Request
(N1SM Container(PDU Session Establishment Req)),
Request-Type: "existing PDU Session", epsInterworkingInd:"WITH_N26")
4.PCF Triggers are detected using Step 3 information, then step 6 and 7 are performed.
4a.Charging Triggers are detected using Step 3 information
4b.Noneed to perform UDM Registration
and UDM Subscription
5.Nsmf_PDUSession_CreateSMContext_Response(200 ok)
6.smPolicy_Control_Update_req(userLocationInfo, ueTimeZone, servingNetwork,
ratType, plmn ..etc.,)
7.smPolicy_Control_Update_resp (200ok with smPolicy_Decision)
8.Prepare Data from existing and newly
received PCCRules
9.CHFUPdateReq(MultiUsageInfo: ratingGroup of pccRules
that are received as part of policy_Update_resp)
10.CHFUpdateResp(MultiUnitInfo)
11.Prepare ModChargData from existing and newly
recieved ChargingData
12.N4ModSessReq
(CreateUlPdr, CreateUlFar, CreateQER for gnbTunnel
CreateUrr for newly received RG
UpdateUrr for modified RG)
13.N4ModSessResp
(CreatedUlPdr)
14.Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list)
15.Namf_Communication_EBIAssignment Response (List of EBIs).
16.N1N2TransferReq
(N2Msg:PduSessSetupReqTransfer
N1Msg:PDUSessEstablishmentAccept)
17.N1N2TransferAck
18.smContextUpdateReq
(N2Msg:PduSessSetupResponseTransfer)
DlData packet are sent on old access (WiFi)
UlData packet are rcvd on old access (WiFi)
UlData packet are rcvd over Default Qfi
of new access(NR) will be allowed
19.N4ModSessReq
(CreateDlPdr, CreateDlFar for gnbTunnel
QueryUrr for wifiTunnel
, Remove resources of wifiTunnel)
Switch to new access data path
Downlink data packet are sent on new access (NR) on Default & Dedicated Bearer
Uplink data packet are rcvd on new access (NR)
Uplink data packet Old access (WiFi) will dropped.
20.N4ModSessResp
(Usage Report for wifiTunnel)
21.smContextUpdateResponse(releaseEbiList:FailedEbiList)
22.CHFUPdateReq/Resp
(To intimate UsageReport of wifiTunnel)
23.GTPv2 DBReq (EBI or List of EBIs)
24.GTPv2 DBResp
25.N1N2TransferReq[N1Msg: PDU Session Modification Command{QoS of FailedQfi}]
26.smContextUpdateReq[N1Msg: PDU Session Modifciation Complete]
27. smContextUpdateResp[200/204 OK]
28. smPolicy_Control_Update(Intimate PCC Rule installation status for step-7)
29. smpolicy_control_Update_resp(200 Ok, smPolicyDecision)
30. SMF handles PCFInitModify for received "SmPolicyDecision"
in Step-33 and trigger PDU Modify Procedure.
UE
AMF
ePDG
SMF+PGW-C
UPF
PCF
CHF
442343

Table 5: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE sends the PDU Session Establishment request through 3GPP access to AMF. This request includes details on PDU session ID, requested PDU session type, requested SSC mode, 5GSM capability PCO, SM PDU DN request container, number of packet filters, and an optional requested always-on PDU session. The request type with an existing PDU session indicates switching between 3GPP access and non-3GPP access or to a PDU session handover from an existing PDN connection in EPC.
3	If the request type is "Existing PDU Session", the AMF selects the SMF based on SMF-ID that is received from UDM. For this request type, if AMF does not identify the PDU Session ID or the subscription context that the AMF received from UDM during the Registration or if the subscription profile update notification procedure contains no SMF ID corresponding to the PDU Session ID, an error occurs. Then, AMF updates the Access Type stored for the PDU session. If the request type with an existing PDU session refers to a PDU session that moved between 3GPP access and non-3GPP access and if the S-NSSAI of the PDU session is available in the Allowed NSSAI of the target access type, the PDU Session Establishment procedure is performed when the SMF ID corresponding to the PDU Session ID and the AMF are part of the same PLMN. AMF sends the NSMF PDU Session Create SM Context Request with the request type "Existing PDU Session" to SMF. This request includes information on SUPI, DNN, S-NSSAIs, PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container including the PDU Session Establishment Request, User location information, Access Type, PEI, GPSI, Subscription For PDU Session Status Notification, DNN Selection Mode. SMF analyzes the existing PDU session from the PDU Session Establishment request using SUPI+PDU-Session-ID. SMF also compare the IPv4 or IPv6 addresses of the received UE against the retrieved PDU session IPv4 or IPv6 addresses. SMF reject the request if the session is not retrieved or IPv4 or IPv6 addresses do not match.
4	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the earlier communication with PCF during Wi-Fi session.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during Wi-Fi session.
4b	SMF does not perform the UDM registration as happens during Wi-Fi Session Establishment.
5	SMF sends the NSMF PDU Session Create SM Context response to AMF. This response includes the cause, SM Context ID or N1 SM container with PDU session rejection cause.
6	Based on the detected armed Policy Control Triggers that are received in Step 4a, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
7	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.

