ERICSSON

LTE Mobility Management

Technical Product Description

44/221 02-AXB 250 05/8 Uen YD

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Contents

1 LTE Mobility Management Overview

EPS mobility management for LTE access tracks the UE in the LTE RAN and enables the UE to register in the network. The radio network for LTE has a dynamic cellular structure. For an overview of the dynamic cellular structure of LTE, see Figure 1. The network must be aware of the location and the EMM state of the UE to maintain connectivity as the UE can move between cells, tracking areas, service areas, and PLMNs.

Depending on the capacity of the networks, mobility management procedures can be either UE-initiated or RAN-initiated. For more information about mobility management procedures, see SoC with 3GPP TS 23.401.

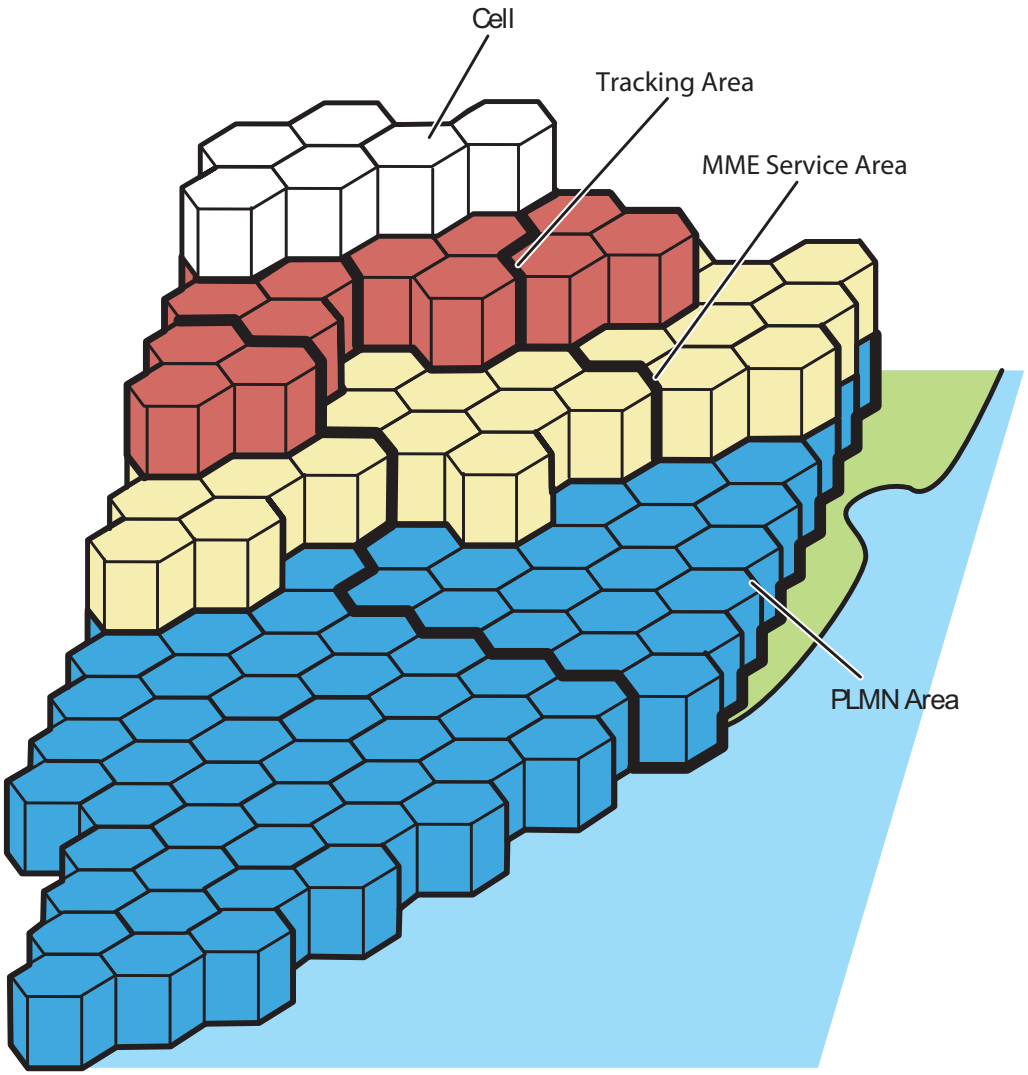


Figure 1 Overview of the LTE Cellular Network Structure

1.1 Mobility and Connection Management States

The EMM states are results of EPS mobility management procedures, for example, Attach and Detach procedures. The mobility management state describes the state of the UE from the perspective of the MME. A UE can have the following EMM states in the MME:

— EMM-REGISTERED

— EMM-DEREGISTERED

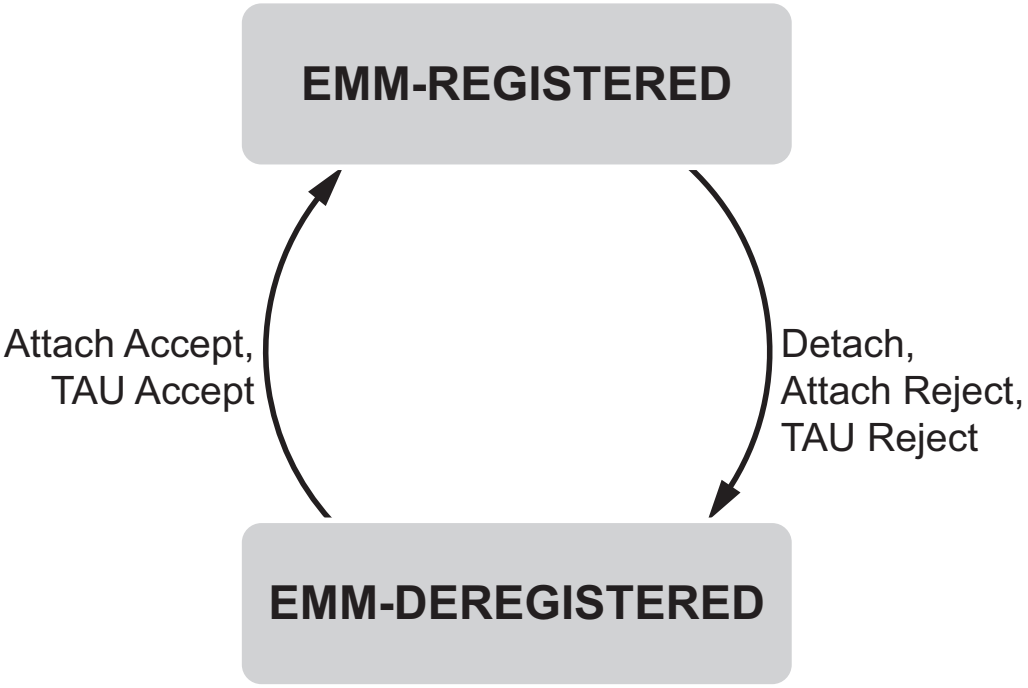


Figure 2 EMM States

The ECM states describe the signaling connectivity between the UE, the MME, and the SGW. A UE can have the following ECM states in the MME:

— ECM-IDLE

— ECM-CONNECTED

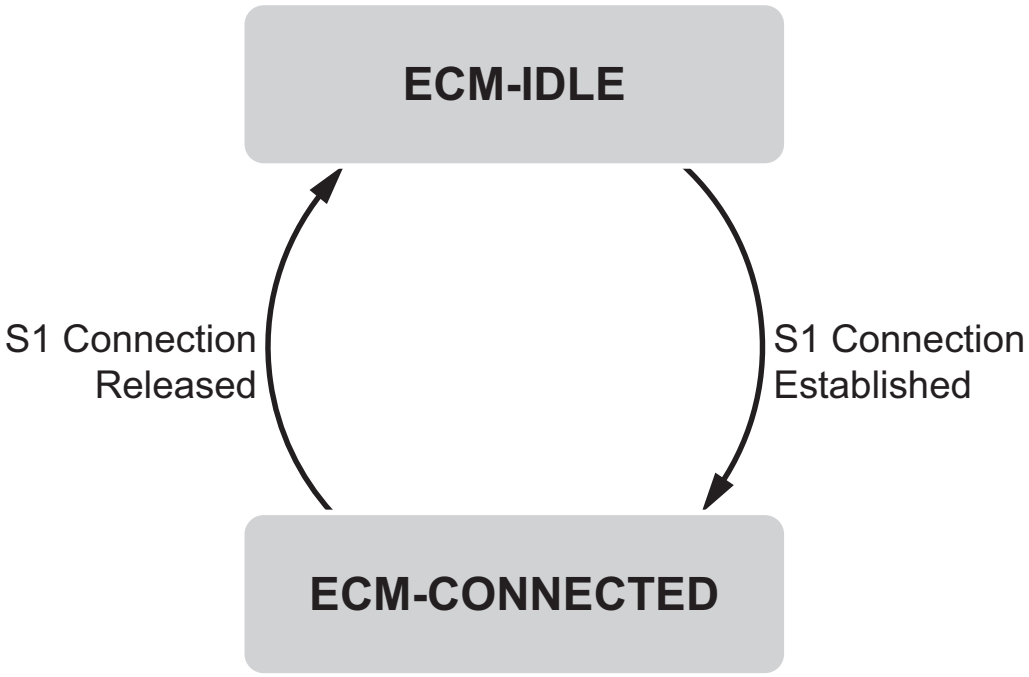


Figure 3 ECM States

The ECM and EMM states are independent of each other. For more information on EMM and ECM states, see SoC with 3GPP TS 23.401.

1.1.1 EMM-REGISTERED

The UE enters the EMM-REGISTERED state after a successful registration procedure, that is, an Attach procedure or a TAU procedure. In the EMM-REGISTERED state, the UE can receive services that require registration in the EPS. The MME knows the current location of the UE through the accuracy of the tracking area list allocated to the UE.

— For a UE that does not support EMM-REGISTERED without PDN Connection, the UE must have one or more PDN connections in the EMM-REGISTERED state. When the last PDN connection is removed, the UE is detached and becomes in the EMM-DEREGISTERED state.

— For a UE that supports EMM-REGISTERED without PDN Connection, the UE can stay in the EMM-REGISTERED state without any PDN connections.

After a successful Detach procedure, the UE EMM state is changed to EMM-DEREGISTERED in the MME.

If the MME rejects the Attach procedure, or if the TAU procedure is rejected, the state of the UE is set to EMM-DEREGISTERED.

If the UE is emergency attached, only IMS Emergency Service is allowed.

1.1.2 EMM-DEREGISTERED

A UE in the EMM-DEREGISTERED state is not attached. The EMM context in the MME holds no valid location information for the UE. The MME cannot reach the UE, as the UE location is not known. No EPS bearer exists for the subscriber. In the EMM-DEREGISTERED state, some UE information can be stored in the UE and MME.

After a successful Attach or TAU procedure, the state is changed to EMM-REGISTERED.

1.1.3 ECM-IDLE

A UE is in the ECM-IDLE state, which is also referred to as idle mode, when no NAS signaling connection between the UE and the network exists. No UE context exists in LTE for a UE in the ECM-IDLE state. Also, no UE-associated logical S1-MME connection exists for a UE in the ECM-IDLE state.

1.1.3.1 Changing State from ECM-IDLE to ECM-CONNECTED

The UE and the MME enter the ECM-CONNECTED state when a signaling connection is established between the UE and the MME.

The following are initial NAS messages trigger a transition from ECM-IDLE to ECM-CONNECTED state:

— `Attach Request`

— `Service Request`

— `TAU Request` with the `active` flag or `signalling active` flag set

— `Control Plane Service Request`

1.1.3.2 Changing State from ECM-CONNECTED to ECM-IDLE

If a UE changes state from ECM-CONNECTED to ECM-IDLE, a configurable mobile reachable timer is triggered. If the UE does not send a `TAU Request` message before the reachable timer expires, an implicit detach timer is triggered and the UE remains in the ECM-IDLE state. The UE is only implicitly detached if the UE does not send a `TAU Request` message before the detach timer expires.

A UE in the ECM-IDLE state with only IMS Emergency Service is implicitly detached once the mobile reachable timer expires. Also, an unauthenticated UE that is emergency attached is removed from the MME.

1.1.4 ECM-CONNECTED

For a UE in the ECM-CONNECTED state, there is a signaling connection between the UE and the MME. The signaling connection consists of two parts, one RRC connection between the UE and the eNodeB, and one UE-associated S1-MME connection between the eNodeB and the MME. The MME knows the UE location through the accuracy of eNodeB. The S1 Release procedure changes the state of both the UE and the MME from ECM-CONNECTED to ECM-IDLE.

2 Attach

The UE announces that it is present in the network by initiating an Attach procedure by signaling to the MME. The initiated Attach procedure can be an EPS Attach procedure or an Emergency Attach procedure. The UE can identify itself by the GUTI, IMSI, or the IMEI that is specific to that UE. On the completion of the Attach procedure, the UE enters the EMM-REGISTERED state.

The UE can also initiate the Attach procedure by sending an `Attach Request` message with a Combined Attach flag and the Attach type 'Combined Attach'. For more information about combined procedures, see EPS Support for CS Services.

As a result of the Attach procedure, an EMM context exists in the MME. For a UE that does not support EMM-REGISTERED without PDN Connection, a default bearer is established between the UE and the PGW, meaning that a PDN connection is created. Dedicated bearers can also be activated during the Attach procedure at the request of the PGW. For more information, see LTE Session Management.

If additional PDN connections are requested, or the first PDN connection is requested for a UE that is attached to the EPS network without PDN Connection, the PDN Connectivity procedure is used after the Attach procedure is completed. For more information about the PDN Connectivity procedure, see LTE Session Management.

For a UE that does not support EMM-REGISTERED without PDN Connection, if the `Attach Request` message includes an `ESM Dummy Message`, neither the Create Session procedure nor the Modify Bearer procedure takes place during the attach.

The Attach procedure is also used when a subscriber moves from a CDMA 2000 network to an LTE network. For more information, see Inter-System Mobility Management.

2.1 Traffic Case

The Attach procedure is shown in Figure 4 .

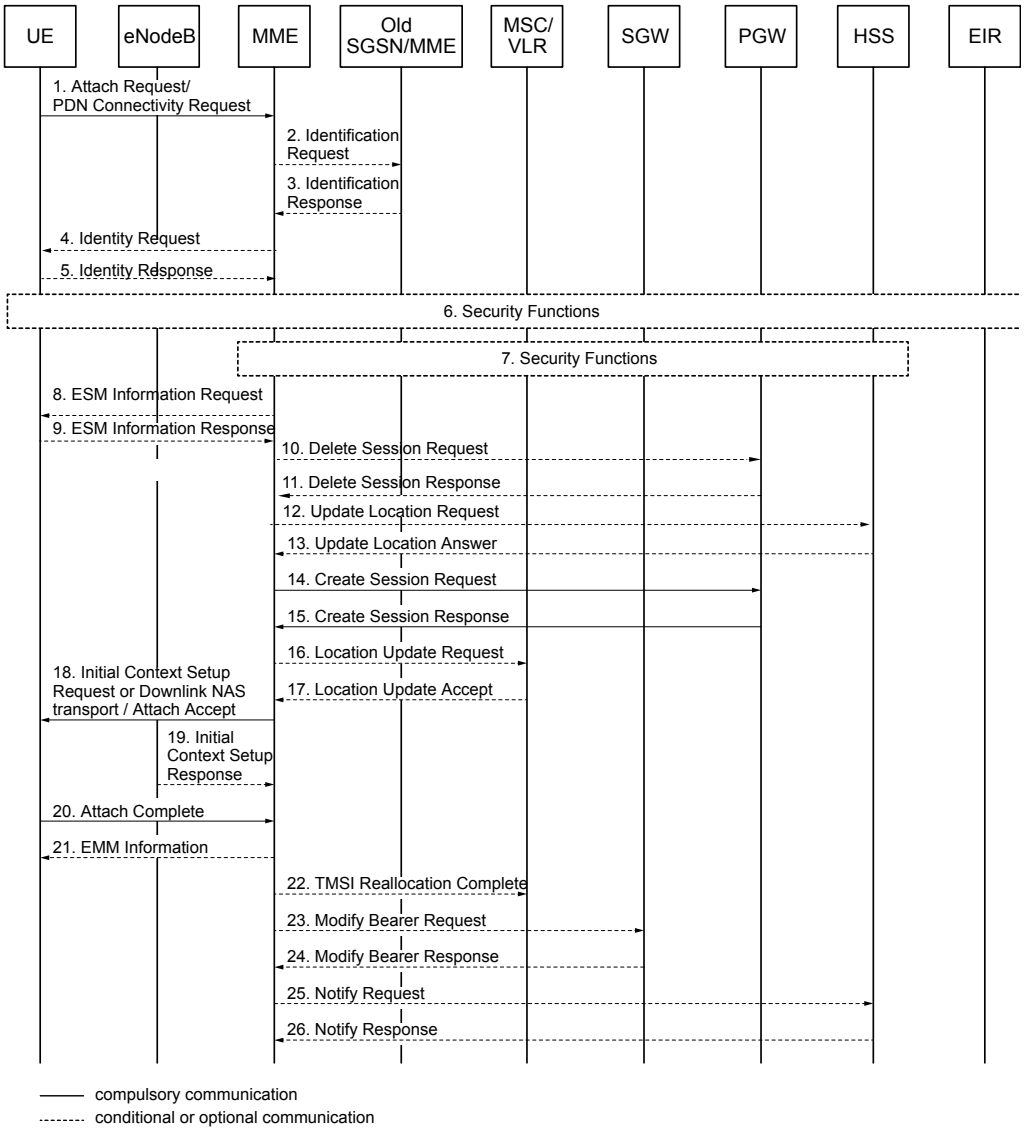


Figure 4 Attach Procedure

The following steps describe the Attach procedure:

1. The UE initiates the Attach procedure by sending an `Attach Request` message, which includes the IMSI, the IMEI, or the GUTI and, if it is available, the last visited registered TAI, through the eNodeB to the MME. For information about the TAI list, see TAI List on page 141.

   If the UE moves from the 5GS, the `Attach Request message` includes a GUTI, mapped from the 5G-GUTI in the `Old GUTI` IE, and includes the `Old GUTI Type` IE set to `Native GUTI`. The UE indicates support of the N1 mode in the `UE Network Capability` IE.

Depending on the UE capacity and the UE behavior, the Attach Request message contains a PDN Connectivity Request or an ESM Dummy Message message.

- For a UE that does not support EMM-REGISTERED without PDN Connection, the Attach Request message contains a PDN Connectivity Request message.
- For a UE that supports EMM-REGISTERED without PDN Connection, the Attach Request message can either contain an ESM Dummy Message, allowing the UE to attach without any PDN connections, or a PDN Connectivity Request message to request a PDN connection.

Attach Request messages that indicate emergency are prioritized in instances of resource limitation.

The MME also checks if access restrictions or roaming restrictions apply. If the UE is restricted, the Attach request is rejected. For more information, see Attach Rejected on page 14. For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123.

The MME checks if APN Restriction applies. If the resolved APN matches the configured APN blacklist for the UE, the Attach procedure is rejected or accepted based on whether the UE supports EMM-REGISTERED without PDN Connection. For more information, see Attach Rejected on page 14.

2. If the UE attaches to a new MME, the MME sends an Identification Request message to the old SGSN, MME or AMF to request the IMSI. The new MME derives the IP address of the old SGSN or MME either through static selection or a DNS query, depending on the configuration. In that case, the UE identifies itself with the old GUTI. For detailed information about the static SGSN or MME selection in MME, see Static and DNS-based SGSN or MME Selection on page 116.

   The AMF derives the IP address of the MME through a DNS query. In that case, the UE identifies itself with an old GUTI. For information about how to select an AMF, see DNS Description.

3. The old SGSN or MME responds with an Identification Response message containing the IMSI and the mobility management context. The old SGSN or MME verifies the Attach Request message by the P-TMSI signature or through an integrity check.

   The UE Radio Capability for Paging information can be included in the Identification Response message and transferred from the old MME to the new MME. For more information, see Massive IoT.

   If an Identification Response message is not received after a time specified by the T3ResponseIdentification parameter, the MME retransmits the Identification Request message several times as specified by the

N3RequestIdentification parameter. After the last retransmission, the IMSI number is instead fetched from the UE.

4. If the UE is unknown to both the old SGSN or MME and the new MME, the new MME sends an Identity Request message to the UE to request the IMSI. This also applies when the old SGSN or MME is not reachable or responds with a failure message.

5. The UE responds with an Identity Response message containing the IMSI. The MME analyzes the IMSI of the UE to verify that the IMSI is part of an IMSI number series that is defined in the MME.

6. Security functions can be performed, for example, to authenticate a subscriber. A security context is established, and ciphering and integrity protection are negotiated. The IMEI Check procedure can also be performed. When an unauthenticated UE requests an Emergency Attach, security functions are handled differently. For more information, see Security. Also, if the GUTI is allocated by the current MME, the IMEI Check for GUTI Attach can be skipped. For more information, see Configuring IMEI Check.

7. If the IMEISV received from the UE during the security functions procedure is different from the previous IMEISV (if available) and there is no Update Location Procedure, the MME initiates a Notification procedure to the HSS with the updated terminal information. For unauthenticated UEs requesting an Emergency Attach, no Notification procedure is triggered toward the HSS.

8. If the Attach Request message contains the PDN connectivity Request message, the UE can set the ESM Information Transfer flag in the PDN Connectivity Request message to either of the following values:

   - If the ESM Information Transfer flag is set to 0, the MME does not send an ESM Information Request message to the UE.

   - If the ESM Information Transfer flag is set to 1, the MME sends an ESM Information Request message to the UE to request the ESM information and gets an ESM Information Response message that includes the APN from the UE. The information is security-protected.

   When security functions are turned off, sending the APN in a PDN Connectivity Request message is not secure. Sending the APN in an ESM Information Response message is secure in this scenario. For an Emergency Attach, the ESM Information Transfer flag is ignored.

9. The UE sends an ESM Information Response message to the MME, containing the ESM information. The ESM information includes PCOs, which need to be transferred with security protection, and the requested APN if necessary.

10. If there are any active bearer contexts for the UE in the new MME, the new MME sends a Delete Session Request message to the PGW. This message contains information on how to delete the active bearer contexts.

11. The PGW acknowledges the request by sending a `Delete Session Response` message to the MME.

12. The MME sends an `Update Location Request` message to the HSS in the following scenarios:

    - The UE provides an IMSI.
    - The TAI supplied by the eNodeB is different from that of the GUTI of the UE.
    - There is no valid subscription data for the UE in the new MME.

    This is to inform the HSS about the identity of the MME currently serving the user and to get subscription data. The message contains the user state and location information if the `-aanh S6aAllowAdditionalNetLocHss` parameter in modify_s6a command is set to true. The message contains the `Emergency Service Continuity` bit in the `Supported-Features` AVP when the licensed feature `IMS-Based Telephony - MMTel` is enabled.

    For an unauthenticated UE requesting an Emergency Attach, no `Update Location Request` message is sent to the HSS.

13. The HSS sends an `Update Location Answer` message to the MME to update the MME subscription data. The MME validates the data and sets up a context for the UE. The MME also checks if CSG restrictions apply. If the UE is restricted, the Attach procedure is rejected. For more information about CSG restrictions, see CSG Restrictions on page 131.

    For IMS Emergency Service, the Attach procedure continues despite a negative response from the HSS.

    If received, the MME stores the following information:

    - If the UE is restricted for NR in the 5GS by the `NR in 5GS Not Allowed` bit in the `Access-Restriction-Data` AVP
    - If the UE is restricted for the 5GS by the `5GC in Core-Network-Restrictions` AVP
    - If the interworking between the 5GS and the EPS is subscribed for the APN in the APN-Configuration by the `Interworking-5GS-Indicator` AVP

14. The Create Session procedure is performed if the `Attach Request` message contains a `PDN Connectivity Request` message.