Step	Description
8	Based on the information received in Step 7 and existing policy data of Wi-Fi session, SMF prepares the information.
9	If SMF receives new PCC rules in Step 7, the SMF sends the Charging Update request to CHF with new rating-group for quota information. This request includes the PDU session information with the new access params.
10	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes quota information for the rating-groups received in Step 9 and for the existing rating-group of Wi-Fi session.
11	SMF processes the data that is received Charging Update response from CHF.
12	SMF sends the N4 session modification request to UPF for gnb tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, update on URR for modified quota information, and creation of FAR.
13	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
14	SMF sends the EBI assignment request to AMF. This request includes the ARP list for the PDU session ID.
15	AMF sends the list of EBIs as response to SMF.
16	SMF sends the N1 N2 Transfer Request toward AMF. This request includes the N2 message as “PDU Session Resource Setup Request Transfer” with supported QFI list and UL Tunnel Information of gnb Tunnel. This request also includes the N1 message as “PDU Session Establishment Accept” with authorized QoS rule, authorized QoS flow description, EPCO, PDN addresses, and session AMBR values.
17	AMF sends the N1 N2 Transfer acknowledgement to SMF.
18	AMF sends the SM Context Update request to SMF with “PDU Session Resource Setup Response Transfer” containing the failed QFI list and the DL tunnel information.
19	SMF sends the N4 session modification request to UPF for the gnb tunnel resources. This request is to create the DL PDR, to create DL FAR with DL tunnel information, include details on RAT-change and delete resources for Wi-Fi tunnel. SMF also deletes the N4 resources of gnb tunnel for received failed QFI list.
20	UPF sends the N4 Session Modification Response with the usage report to SMF.
21	SMF sends the SM Context Update response to AMF.
22	SMF sends the Charging Update request to PCF. This request includes the PDU session information with new access params and multi-usage report with old access-params and usage report that is received in Step 18. SMF receives the Charging Update response that includes new quota information for existing rating-groups.
23	SMF+PGW-C initiates the GTPv2 DB request, which includes EBIs, to ePDG.

Step	Description
24	ePDG sends the GTPv2 DB response to SMF+PGW-C.
25	SMF receives the SM Context Update request with N1 message for PDU session modification completion from AMF.
26	SMF sends 200/204 OK as SM Context Update response to AMF.
27	SMF sends the SM policy decision as SM Policy Control Update response to AMF.
28	SMF sends the SM Policy Control Update request to PCF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of N2 message.
29	PCF sends the SM policy decision as SM Policy Control Update response to SMF.
30	SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the 5GS to non-3GPP untrusted Wi-Fi handover call flow.

Figure 6: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

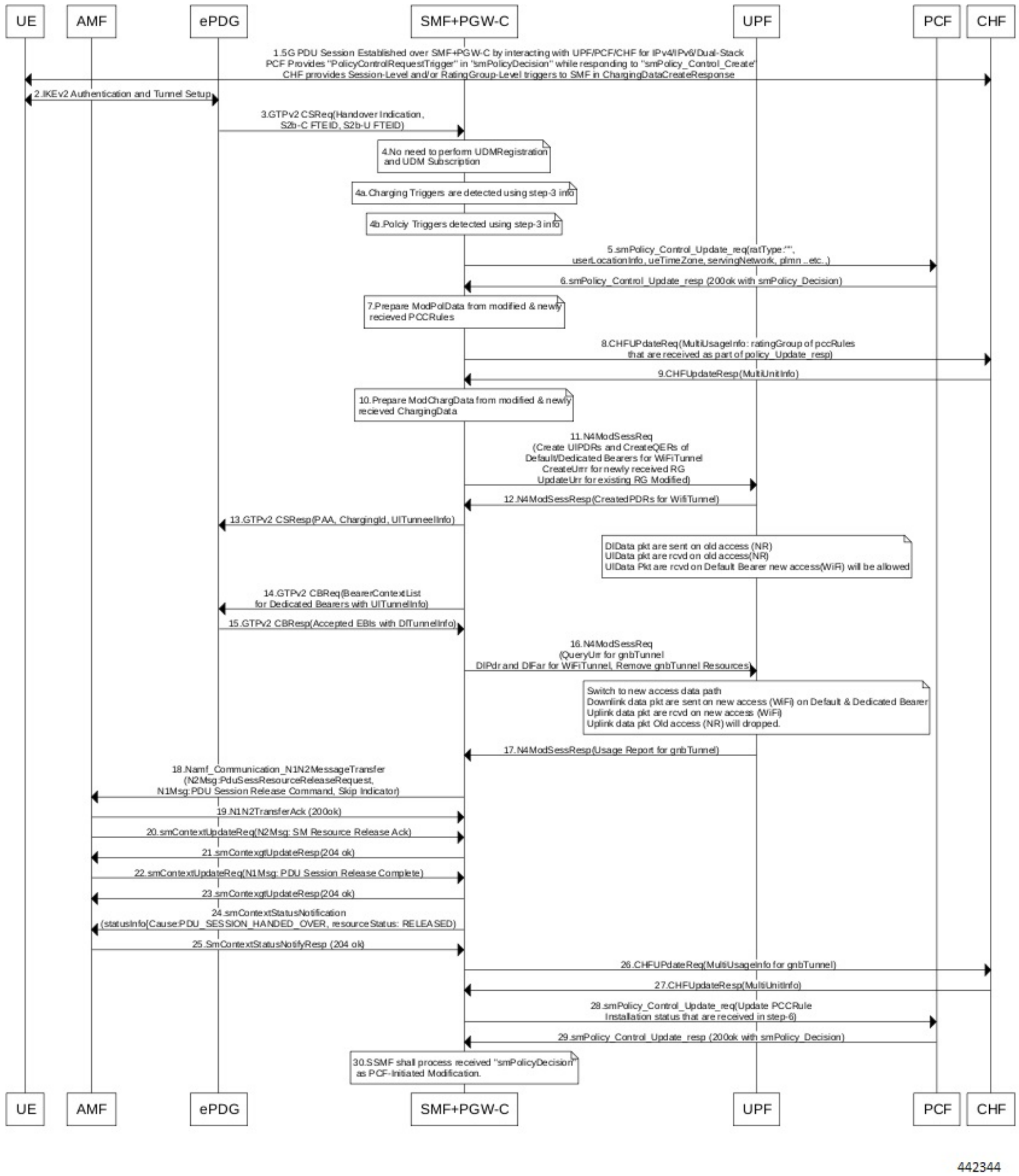

UE
AMF
ePDG
SMF+PGW-C
UPF
PCF
CHF
1.5G PDU Session Established over SMF+PGW-C by interacting with UPF/PCF/CHF for IPv4/IPv6/Dual-Stack
PCF Provides "PolicyControlRequestTrigger" in "smPolicyDecision" while responding to "smPolicy_Control_Create"
CHF provides Session-Level and/or RatingGroup-Level triggers to SMF in ChargingDataCreateResponse
2.IKEv2 Authentication and Tunnel Setup
3.GTPv2 CSReq(Handover Indication,
S2b-C FTEID, S2b-U FTEID)
4.No need to perform UDMRegistration
and UDM Subscription
4a.Charging Triggers are detected using step-3 info
4b.Policiy Triggers detected using step-3 info
5.smPolicy_Control_Update_req(ratType:"",
userLocationInfo, ueTimeZone, servingNetwork, plmn ..etc..)
6.smPolicy_Control_Update_resp (200ok with smPolicy_Decision)
7.Prepare ModPolData from modified & newly
recieved PCCRules
8.CHFUPdateReq(MultiUsageInfo: ratingGroup of pccRules
that are received as part of policy_Update_resp)
9.CHFUpdateResp(MultiUnitInfo)
10.Prepare ModChargData from modified & newly
recieved ChargingData
11.N4ModSessReq
(Create UlPDRs and CreateQERs of
Default/Dedicated Bearers for WiFiTunnel
CreateUrr for newly received RG
UpdateUrr for existing RG Modified)
12.N4ModSessResp(CreatedPDRs for WifiTunnel)
13.GTPv2 CSResp(PAA, ChargingId, UlTunneelInfo)
DlData pkt are sent on old access (NR)
UlData pkt are rcvd on old access(NR)
UlData Pkt are rcvd on Default Bearer new access(WiFi) will be allowed
14.GTPv2 CBReq(BearerContextList
for Dedicated Bearers with UlTunnelInfo)
15.GTPv2 CBResp(Accepted EBIs with DlTunnelInfo)
16.N4ModSessReq
(QueryUrr for gnbTunnel
DlPdr and DlFar for WiFiTunnel, Remove gnbTunnel Resources)
Switch to new access data path
Downlink data pkt are sent on new access (WiFi) on Default & Dedicated Bearer
Uplink data pkt are rcvd on new access (WiFi)
Uplink data pkt Old access (NR) will dropped.
17.N4ModSessResp(Usage Report for gnbTunnel)
18.Namf_Communication_N1N2MessageTransfer
(N2Msg:PduSessResourceReleaseRequest,
N1Msg:PDU Session Release Command, Skip Indicator)
19.N1N2TransferAck (200ok)
20.smContextUpdateReq(N2Msg: SM Resource Release Ack)
21.smContexgtUpdateResp(204 ok)
22.smContextUpdateReq(N1Msg: PDU Session Release Complete)
23.smContexgtUpdateResp(204 ok)
24.smContextStatusNotification
(statusInfo[Cause:PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED)