    - If the `Attach Request` message contains an `ESM Dummy Message`, the session management-related procedures are not performed. For example, APN resolving, SGW selection, PGW selection, creating sessions, setting up bearers toward the UE, and modifying bearers procedures described in the Attach traffic case.

- If the `Attach Request` message contains a `PDN Connectivity Request` message with PDN Type 'non IP' , the MME uses the subscription data to verify that the APN that is requested by the UE is allowed and determines which SCEF to be used to set up the PDN connection. For more information, see Non-IP Data Delivery over SCEF.

- If the `Attach Request` message contains a `PDN Connectivity Request` message, the MME uses the subscription data to verify that the APN that is requested by the UE is allowed and determines which PGW to contact. For more information about APN resolving and PGW selection, see LTE Session Management. For an emergency-attach, the MME emergency configuration data is used to determine the APN. The MME sends the `Create Session Request` message through the SGW to the PGW to start establishing a default EPS bearer.

  If the UE supports the N1 mode and the subscription data indicates that the interworking between the 5GS and the EPS is supported, a combined PGW-C and SMF is selected, and the `5GS Interworking Indication` IE is included in the `Create Session Request` message.

  If the request type indicates `handover of emergency bearer services`, for the non-roaming authenticated UE, either the emergency PGW from the MME emergency configuration data or the emergency PGW from the HSS is used according to the `-ecvh EmergencyContinuityViaHss` parameter in modify_plmn command. For the roaming authenticated UE and the unauthenticated UE, the emergency PGW is used from the MME emergency configuration data.

  For more information about emergency, see Configuring MMTel Service. For more information, see LTE Session Management.

  If the UE uses EPS services with DoNAS, the MME includes an S11-GTP-U F-TEID in the `Create Session Request` message.

  The MME can set the Control Plane Only Connection Indication flag in the `Create Session Request` message according to the MME local configuration policies, the UE-preferred CIoT network behavior and the UE-supported CIoT network behavior. For more information, see Massive IoT.

15. The PGW creates an entry in the EPS bearer context table and generates a Charging ID. After negotiating with the PCRF, the PGW optionally sends a `Create Session Response` message through the SGW to the MME.

    If a `Combined Attach Request` message was sent in and the `PreventCombinedRegistration` parameter is set to false, the MME proceeds with the action in . Otherwise, it proceeds with the action in .

16. The MME sends a `Location Update Request` message to the Mobile services Switching Center/Visitor Location Register (MSC/VLR).

17. The MSC/VLR responds by sending a `Location Update Accept` message to the MME.

18. The MME sends the `Initial Context Setup Request` message to the eNodeB.

    The `Initial Context Setup Request` message contains an `Attach Accept` message, which is forwarded to the UE. This message contains the TEID and the IP address of the SGW for user plane traffic.

    A new GUTI is allocated.

    The `Handover Restriction List` IE and the `Subscriber Profile ID` IE for the RAT and frequency priority are defined by the RFSP value. If an RFSP value exists in the MME, it is also included in the `Initial Context Setup Request` message. If no RFSP value exists, the `Subscriber Profile ID` IE is not included in the message. For the RFSP selection for a home or a roaming subscriber, see section Mobility-Based Policy Selection on page 120.

    The MME does not send an `Initial Context Setup Request` message. Instead, the `Attach Accept` message is included in the `Downlink NAS transport` message in either of the following cases:

    - The UE is using EPS services with DoNAS. No RABs are established when DoNAS is used.

      For more information about DoNAS, see Massive IoT.

    - The UE supports EMM-REGISTERED without PDN Connection, and the `Attach Request` message contains an `ESM Dummy Message`.

    If the `Attach Request` message contains a `PDN Connectivity Request` message, the MME includes the `Activate Default EPS Bearer Request` message in the `Attach Accept` message. For more information, see LTE Session Management.

    If the `Attach Request` message indicates support for N1 mode, the MME sets the `IWK N26` bit to zero to indicate that the MME supports interworking over the N26 interface.

    The MME informs the UE of the supported features, such as IMS Voice Service or IMS Emergency Service by sending the `EPS network feature support` IE in the `Attach Accept` message. Supported features are based on the configuration of the MME.

Note: The MME sets the `IMS VoPS` bit in the `EPS network feature support` IE based on the configuration of the IMS Voice Service. Also, for UEs with at least one non-emergency PDN, the MME also checks the subscribed IMS APN Configuration profile, the subscribed STN-SR, and the SRVCC capability of the UE. This is controlled by configuring the vops_based_on_ims_apn, the vops_based_on_stn_sr, and the vops_based_on_ue_srvcc_capability node functions respectively.

When the vops_based_on_ue_srvcc_capability node function is enabled, for non-SRVCC-capable UEs, the MME also checks the SRVCC white list (based on IMSI range or IMEI range). If a non-SRVCC-capable UE matches the white list and meets all other criteria, the MME allows IMS VoPS for the UE.

For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on configuring IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service, and IMSI Number Series (CLI).

The MME can set the Control Plane Only Indication flag in the `Activate Default EPS Bearer Request` message according to the MME local configuration policies, the UE-preferred CIoT network behavior, and the UE-supported CIoT network behavior. For more information, see Massive IoT.

19. Optionally, the eNodeB sends the `Initial Context Setup Response` message to the MME after the bearers toward the UE are set up. This message contains the TEID and the IP address of the eNodeB for user plane traffic.

20. The UE sends the `Attach Complete` message containing the identity of the bearers through the eNodeB to the MME.

    If a `Combined Attach Request` message was sent in , continue with . Otherwise, continue with .

    In response to the `Activate Default EPS Bearer Request` message, the UE sends an `Activate Default EPS Bearer Accept` message.

21. The MME sends the `EMM INFORMATION` message to the UE through the eNodeB. During an established EMM context, the MME can send none, one, or more `EMM INFORMATION` messages to the UE. If more than one `EMM INFORMATION` message is sent, the messages do not need to have the same content.

22. For a Combined Attach Request, the MME sends a `TMSI Reallocation Complete` message to the MSC/VLR.

23. The MME sends a `Modify Bearer Request` message to the SGW, containing the TEID of the eNodeB and the IP address of the eNodeB.

The MME does not send the Modify Bearer Request message unless it is required by other features in the following cases:

- The UE is using EPS services with DoNAS and an S11-GTP-U F-TEID is included in the Create Session Request message.
- The UE initiates the Attach procedure including an ESM Dummy Message in the Attach Request message.

24. The SGW acknowledges the request by sending the Modify Bearer Response message, which contains the identity of the bearers, to the MME.
25. Based on the configuration, the MME can send a Notify Request message to the HSS.

    For the non-roaming authenticated UE, if the Emergency Service Continuitybit is set in the Supported-Features AVP of the Update Location Answer message, if needed, the MME sends a Notify Request message to the HSS to update the emergency PGW information in use for emergency services.

    For more information about the Notification procedure, see Subscriber Data Management.
26. The HSS sends the Notify Response message back to the MME.

2.2 Attach Rejected

If the Attach procedure is rejected, either an Attach Reject message is sent to the UE, which includes the reason for the rejection, or the Attach procedure is ended without notifying the UE.

The Attach procedure is ended without notifying the UE, for example, in cases when no S1-AP Initial Context Setup Response message is received during the Attach procedure. An Attach Reject message is sent, for example, if the MME detects a protocol error in the Attach Request message.

If the Attach procedure is rejected based on roaming restrictions, an operator-configured cause code is sent to the UE. For more information, see Roaming Restrictions on page 123.

If the Attach procedure is rejected based on access restrictions, an operator-configured cause code is sent to the UE. For more information, see Access Restrictions on page 126.

If the Attach procedure is rejected based on CSG restrictions, a cause code is sent to the UE. For more information, see CSG Restrictions on page 131.

If the Attach procedure is rejected based on the ODB information in the subscription data, a cause code is sent to the UE. For more information, see Subscription-Based Restrictions on page 127.

If the Attach procedure is rejected based on Diameter S6a errors received from the HSS, a configurable NAS cause code that corresponds with the Diameter S6a error code is sent to the UE. For the mapping of Diameter S6a error codes to NAS cause codes, see Diameter S6a Error Code to NAS Cause Code Mapping on page 147.

If the Attach procedure is rejected because of APN Restriction, a cause code is sent to the UE. For more information, see APN Resolve and Redirect for LTE Access.

All `Attach Reject` messages caused by network failure are logged in the Mobility Event Log. For more information, see Mobility Event Log.

If an `Attach Complete` message is not received from the UE after the time specified by the Attach Complete timer, the MME retransmits the `Attach Accept` message. After four retransmissions, with no `Attach Complete` message from the UE, the Attach procedure is ended and the UE is implicitly detached.

The MME can be configured to throttle `Attach Request` messages.

2.3 Selective EPL

A selective EPL can be configured to steer the UE into selecting a preferred equivalent PLMN from a group of networks at cell selection or relocation. If a selective EPL exists, the MME sends the UE a selective EPL in the `Attach Accept` and `TAU Accept` messages. A selective EPL contains a configurable number of equivalent PLMN IDs. Several unique EPLs can be set up in the MME. For each subscriber, one of the EPLs is selected by the MME, based on the IMSI number of the subscriber and the current tracking area within a geographical area. A geographical area consists of a predefined range of tracking areas. For information on how to configure a selective EPL, see Configuring a Selective Equivalent PLMN List for LTE Access.

3 Detach

The UE can be detached explicitly or implicitly.

— During an explicit detach, the network or the UE explicitly requests the detach.

— During an implicit detach, the UE is detached by the network without being notified. This can occur when the network assumes that communication with the UE is unavailable, for example, because of radio conditions.

On completion of the Detach procedure, the UE is in the EMM-DEREGISTERED state. If the UE is emergency attached and unauthenticated, the UE is removed from the MME.

All PDN connections are deactivated when the UE detaches from the network. If the UE or MME requests the disconnection of specific PDN connections, the PDN Disconnection procedure is performed. The Detach procedure is used when deactivating the last PDN connection for a UE not supporting EMM-REGISTERED without PDN Connection.

For more information about the PDN Disconnection procedure, see LTE Session Management.

3.1 UE-Initiated Detach

The UE-Initiated Detach procedure is used by the UE to inform the network that the UE no longer requires access to the EPS, that is, to detach explicitly from the EPS. This procedure is started, for example, by the UE if the UE is switched off or if the USIM card is removed from the UE. If the UE is emergency attached, the UE can regain normal services by detaching and reattaching.

3.1.1 Traffic Case

The UE-Initiated Detach procedure without NR Usage Data Reporting is shown in Figure 5, and is described below the figure.

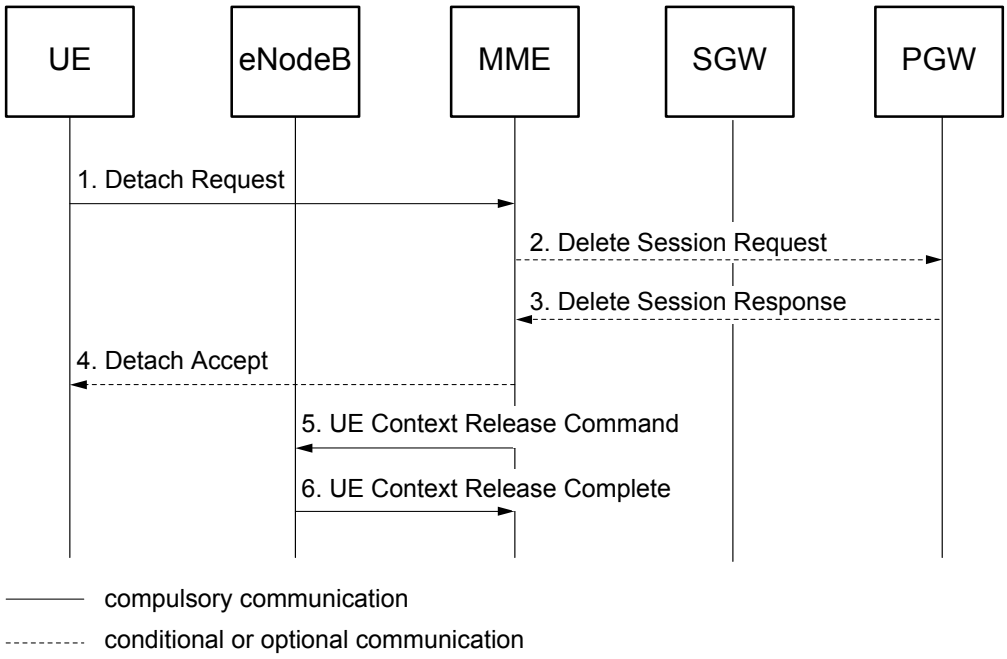


Figure 5 UE-Initiated Detach Procedure

The following steps describe the UE-Initiated Detach procedure:

1. The UE sends the `Detach Request` message, which includes a Switch Off indicator, to the MME. The Switch Off indicator shows if Detach is caused by a switch off situation.

2. If the UE has PDN connections toward the SGW or the PGW, the MME sends a `Delete Session Request` message to deactivate the PDN connection in the SGW and the PGW associated with the UE. One `Delete Session Request` message is sent through the SGW to the PGW for each PDN connection.

   If the UE has PDN connections towards the SCEF, the MME sends a `Connection Management Request` message to deactivate the PDN connection in the SCEF associated with the UE. One `Connection Management Request` message is sent to the SCEF for each PDN connection. For more information, see Non-IP Data Delivery over SCEF.

3. The PGW acknowledges the request by sending the `Delete Session Response` message through the SGW to the MME.

4. If Detach is not caused by a switch off situation, the MME sends a `Detach Accept` message to the UE.

5. The MME releases the connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach.

6. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME.

3.1.2 Traffic Case with NR Usage Data Reporting

The UE-Initiated Detach procedure with NR Usage Data Reporting is shown in Figure 6, and is described below the figure.

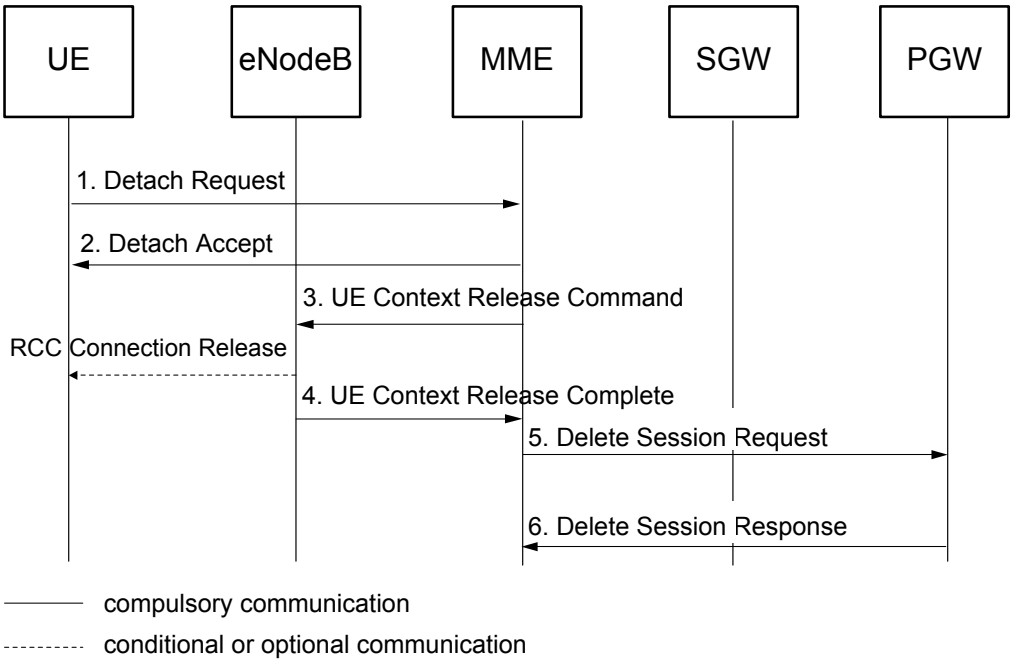


Figure 6 UE-Initiated Detach Procedure with NR Usage Data Reporting

If the NR Usage Data Reporting feature is activated, and the UE is NR capable and not restricted from using NR, the following steps describe the UE-Initiated Detach procedure:

1. The UE sends the `Detach Request` message, which includes a Switch Off indicator, to the MME. The Switch Off indicator shows if Detach is caused by a switch off situation.

2. If Detach is not caused by a switch off situation, the MME sends a `Detach Accept` message to the UE and releases S1.

3. The MME releases the connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach.

4. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME. The `Secondary RAT Usage Report List` IE can be included if data is received.

5. The MME sends a `Delete Session Request` message to deactivate the PDN connection in the SGW and PGW associated with the UE. One `Delete`

`Session Request` message is sent through the SGW to the PGW. for each PDN connection.

The `Secondary RAT Usage Data Report` IE can be included in the `Delete Session Request` message if it was received in step 4. The `IRSGW` and the `IRPGW` bits indicate if the usage data is to be reported to the SGW, the PGW or both.

6. The PGW acknowledges the request by sending a `Delete Session Response` message through the SGW to the MME for each PDN connection.

3.2 HSS-Initiated Detach

The HSS uses the HSS-Initiated Detach procedure for operator-determined purposes to request the deletion of an EMM context of a subscriber in the MME. The HSS-Initiated Detach procedure, also called the Cancel Location procedure, is further described in Subscriber Data Management.

3.2.1 Traffic Case

The HSS-Initiated Detach procedure without NR Usage Data Reporting is shown in Figure 7, and is described below the figure.

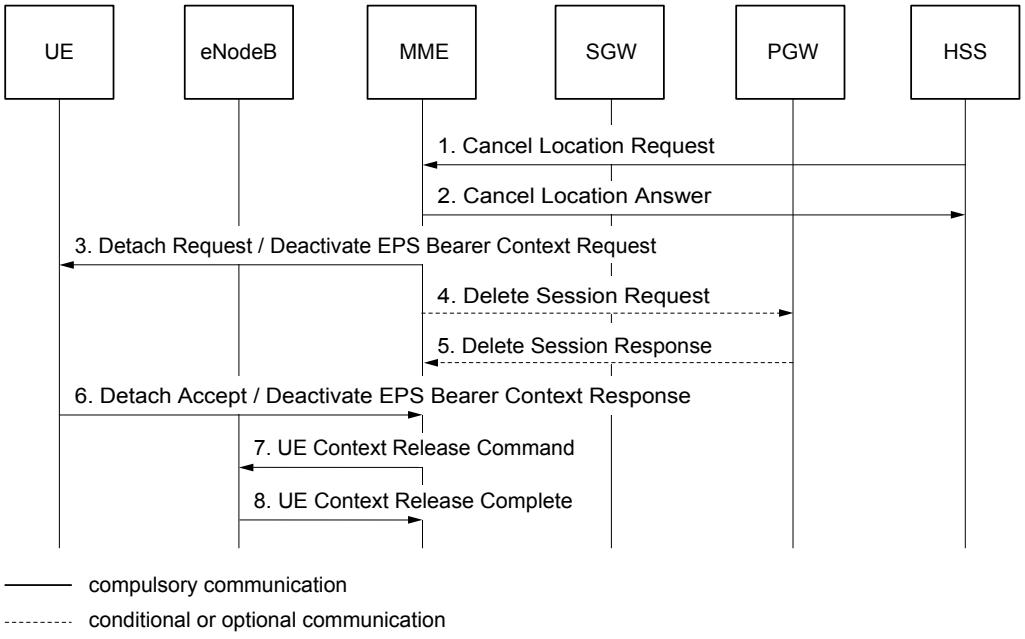


Figure 7 HSS-Initiated Detach Procedure

The following steps describe the HSS-Initiated Detach procedure:

1. The HSS-Initiated Detach procedure is initiated by the HSS sending a `Cancel Location Request` message with the Cancellation Type `Subscription Withdrawal` to the MME. This is performed to request the immediate deletion of an EMM context of a subscriber.

2. The MME responds by sending a `Cancel Location Answer` message to the HSS.

3. The MME informs the UE that the UE is being detached by sending a `Detach Request` message. The `Detach Request` message includes the `Detach Type` IE and the optional `EMM Cause` IE. If the received `Cancel Location Request` message includes the `CLR-Flags` IE and the `Reattach-Required` bit in the `CLR-Flags` IE is set, the `Detach Type` IE is set to **`re-attach required`** and the `EMM Cause` IE is not included. Otherwise, the `Detach Type` IE is set to **`re-attach not required`** and the `EMM Cause` IE is set according to the value of the `CcDetReqBySubWithdrawal` parameter.

   For a UE with IMS Emergency Service, the MME sends a `Deactivate EPS Bearer Context Request` message to the UE, removing all non-emergency PDN connections. The UE then becomes emergency attached. If the UE was already emergency attached, no action is taken.

4. If the UE has PDN connections toward the SGW and the PGW, the MME sends a `Delete Session Request` message to deactivate the PDN connections in the SGW and the PGW associated with the UE. One `Delete Session Request` message is sent through the SGW to the PGW for each PDN connection.

   If the UE has PDN connections toward the SCEF, the MME sends a `Connection Management Request` message to deactivate the PDN connections in the SCEF associated with the UE. One `Connection Management Request` message is sent to the SCEF for each PDN connection. For more information, see Non-IP Data Delivery over SCEF.

5. The PGW acknowledges the request by sending the `Delete Session Response` message through the SGW to the MME.

6. The UE sends a `Detach Accept` or `Deactivate EPS Bearer Context Response` message to the MME.

7. The MME releases the connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach.

8. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME.

3.2.2 Traffic Case with NR Usage Data Reporting

The HSS-Initiated Detach procedure with NR Usage Data Reporting is shown in Figure 8, and is described below the figure.

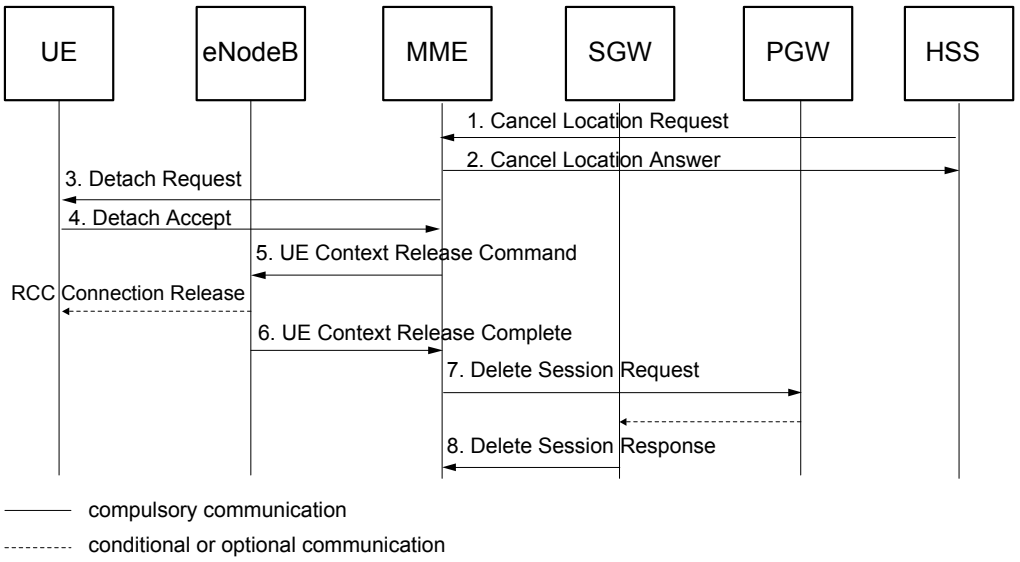


Figure 8 HSS-Initiated Detach Procedure with NR Usage Data Reporting.