25.SmContextStatusNotifyResp (204 ok)
26.CHFUPdateReq(MultiUsageInfo for gnbTunnel)
27.CHFUpdateResp(MultiUnitInfo)
28.smPolicy_Control_Update_req(Update PCCRule
Installation status that are received in step-6)
29.smPolicy_Control_Update_resp (200ok with smPolicy_Decision)
30.SSMF shall process received "smPolicyDecision"
as PCF-Initiated Modification.
UE
AMF
ePDG
SMF+PGW-C
UPF
PCF
CHF
442344

Table 6: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE and the SMF or the UPF interact through the NG-RAN to establish one or more PDU sessions.

Step	Description
2	The UE connects to an untrusted non-3GPP access and selects an ePDG. Then, the UE initiates the handover attach procedure, as defined in *3GPP TS 23.402, section 8.6.2.1*. After establishing the IKE tunnel between the UE and the ePDG, and authenticating the UE over SWm interface with the AAA server, the UE initiates IKE_AUH. The IKE_AUH includes cfg_params of the earlier assigned IPv4 or IPv6 addresses in 5GS and P-CSCF and DNS options.
3	The ePDG sends a Create Session request to the P-GW. This request includes the following details: • IMSI • APN • handover indication • RAT type • ePDG TEID of the control plane • ePDG address for the user plane • ePDG TEID of the user plane • EPS bearer identity • user location The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and includes it in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session request. This configuration allows the P-GW to reallocate the same IP address or the prefix assigned to the UE. The IP address or prefix assignment occurs while the UE is connected to the 3GPP IP access. The policy modification procedure begins with the PCF.
4	The SMF does not perform the UDM registration as it has already been registered with UDM during the 5GS session establishment.
4a	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during the Wi-Fi session.
4b	The SMF detects the policy triggers with the information available in Step 3 against the requested policy control triggers that are received while communicating with PCF during the Wi-Fi session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters to the PCF.
6	The PCF sends the SM policy decision in the SM Policy Control Update response by including new or updated PCC rules.
7	Based on the information received in Step 6 and the existing policy data of 5GS session, the SMF prepares the “ModPolData” information.

Step	Description
8	If the SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request to the CHF with new rating-group for quota information. This request includes the PDU session information with the new access parameters.
9	The CHF sends the multi-unit information as Charging Update response to the SMF. The multi-unit information includes quota information for the rating-groups received in Step 8 and for the existing rating-group of 5GS session.
10	The SMF processes the ModChargingData in the Charging Update response received from the CHF.
11	The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnels. This request includes details on creation of uplink FAR, creation of QER, creation of URR for the received new rating-group quota information, and update on URR for the modified quota information.
12	The UPF sends the N4 session modification response to the SMF with the UL tunnel information in the created PDR.
13	The SMF sends the GTPv2 Create Session response to the S-GW. The response includes details on accepted request or partially accepted request, P-GW S2b F-TEID, PAA, APN-AMBR, creation of bearer context, charging gateway address, and APCO.
14	The SMF sends the GTPv2 Create Bearer request to the S-GW. This request includes information on bearer context list, which contains UL tunnel information for each dedicated bearer to end-user.
15	The S-GW sends the GTPv2 Create Bearer response to the SMF. The response includes details on accepted request or partially accepted request and bearer contexts.
16	The SMF processes the Create Bearer response and derives the DL tunnel information for the established bearer and the failed EBI list, if any. The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnel. This request is to create DL PDR and DL FAR with the DL tunnel information or list of charging description IDs for the detected charging triggers. The SMF deletes the gnb tunnel resources and the N4 resources of the Wi-Fi tunnel for the failed bearer context list.
17	The UPF sends the usage report in the N4 Session Modification response to the SMF.
18	The SMF initiates the NAMF communication N1 N2 message transfer, to the S-GW. This transfer message includes the PDU Session Resource Release Request N2 message.
19	The AMF sends N1 N2 Transfer Acknowledgement to the SMF.
20	The AMF sends the SM Context Update request to the SMF. This request includes the SM Resource Release Acknowledgement N2 message.
21	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
22	The AMF sends the SM Context Update request to the SMF. This request includes the PDU Session Release Complete N1 message.
23	The SMF sends the 200/204 OK as SM Context Update response to the AMF.

Step	Description
24	If the SMF supports the June 2019 compliance version of 3GPP specification 23.502, the SMF indicates the release details to the AMF. The SMF achieves this functionality by sending the SM Context Status Notification message (statusInfo {Cause: PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED). The SMF sends this notification after a successful handover of 5GS to Non-3GPP Untrusted WiFi session. The SMF processes the message as per the compliance profile configured for the corresponding service. For information on the compliance profile configuration, see the Configuring Compliance Profile, on page 21 section. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
25	The AMF sends the 204 OK as SM Context Status Notify response to the SMF. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
26	The SMF sends the Charging Update request to the CHF. This request includes the PDU session information with the new access parameters and multi-usage report containing details on the old access parameters and the usage report that is received in Step 17.
27	The CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the existing rating-groups.
28	The SMF sends the SM Policy Control Update to PCF. This update includes the new access parameters and rule report for failed QFI list that are received from the AMF as part of Create Bearer response.
29	The PCF sends the SM policy decision through the SM Policy Control Update response to the SMF.
30	The SMF processes the SM policy decision and handles it as PCF-initiated modification procedure as defined in *3GPP TS 23.502, section 4.3.3.2*.

Non 3GPP Untrusted LTE to WiFi Handover

This section describes the non-3GPP untrusted LTE to WiFi handover call flow.