If the NR Usage Data Reporting Feature is activated, and the UE is NR-capable and not restricted from using NR, the following steps describe the HSS-Initiated Detach procedure:

1. The HSS-Initiated Detach procedure is initiated by the HSS sending a `Cancel Location Request` message with the Cancellation Type `Subscription Withdrawal` to the MME. This is performed to request the immediate deletion of an EMM context of a subscriber.

2. The MME responds by sending a `Cancel Location Answer` message to the HSS.

3. The MME sends the `Detach Request` message including a Switch Off indicator to the UE.

4. If Detach is not caused by a switch off situation, the UE sends a `Detach Accept` message to the MME and releases the S1 connection.

5. The MME releases the connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach.

6. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME. The `Secondary RAT Usage Report List` IE is included if data is received.

7. The MME sends a `Delete Session Request` message to deactivate the PDN connections in the SGW and the PGW associated with the UE. One `Delete Session Request` message is sent through the SGW to the PGW for each PDN connection.

The Secondary RAT Usage Data Report IE can be included if it was received in step 6. The IRSGW and IRPGW bits indicate if the usage data is to be reported to the SGW, the PGW, or both.

8. The PGW acknowledges the request by sending the Delete Session Response message through the SGW to the MME.

3.3 MME-Initiated Detach

The MME-Initiated Detach procedure can be explicit or implicit. During an explicit detach, the MME-Initiated Detach procedure is used by the MME to inform the UE that the UE no longer has access to the EPS.

When the UE is in the ECM-IDLE state and is explicitly detached, the MME pages the UE before detaching it. For more information, see Paging Triggered by the MME on page 33. When the UE is implicitly detached, the MME does not send the Detach Request message to the UE.

The MME-Initiated Detach procedure is triggered by one of the following criteria:

— The delete_subscriber CLI command in the MME

— The action_ue_detach_start CLI command in the MME

— Release of the last PDN connection for UEs not supporting EMM-REGISTERED without PDN Connection

— The IMEI Check procedure

— All PDN connections barred by the ODB function in the HSS for UEs that do not support EMM-REGISTERED without PDN Connection

— UEs not permitted access after sending a Detach Request message from a CSG

3.3.1 Traffic Case for Explicit Detach

The MME-Initiated Detach procedure without NR Usage Data Reporting is shown in Figure 9, and is described below the figure.

This procedure is also valid for NR-capable UEs in ECM-IDLE.

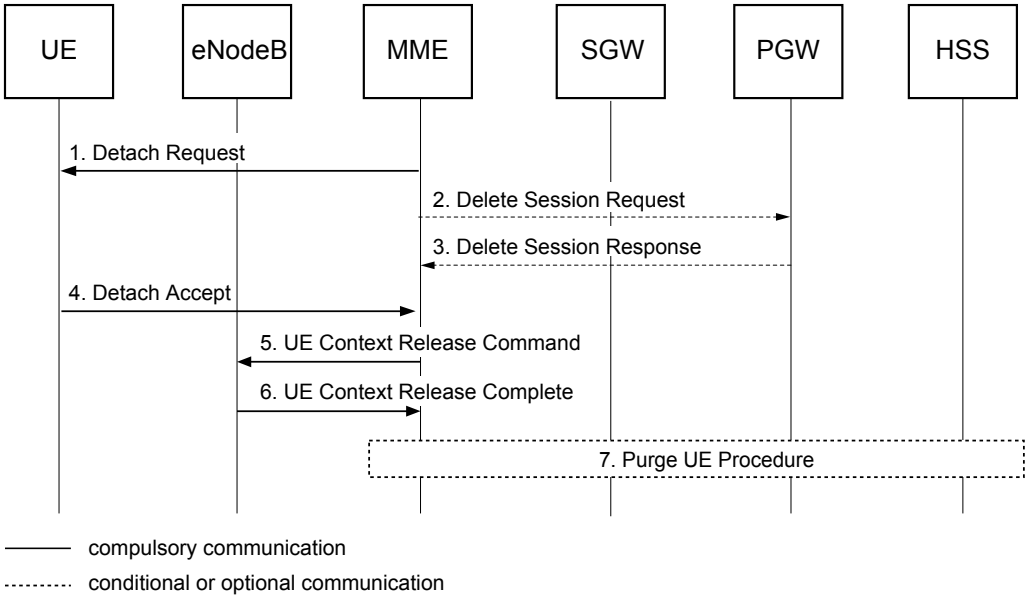


Figure 9 MME-Initiated Detach Procedure

The following steps describe the MME-Initiated Detach procedure:

1. The MME detaches the UE by sending a `Detach Request` message including the `Detach Type` IE to the UE. The Detach Type can be set to `Re-attach` in which case the UE is requested to reattach after the Detach procedure is completed.

   If the UE does not support EMM-REGISTERED without PDN Connection, and the MME-Initiated Detach procedure is triggered by the `Delete Bearer Request` message received from the SGW including the GTPv2 cause code `PDN reconnection to this APN disallowed`, and this is the last PDN connection, the `Detach Request` message includes the `Detach Type` IE, which is set to **`re-attach not required`**. The `EMM Cause` IE is also set according to the `CcDetReqByPgwInitPdnDisc` parameter.

   Note: If the `CcDetReqByPgwInitPdnDisc` parameter is set to **none**, the `EMM Cause` IE is not included in the `Detach Request` message.

2. If the UE has PDN connections toward the SGW and the PGW, the MME sends a `Delete Session Request` message to deactivate the PDN connection in the SGW and the PGW associated with the UE. One `Delete Session Request` message is sent through the SGW to the PGW for each PDN connection.

   If the UE has PDN connections toward the SCEF, the MME sends a `Connection Management Request` message to deactivate the PDN connections in the SCEF associated with the UE. One `Connection Management Request` message is sent to the SCEF for each PDN connection. For more information, see Non-IP Data Delivery over SCEF.

3. The PGW acknowledges the request by sending the `Delete Session Response` message through the SGW to the MME.

4. If the UE receives the `Detach Request` message from the MME, the UE sends a `Detach Accept` message to the MME any time after the `Detach Request` message.

5. The MME releases the S1-MME signaling connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach. If the `Detach Type` IE is set to **`Re-attach`**, the UE reattaches after the RRC Connection Release is completed.

6. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME.

7. If the delete_subscriber CLI command or the action_ue_detach_start CLI command is used to trigger the Detach with `Purge UE Request`, the MME sends a `Purge UE Request` message to the HSS. The HSS sets the UE Purged flag and responds by sending the `Purge UE Answer` message to the MME. The message contains the user state and location information if the `–aanh S6aAllowAdditionalNetLocHss` parameter in the modify_s6a CLI command is set to true.

3.3.2 Traffic Case with NR Usage Data Reporting

The MME-Initiated Detach procedure with NR Usage Data Reporting is the same as step 3 to step 8 in the HSS-Initiated Detach procedure with NR Usage Data Reporting shown in Traffic Case with NR Usage Data Reporting on page 20 if the UE fulfills the following conditions:

— The UE is NR capable.

— The UE is not restricted from using NR.

— The UE is in the ECM-CONNECTED state.

3.3.3 Implicit Detach

The network detaches the UE implicitly without a notification. This is because of the expiration of the configuration-dependent implicit detach timer, which is triggered when the mobile reachable timer has expired, or an irrecoverable radio error causing a loss of the logical link. The EMM context and the PDN connections of the subscriber are deleted from the MME, but the GUTI, NAS security context, and the unused authentication data are kept.

An emergency attached UE is implicitly detached once the mobile reachable timer expires. An unauthenticated UE that is emergency attached is removed from the MME.

3.4 PGW-Initiated Detach

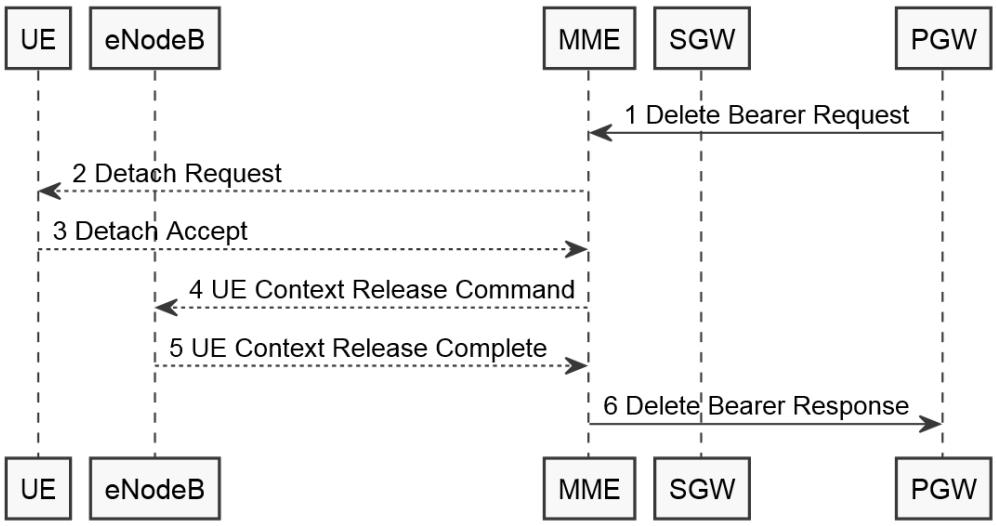
The PGW initiates a Detach procedure when the network initiates a PDN Disconnection procedure by which the last PDN connection of the UE is removed for UEs not supporting EMM-REGISTERED without PDN Connection.

For more information on the PGW-initiated PDN Disconnection procedure, see LTE Session Management.

3.4.1 Traffic Case

The PGW-Initiated Detach procedure is shown in Figure 10 and is described below the figure.

Figure 10 PGW-Initiated Detach Procedure



The following steps describe the PGW-Initiated Detach procedure:

1. The PGW-Initiated Detach procedure is initiated by the PGW sending a `Delete Bearer Request` message to the MME.
2. The MME sends the `Delete Bearer Response` message through the SGW to the PGW.

3. The MME informs the UE that the UE is being detached by sending a `Detach Request` message. The `Detach Request` message includes the `Detach Type` IE that is set to **`re-attach required`** and does not include the `EMM Cause` IE.

4. The UE sends a `Detach Accept` message to the MME.

5. The MME releases the connection for the UE by sending the `UE Context Release Command` message to the eNodeB with the cause set to Detach.

   If the NR Usage Data Reporting feature is activated, the `Secondary RAT usage report list` IE can be included, if data is received.

6. The eNodeB acknowledges the request by sending the `UE Context Release Complete` message to the MME.

   The MME can include the `Secondary RAT usage report list` IE, if received in step 5.

Note: For implicit detach, to are skipped.

4 Paging

Paging, also referred to as the Network-Initiated Service Request, is used for signaling between a UE and the MME when the UE is in the ECM-IDLE state. This procedure triggers the setup of the S1 connection, which changes the state of the UE to ECM-CONNECTED.

When a UE in the ECM-IDLE state receives a paging indication, the UE initiates the UE triggered Service Request procedure.

When a UE in the ECM-IDLE state using DoNAS receives a paging indication, the UE can also send a `Control Plane Service Request` message to the MME. For more information, see Massive IoT.

When a UE in the ECM-IDLE state and using User Plane CIoT EPS optimization, that has been suspended by the eNodeB, receives a paging indication, the UE initiates the Connection Resume procedure.

The operator can configure the Paging procedure to reduce the number of paging messages, which in turn can contribute to reduction in the network load. By reducing the number of paging messages, fewer resources are allocated to the MME. The available resources can be used for handling more users. Less paging also reduces the signaling in the radio access network.

The `Paging` message carries the `Assistance Data for Recommended Cells` IE if the `Recommended Cells for Paging` IE is present in the `UE Context Release Complete` message received from the eNodeB during procedures such as S1 Release and TAU.

Paging is attempted only if the PPF is set to `true`.