Figure 7: Non-3GPP Untrusted LTE to WiFi Handover with TFTs more than 4 for a Dedicated Bearer

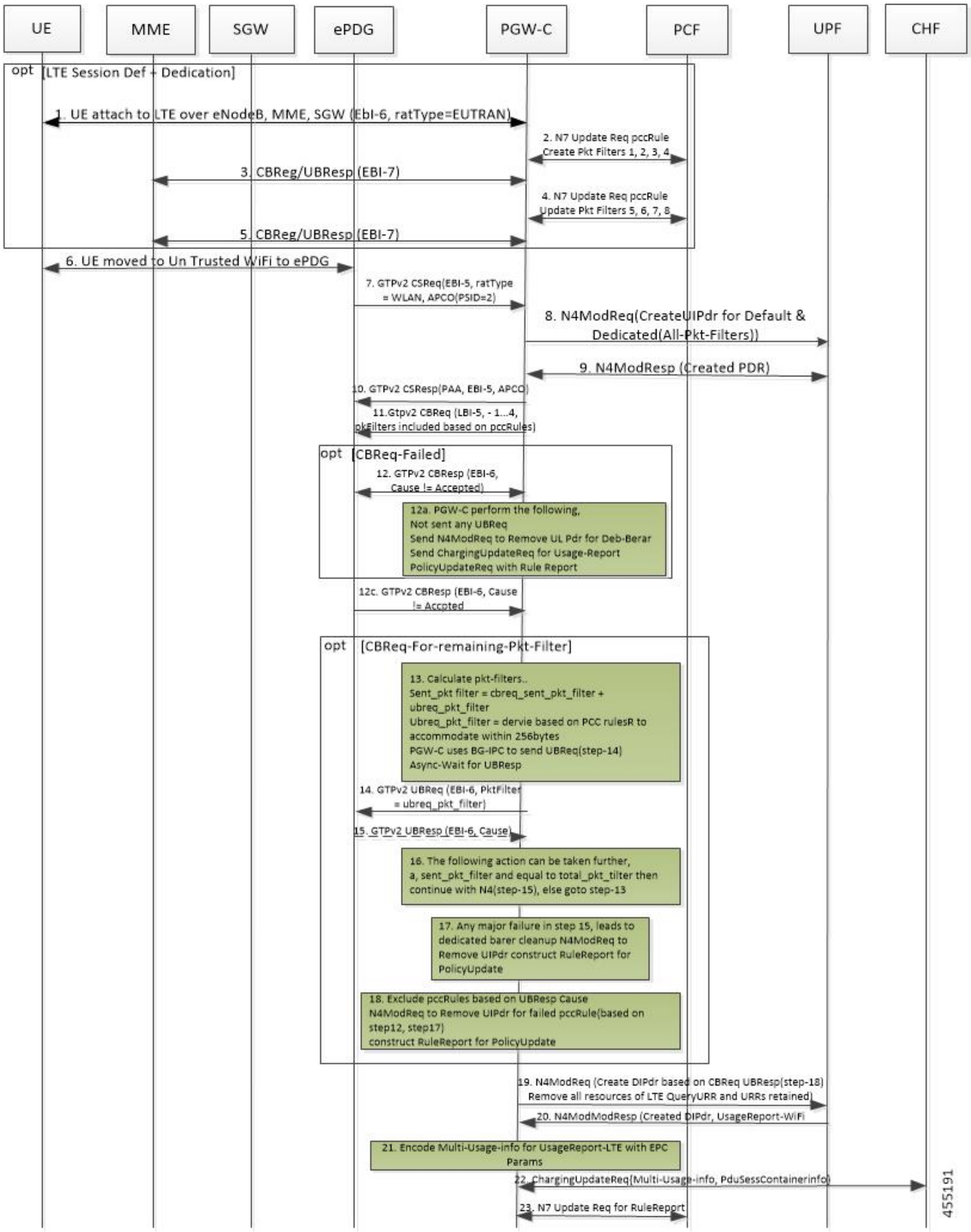

UE
MME
SGW
ePDG
PGW-C
PCF
UPF
CHF
opt [LTE Session Def + Dedication]
1. UE attach to LTE over eNodeB, MME, SGW (EbI-6, ratType=EUTRAN)
2. N7 Update Req pccRule Create Pkt Filters 1, 2, 3, 4
3. CBReg/UBResp (EBI-7)
4. N7 Update Req pccRule Update Pkt Filters 5, 6, 7, 8
5. CBReg/UBResp (EBI-7)
6. UE moved to Un Trusted WiFi to ePDG
7. GTPv2 CSReq(EBI-5, ratType = WLAN, APCO(PSID=2)
8. N4ModReq(CreateUIPdr for Default & Dedicated(All-Pkt-Filters))
9. N4ModResp (Created PDR)
10. GTPv2 CSResp(PAA, EBI-5, APCO)
11.Gtpv2 CBReq (LBI-5, - 1...4, pkFilters included based on pccRules)
opt [CBReq-Failed]
12. GTPv2 CBResp (EBI-6, Cause != Accepted)
12a. PGW-C perform the following,
Not sent any UBReq
Send N4ModReq to Remove UL Pdr for Deb-Berar
Send ChargingUpdateReq for Usage-Report
PolicyUpdateReq with Rule Report
12c. GTPv2 CBResp (EBI-6, Cause != Accpted
opt [CBReq-For-remaining-Pkt-Filter]
13. Calculate pkt-filters..
Sent_pkt filter = cbreq_sent_pkt_filter + ubreq_pkt_filter
Ubreq_pkt_filter = dervie based on PCC rulesR to accommodate within 256bytes
PGW-C uses BG-IPC to send UBReq(step-14)
Async-Wait for UBResp
14. GTPv2 UBReq (EBI-6, PktFilter = ubreq_pkt_filter)
15. GTPv2 UBResp (EBI-6, Cause)
16. The following action can be taken further,
a, sent_pkt_filter and equal to total_pkt_tilter then continue with N4(step-15), else goto step-13
17. Any major failure in step 15, leads to dedicated barer cleanup N4ModReq to Remove UIPdr construct RuleReport for PolicyUpdate
18. Exclude pccRules based on UBResp Cause
N4ModReq to Remove UIPdr for failed pccRule(based on step12, step17)
construct RuleReport for PolicyUpdate
19. N4ModReq (Create DIPdr based on CBReq UBResp(step-18) Remove all resources of LTE QueryURR and URRs retained)
20. N4ModModResp (Created DIPdr, UsageReport-WiFi
21. Encode Multi-Usage-info for UsageReport-LTE with EPC Params
22. ChargingUpdateReq(Multi-Usage-info, PduSessContainerinfo)
23. N7 Update Req for RuleReport
455191

Table 7: Non-3GPP Untrusted LTE to WiFi Handover Call Flow Description