If the Configurable and Adaptive Paging feature is activated, the MME initiates the Paging procedure by going through the paging profile selection table. If the Configurable and Adaptive Paging feature is deactivated, the MME skips the paging profile selection table, and uses the default paging profile 1. The number of paging attempts can still be configured. An example of the paging profile selection table is shown in Table 1. The paging profile selection table identifies which paging profile in the paging profile table is used. The default paging profile table is shown in Table 1.

The paging profile selection table is configured by the operator to fit the network configuration and the UE behavior. The selected paging profile is based on the configured parameter values. The current values of the parameters are compared with the table values, and the paging profile with a full row match is selected. If no paging profile selection table has been configured by the operator, the default paging profile selection with priority rule `100` and paging profile 1 is used.

The following information can be used for selecting a paging profile:

— The time since the UE last reported its location

— The Allocation/Retention Priority (ARP) priority level value

— The value of the QCI range

— The APN

— The IMSI Number Series

— The IMEI Number Series

— The Geographical Area Name (GAN)

The QCI, APN, and the ARP are related to individual bearers, therefore the MME needs to know which bearer is intended for paging. The MME finds the QCI, the APN, and the ARP using the `EPS Bearer IIE` (EBI), the `ARP` IE, and the `Private Extension` IE that are optionally included in the `Downlink Data Notification` (DDN) message, described as followed:

— QCI

  The MME uses the QCI stored in the MME and identified by the EBI. The EBI is obtained either from the `EBI` IE or from the `Private Extension` IE. If multiple EBIs are present in the DDN message, the MME uses the minimum QCI for paging profile selection.

— APN

  The MME uses the APN stored in the MME and identified by the EBI. If multiple EBIs are present in the DDN message, the MME uses the corresponding APN for paging profile selection only when all the EPS bearers belong to the same PDN connection.

— ARP

  The MME obtains the ARP from the following sources:

  - If the `ARP` IE is included in the DDN message, the MME uses the ARP in the `ARP` IE.
  - If the `ARP` IE is not included in the DDN message but the EBI is available, the MME uses the ARP stored in the MME and identified by the EBI. If multiple EBIs are present in the DDN message, the MME uses the minimum ARP for paging profile selection.

For SMS over SGs, the operator selects a paging profile that does not page the TA list directly and adds a row in the paging profile selection table including `Time since UE location reportedMin/Max`, `IMSI ns`, or `IMEI ns` that points to such a profile. If such row does not exist in the paging profile selection table, the default profile is selected. Alternatively, the operator adds a row in the paging selection table for this to alter the default paging profile. If the operator configured a profile for priority `100`, that profile is used as the default. Otherwise, Ericsson predefined profile 1 is used as default.

In some special areas like high-speed railway, operators can allocate high priority for the row including that GAN in the paging profile selection table.

Table 1 Example of a Paging Profile Selection Table

Priority	Time since UE Location reportedMin	Time since UE Location reportedMax	ARPMin	ARPMax	QCIMin	QCIMax	APN	IMSI Number Series	IMEI Number Series	GAN	Comment	Paging Profile
1	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	Ga1	High-speed railway	1
2	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	Ga2	High-speed railway	2
5	0	300	NULL	NULL	NULL	NULL	NULL	NULL	NULL	undefined	NULL	3
10	NULL	NULL	4	4	NULL	NULL	ericsson.se.mnc015.mcc234.GPRS	NULL	NULL	undefined	NULL	2
15	NULL	NULL	NULL	NULL	NULL	NULL	ericsson.se.mnc015.mcc234.GPRS	NULL	NULL	undefined	NULL	3
20	NULL	NULL	NULL	NULL	NULL	NULL	NULL	123456	NULL	undefined	NULL	2
25	NULL	NULL	1	3	5	5	ericsson2.se.mnc015.mcc234.GPRS	654321	654323	undefined	EXAMPLE	3
30	NULL	NULL	NULL	NULL	1	1	NULL	NULL	NULL	undefined	NULL	1
35	NULL	NULL	NULL	NULL	2	2	NULL	NULL	NULL	undefined	NULL	1
40	NULL	NULL	NULL	NULL	5	5	NULL	NULL	NULL	undefined	NULL	2
45	NULL	NULL	NULL	NULL	9	9	NULL	NULL	NULL	undefined	NULL	3
50	NULL	NULL	4	15	NULL	NULL	NULL	NULL	NULL	undefined	NULL	2
100	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	undefined	DEFAULT	1

Note: For more information on how to configure the paging profile selection table, see Configuring Adaptive Paging.

Configuring the paging profile selection table reduces the number of paging messages. Finding the UE using paging profile 2 or 3 can be more time consuming if the UE is not located where it is expected.

The target width of the paging profiles specifies the number of paging attempts, see Table 1 .

Table 2 Number of Paging Messages Sent per Target Width for Default Paging Profiles

Paging Profile	Target Width				Paging Timer (T3413) (1)	Confidence Level for Probabilistic eNodeB List Paging
	Last Visited eNodeB	Latest Visited eNodeB List or Probabilistic eNodeB List (2)	Last Visited Tracking Area	TAI List		
1	0	0	0	4 (3)	-	-
2	0	0	2	3	-	-
3	2	0	2	2	-	-
4	0	2	2	3	2	0.8, 0.99
...	...	...	...	...	...	...
20	3	2	3	2	4	0.8, 0.99

(1) The Default Paging Timer Value for All Paging Profiles Is Defined by the `S1T3413PagingTimer` Parameter.

(2) For more information about the Probabilistic eNodeB List paging, see Machine Learning Enhanced Adaptive Paging.

(3) Configurable Value

The following paging profiles are available:

— Paging profile 1

  If paging profile 1 is selected, all eNodeBs that are related to the TAs listed in the TAI list of the UE receive a paging message. By default, four paging attempts are performed, unless the UE responds earlier. Paging profile 1 is recommended to use when short latency is critical or when a considerable amount of time has elapsed since the last contact with the UE. For IMS Emergency Service and CSFB, paging profile 1 is used independently of the configuration.

— Paging profile 2

  If paging profile 2 is selected, all eNodeBs that are related to the last visited TA of the UE receive a paging message. Two paging attempts are made, and if no `Service Request` message is received, all eNodeBs that are related to the TAs listed in the TAI list receive a paging message. Paging profile 2 is recommended to use when the UE is expected to be in the same TA, but not necessarily in the same eNodeB. For information about TAI lists, see TAI List on page 141.

— Paging profile 3

If paging profile 3 is selected, a paging message is sent to the last visited eNodeB first. If the UE is not found after two paging attempts, all eNodeBs that are related to the last visited TA will receive two paging messages. If the UE is still not found, two paging messages are sent to all eNodeBs that are related to the TAs listed on the TAI list. Paging profile 3 is recommended when paging a UE that has recently been present in an eNodeB, and when short latency is not critical.

Note: Paging profiles 1–3 are default profiles and cannot be deleted. Only the number of paging attempts for the TAI list in paging profile 1 can be modified.

— Paging profiles 4–20

It is possible for the operator to create and configure paging profiles 4–20 in the paging profile table. This includes:

- The configuration of individual paging timer values for separate paging profiles with the `ProfileT3413PagingTimer` parameter.
- The confidence level used by probabilistic eNodeB list paging.

For information on how to create and modify paging profiles, see Configuring Adaptive Paging.

4.1 Paging Examples

The following two tables show examples of the number of paging attempts that are performed, and the number of paging messages that are sent depending on which paging profile is used. In these examples, the TAI list registered in the UE contains five tracking areas. Each tracking area contains ten eNodeBs. The latest visited eNodeB list or the probabilistic eNodeB list contains five eNodeBs. For more information about the Probabilistic eNodeB List, see Machine Learning Enhanced Adaptive Paging

Example 1

Table 3 illustrates the number of paging messages sent for a UE that has not moved from the last visited eNodeB. Each row in the table represents one paging profile. The UE is found equally fast, regardless of which paging profile is used. However, the number of paging messages differs in quantity, and Ericsson recommends to use paging profile 3.

Table 3 Number of Paging Messages for a UE Remaining in the Last eNodeB

Paging Profile	Paging Width	Paging Messages	Found
1	TAI List	50	Yes
2	TA	10	Yes

Paging Profile	Paging Width	Paging Messages	Found
3	eNodeB	1	Yes
4	Latest Visited eNodeB List or Probabilistic eNodeB List	5	Yes

Example 2

Table 4 illustrates the number of paging messages for a UE that has moved not only from its last visited eNodeB, but also to a new tracking area. In this example, the UE is found quickly and with a minimum of paging attempts if paging profile 4 is used. In this case, paging profile 3 causes a delay because the UE is not found until the entire TAI list is used, that is after the fifth round of paging attempts.

Ericsson recommends using paging profile 4 when the UE does not remain in the last visited eNodeB and a large tracking area is configured in the network, for example, a tracking area includes about 100 eNodeBs.

Table 4 Number of Paging Messages for a UE Having Moved to a New Tracking Area

Paging Profile	Paging Width	Paging Messages	Found	Total Number of Paging Messages
1	TAI List	50	Yes	50
2	TA × 2	10 × 2 = 20	No	70
	TAI List	50	Yes	
3	eNodeB × 2	1 × 2 = 2	No	72
	TA × 2	10 × 2 = 20	No	
	TAI List	50	Yes	
4	Latest Visited eNodeB List or Probabilistic eNodeB List	5	Yes	5

4.2 Paging Procedure

Paging is performed when the MME receives signaling towards a UE in the ECM-IDLE state, or through the MME when the MSC/VLR wants the UE to be paged. A `Paging` message is sent to the eNodeB, or the eNodeBs, based on the selected paging profile.

The following subsections describe example scenarios where paging is triggered by the MME, SGW, PGW, MSC/VLR, and the HSS.

4.2.1 Paging Triggered by the MME

This section describes an example scenario where paging is triggered by an MME-initiated explicit detach when the UE is in the ECM-IDLE state.

4.2.1.1 Traffic Case

The Paging procedure triggered by an MME-initiated explicit detach is shown in Figure 11 and is described below the figure.

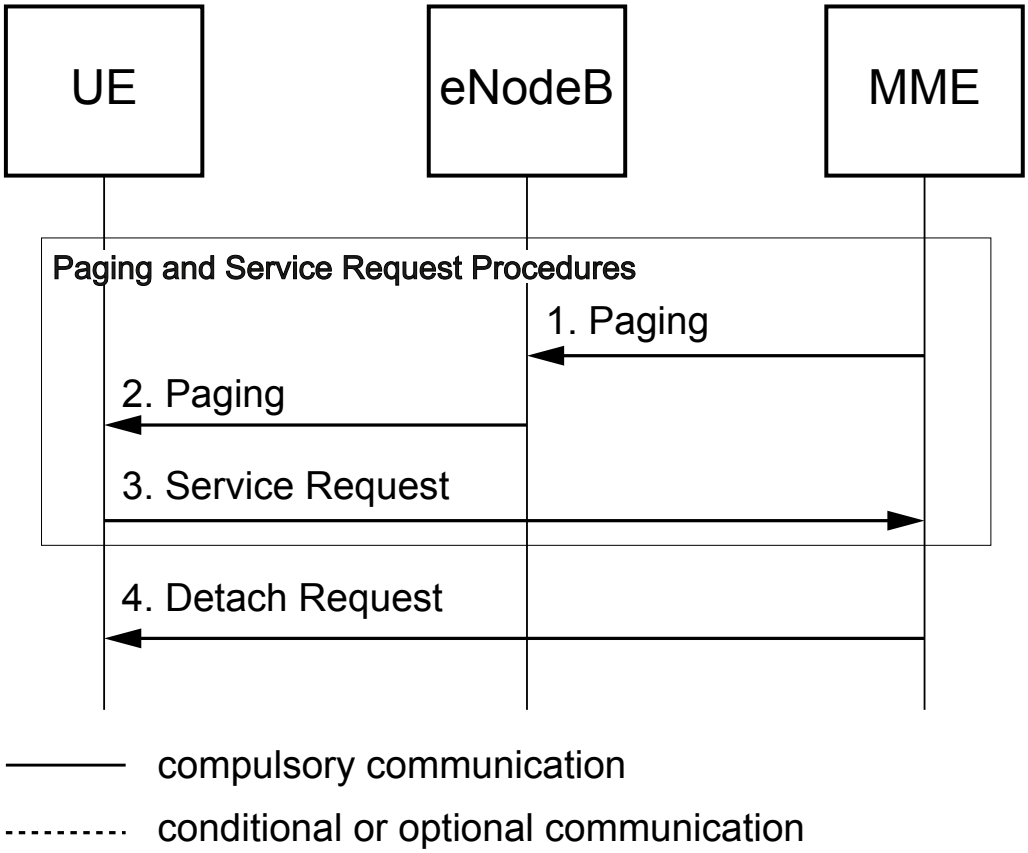


Figure 11 Paging Triggered by an MME-Initiated Explicit Detach

The following steps describe the Paging procedure triggered by an MME-initiated explicit detach:

1. When the UE is in the ECM-IDLE state, the MME sends `Paging` messages to the eNodeB or the eNodeBs, based on the selected paging profile.

   The MME can include the `UE Radio Capability for Paging` IE and the `Assistance Data for Paging` IE in the `Paging` message. For more information, see Massive IoT.

2. If the eNodeB or the eNodeBs receive the `Paging` messages from the MME, the eNodeB or the eNodeBs page the UE.

3. The UE responds to the `Paging` message by sending a `Service Request` message to the MME to initiate the Service Request procedure.

   For more information about the Service Request procedure, see Service Request on page 45.

4. The MME sends a `Detach Request` message to the UE to initiate an explicit Detach procedure, as described in MME-Initiated Detach on page 22.

4.2.2 Paging Triggered by the SGW

This section describes an example scenario where paging is triggered by a DDN message sent on the S11 interface from an SGW as part of the network-triggered Service Request procedure when the UE is in the ECM-IDLE state.

4.2.2.1 Traffic Case

The Paging procedure triggered by a DDN message from the SGW is shown in Figure 12 and is described below the figure.

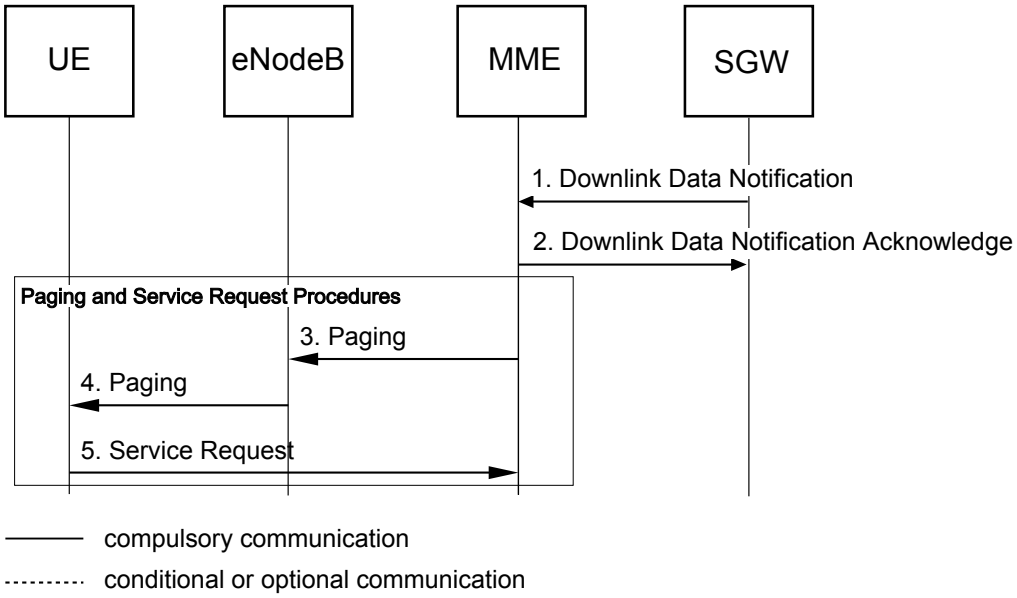


Figure 12 Paging Triggered by a DDN Message from the SGW

The following steps describe the Paging procedure triggered by a DDN message from the SGW:

1. The SGW sends a DDN message to the MME.

   The DDN message includes an ARP level possibly indicating that the procedure is MPS-classified. For more information, see Configuring Multimedia Priority Service .

2. The MME responds by sending a `Downlink Data Notification Acknowledgement` message to the SGW.
3. When the UE is in the ECM-IDLE state, the MME sends `Paging` messages to the eNodeB, or the eNodeBs, based on the selected paging profile.

   If the procedure is MPS-classified, the MME includes the `Paging Priority` IE in the `Paging` messages.

   The MME can include the `UE Radio Capability for Paging` IE and the `Assistance Data for Paging` IE in the `Paging` messages. For more information, see Massive IoT.
4. If the eNodeB(s) receive the `Paging` messages from the MME, the eNodeB or the eNodeBs paUE is paged by the eNodeB(s).
5. The UE responds to the `Paging` message by sending a `Service Request` message to the MME to initiate the Service Request procedure.

   For more information about the Service Request procedure, see Service Request on page 45.

4.2.3 Paging Triggered by the PGW

This section describes an example scenario where paging is triggered by a `Create Bearer Request`, `Update Bearer Request`, or a`Delete Bearer Request` message from the PGW when the UE is in the ECM-IDLE state. The activation, update, or the deletion of bearers continues after the Paging and the Service Request procedures are finished. For more information about the activation, update, or the deletion of bearers, see LTE Session Management.

4.2.3.1 Traffic Case

The Paging procedure triggered by the activation of bearers is shown in Figure 13 and is described below the figure. The Paging procedure triggered by the update or the deletion of bearers is identical to this procedure.

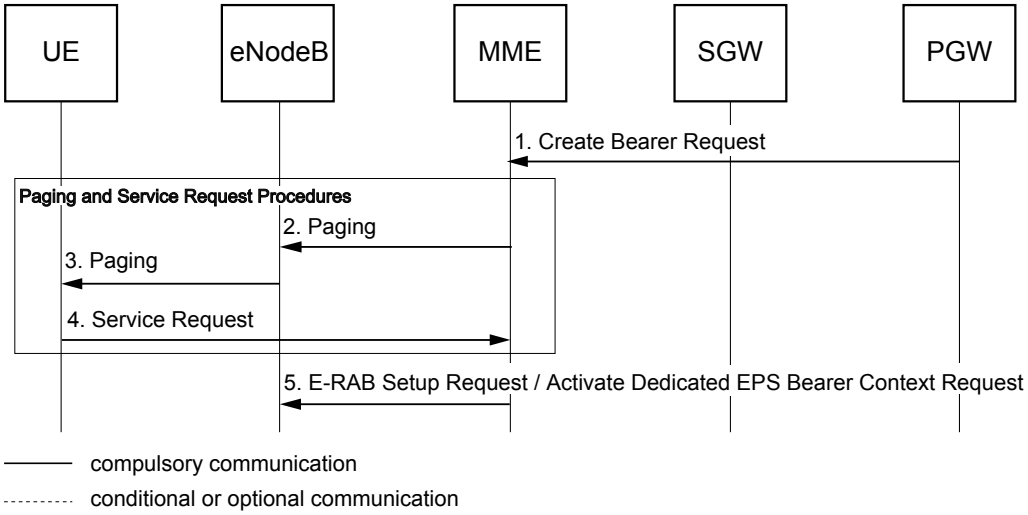


Figure 13 Paging Triggered by a Create Bearer Request Message from the PGW

The following steps describe the Paging procedure triggered by a `Create Bearer Request` message from the PGW:

1. The PGW initiates the activation of bearers by sending a `Create Bearer Request` message through the SGW to the MME.

   The `Create Bearer Request` message includes an ARP level possibly indicating that the procedure is MPS-classified. For more information, see Configuring Multimedia Priority Service.

2. When the UE is in the ECM-IDLE state, the MME sends `Paging` messages to the eNodeB, or the eNodeBs, based on the selected paging profile.

   If the procedure is MPS-classified, the MME includes the `Paging Priority` IE in the `Paging` messages.

   The MME can include the `UE Radio Capability for Paging` IE and the `Assistance Data for Paging` IE in the `Paging` messages. For more information, see Massive IoT.

3. If the eNodeB(s) receive the `Paging` messages from the MME, the eNodeB or the eNodeBs page the UE.

4. The UE responds to the `Paging` message by sending a `Service Request` message to the MME to initiate the Service Request procedure.

   For more information about the Service Request procedure, see Service Request on page 45.

5. The MME selects an EPS Bearer Identity, and then sends an `E-RAB Setup Request` message containing the EPS Bearer Identity to the eNodeB. The `E-RAB Setup Request` message contains one `Activate Dedicated EPS Bearer Context Request` message for each bearer to be set up.

The activation of dedicated bearers continues as described in LTE Session Management.

4.2.4 Paging Triggered by the MSC/VLR

This section describes an example scenario where paging is triggered by a `Paging Request` message for SMS from the MSC/VLR.

4.2.4.1 Traffic Case

The Paging procedure triggered by a `Paging Request` message from the MSC/VLR is shown in Figure 14 and is described below the figure.

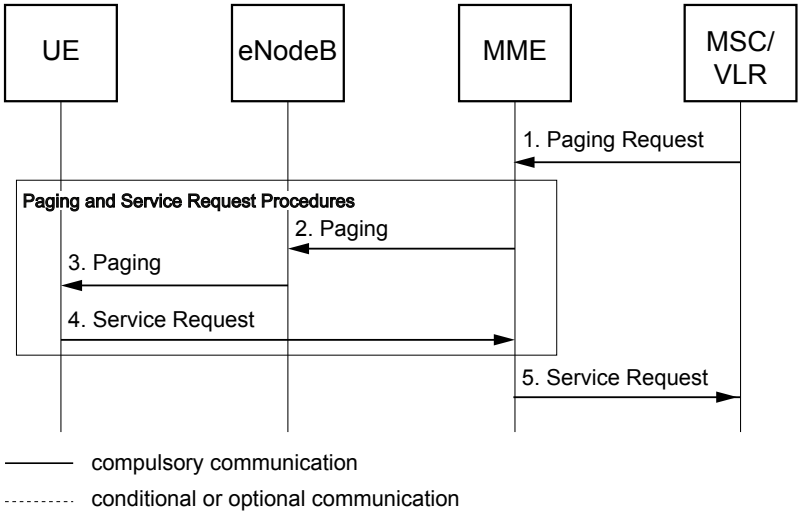


Figure 14 Paging Triggered by a Paging Request Message from the MSC/VLR

The following steps describe the Paging procedure triggered by a `Paging Request` message from the MSC/VLR:

1. The MSC/VLR sends a `Paging Request` message for SMS to the MME.
2. When the UE is in the ECM-IDLE state, the MME sends `Paging` messages to the eNodeB, or the eNodeBs, based on the selected paging profile.

   The MME can include the `UE Radio Capability for Paging` IE and `Assistance Data for Paging` IE in the `Paging` messages. For more information, see Massive IoT.
3. If the eNodeB or the eNodeBs receive the `Paging` messages from the MME,the eNodeB or the eNodeBs page the UE.
4. The UE responds to the `Paging` message by sending a `Service Request` message to the MME to initiate the Service Request procedure.

For more information about the Service Request procedure, see Service Request on page 45.

5. The MME sends an SGsAP `Service Request` message to the MSC/VLR.

   The MT-SMS procedure continues as described in EPS Support for CS Services.

4.2.5 CS Fallback Paging Triggered by the MSC/VLR

This section describes an example scenario where CS Fallback paging is triggered by a voice call from the MSC/VLR for an SMS-only UE.

4.2.5.1 Traffic Case

The CS Fallback Paging procedure triggered by a voice call from the MSC/VLR is shown in Figure 15 and is described below the figure.