Step	Description
1	Session established in LTE with a default bearer and dedicate bearer with 8 TFTs.
2	LTE->Wifi Handover triggered, when CSReq is received with hi flag set from ePDG.

Step	Description
3	After successfully handling CSReq, CSResp is sent back to ePDG, indicating default bearer successfully handed over.
4	For the dedicated bearer which has 8 TFT, since all TFTs cannot be sent in CBReq, CBReq message is triggered with only 4 TFTs toward ePDG.
5	After successful CBResponse from ePDG, SMF shall send remaining TFTs in the UBReq message.
6	After successful UBResponse from ePDG, SMF continues with completion of establishing the bearer towards UPF.
7	At step 5. or step 6., if there is failure in CBResponse or failure in UBResponse, SMF deletes that bearer and if armed, sends rule report to PCF mentioning the corresponding rules as Inactive.

Important Steps 4-7 are applicable for LTE → WiFi and NR → WiFi if a dedicate bearer has more than 4 TFTs.

Configuring the WiFi Handovers Feature

This section describes the configurations related to the Wi-Fi Handovers feature.

Configuring Compliance Profile

The SMF provides the compliance profile support for the 3GPP specification 23.502 through the CLI configuration. This compliance profile is in use during the 5GS to non-3GPP untrusted WiFi handover procedure.

Use the following configuration to configure the SMF in compliance with the 3GPP specification.

```
configure
   profile compliance profile_name
      service threegpp23502 version spec spec_version full version_format
      uri_version uri_version
         range
         !
         !
```

NOTES:

- **full**: Specifies the full version in the format — <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]
- **spec**: Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.4.0
  - 15.6.0

To support 3GPP December 2018 specification compliance, configure the specification version as 15.4.0. The default version is 15.4.0.

To support 3GPP June 2019 specification compliance, configure the specification version as 15.6.0.

- **uri**: Specifies the URI version in the format — "v" concatenated with a number. It can be both v1 and v2, or either v1 or v2.