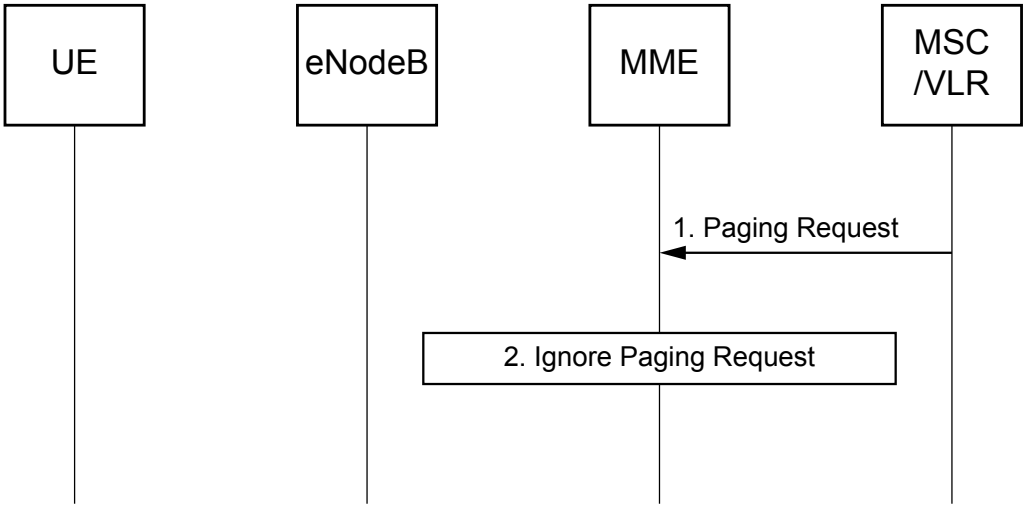


Figure 15 CS Fallback Paging Triggered by a Voice Call from the MSC/VLR

The following steps describe the CS Fallback Paging procedure triggered by a voice call from the MSC/VLR:

1. The MSC/VLR sends a `Paging Request` message to the MME. The value of the `Service Indicator` IE in the `Paging Request` message is `CS Call`.

2. When the node function `ignore_csfb_call_paging_request_for_sms_only_ue` on the MME is enabled, the MME ignores the `Paging Request` message from the MSC/VLR for an SMS-only UE, and suppresses the `Paging Reject` message toward the MSC/VLR.

Note: The following examples are the UEs that are given the SMS-only authority:

- When the feature parameter `csfb_to_wg` is set to on and the feature parameter `sms_over_sgs` is set to on, the UE is in a Combined Attach/TAU or an EPS Attach/TAU procedure with the `Additional Update Type` IE set as `SMS only`.
- When the feature parameter `csfb_to_wg` is set to off and the feature parameter `sms_over_sgs` is set to on, the UE is in a Combined Attach/TAU with or without the `Additional Update Type` IE set as `SMS only`, or in an EPS Attach/TAU procedure with the `Additional Update Type` IE set as `SMS only`.
- When the feature parameter `csfb_to_wg` is set to on, the feature parameter `sms_over_sgs` is set to on, but the LA is limited to SMS-only services due to the configuration, the MME only provides SMS Services when the UE moves into this LA.
- When the feature parameter `csfb_to_wg` is set to off, the feature parameter `sms_over_sgs` is set to on, and the `CombinedRegistrationSetting` parameter in the `IMSINS` CLI command is set to `dummy_cs_service`, then the UE is in a Combined Attach/TAU procedure with CSFB capability.

4.2.6 Paging Triggered by the HSS

This section describes an example scenario where paging is triggered by a `Cancel Location Request` message with the `Cancellation Type` IE set to `Subscription Withdrawal` from the HSS when the UE is in the ECM-IDLE state.

4.2.6.1 Traffic Case

The Paging procedure triggered by a `Cancel Location Request` message from the HSS is shown in Figure 16 and is described below the figure.

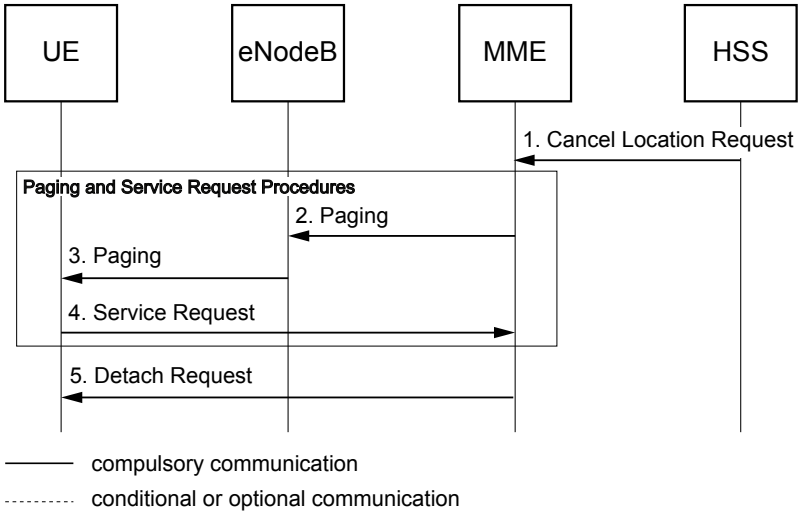


Figure 16 Paging Triggered by a Cancel Location Request Message from the HSS

The following steps describe the paging triggered by a `Cancel Location Request` message from the HSS:

1. The HSS sends a `Cancel Location Request` message with the `Cancellation Type` IE set to `Subscription Withdrawal` to the MME.
2. When the UE is in the ECM-IDLE state, the MME sends `Paging` messages to the eNodeB, or the eNodeBs, based on the selected paging profile.

   The MME can include the `UE Radio Capability for Paging` IE and the `Assistance Data for Paging` IE in the `Paging` messages. For more information, see Massive IoT.
3. If the eNodeB or the eNodeBs receive the `Paging` messages from the MME, the eNodeB or the eNodeBs page the UE.
4. The UE responds to the `Paging` message by sending a `Service Request` message to the MME to initiate the Service Request procedure.

   For more information about the Service Request procedure, see Service Request on page 45.
5. The MME sends a `Detach Request` message to the UE to initiate an explicit Detach procedure, as described in MME-Initiated Detach on page 22.

4.3 Paging Failure

Paging is not started or fails when an S1 connection cannot be established.

Paging is not started in the following cases:

— If the PPF is set to `false`

— If the UE is suspended

Paging is started but fails in the following case:

— If all the paging retransmissions fail

If paging fails because there is no response from the UE, the MME initiates the Dedicated Bearer Deactivation procedure for GBR bearers.

If the rejected Paging procedure was triggered by an MME-Initiated Detach procedure, the MME detaches the UE implicitly without notifying the UE.

Without smart paging, if all paging retransmissions have failed and a new DDN arrives, the paging cycle starts again. For information on smart paging, see Smart Paging on page 41.

4.4 Smart Paging

Smart paging reduces the signaling load generated by unsuccessful Paging procedures in radio networks that have a massive paging load. By using smart paging for LTE access, the load on the E-UTRAN can be decreased. Smart paging allows the customization of the paging in the network through configurable timers. When configuring the smart paging restrictions, it is important to consider the current network situation.

Smart paging allows configuration of the following properties:

— The time interval between the paging attempts

  A longer time interval between the paging attempts increases the possibility for the UE to reach coverage.

— The quarantine time for Paging procedures triggered by DDN messages

  It is possible to increase the quarantine time gradually until the next Paging procedure triggered by a DDN message can begin.

  Note: Other downlink signaling, including the `Create Bearer Request`, `Update Bearer Request`, control plane signaling, and the CS call, trigger a paging procedure immediately, even if the quarantine timer is running. The downlink signaling does not affect the timer.

For smart paging, the following parameters can be configured using the create_s1_mme and the create_paging_profile CLI commands:

— S1RepeatPaging

— S1RepeatPagingStep

— S1T3413PagingTimer

— ProfileT3413PagingTimer

Note: The Configurable and Adaptive Paging feature must be enabled to allow configuration of the paging timer value per paging profile.

During the paging quarantine time, the UE is unreachable, that is, a DDN message cannot trigger a new Paging procedure. Smart paging introduces a gradually increasing quarantine time that can be used to reduce the paging load by less frequent paging. The gradually increasing quarantine time is further described in Figure 17.

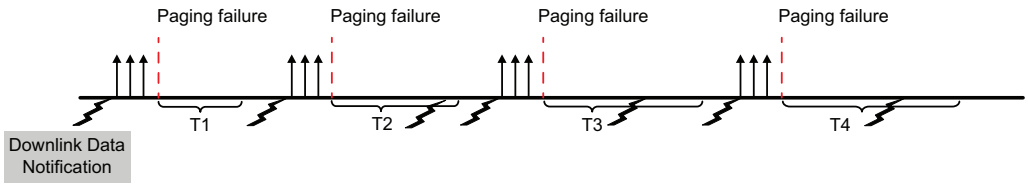


Figure 17 Gradually Increased Quarantine Time

The quarantine time is increased as follows:

T1 S1RepeatPaging

T2 T1 + S1RepeatPagingStep

T3 T1 + 2 * S1RepeatPagingStep

T4 T1 + 3 * S1RepeatPagingStep

The Paging procedure is repeated by using this pattern until the SGSN-MME receives an `Initial UE` message or the mobile reachable timer expires. If all retransmissions of the `Paging Request` message fail, the paging is rejected.

4.5 Service Priority Based Paging

Service Priority Based Paging enables the MME to prioritize the paging for specific services based on the ARP of the DDN message sent from the SGW. This enhancement is applicable only when the IMS-Based Telephony - MMTel feature is enabled.

The MME does the following for high-priority services when receiving a DDN message that has an ARP priority equal to or higher than the priority configured through the PrioritizePagingBasedOnArp parameter:

— The MME immediately starts a Paging procedure regardless of the paging quarantine timer.

— When the MPS-classified ARP level is not configured, the MME ends the ongoing Paging procedure and starts a new Paging procedure if the ARP

priority of the DDN message is higher than that of the previously received message.

For more information on MPS-classified ARP level, see Quality of Service and Configuring Multimedia Priority Service.

The MME obtains the ARP from the ARP IE of the DDN message. If the ARP IE is not available, the MME uses the ARP identified by the EBI.

For the definition of ARP priority level, see Quality of Service.

For more information on how to configure Service Priority Based Paging, see Configuring MMTel Service.

4.6 Paging Suppression for Fixed Wireless Access

The Paging Suppression for Fixed Wireless Access feature reduces the signaling for Fixed Wireless Access (FWA) devices that do not need to be paged. This feature enables the number of paging attempts to be set to 0 for all paging widths in the paging profile. This enhancement is applicable only when the Adaptive Paging for LTE feature is enabled.

To configure the Paging Suppression for Fixed Wireless Access feature, do the following:

1. Enable the Adaptive Paging for LTE feature by setting the feature parameter `lte_adaptive_paging` to `ACTIVATED`.
2. Enable the Paging Suppression for Fixed Wireless Access feature by setting the feature parameter `paging_suppression_for_fwa` to `ACTIVATED`.
3. Configure the paging profile table by using the `create_paging_profile` CLI command to create a paging profile with zero paging attempts to all the paging widths. For example, `create_paging_profile -id 4 -enb 0 -enbl 0 -ta 0 -talist 0`.
4. Configure the paging profile selection table using the `create_paging_selection` CLI command.

Note: When the Paging Suppression for Fixed Wireless Access feature is disabled, Ericsson recommends to delete the paging profile with zero attempts to improve the adaptive paging performance.

For information on how to configure the Adaptive Paging for LTE feature, see Configuring Adaptive Paging.

4.6.1 Paging Suppression for FWA Devices in the DDN Procedure

The `Download Data Notification` (DDN) message is sent from the SGW to the MME. If a UE is in the ECM-IDLE state and the paging profile is configured with all the paging widths as `0`, the MME responds with a `Download Data`

Notification Acknowledge (DDN ACK) message to the SGW including the following:

— The cause code #16 Request Accepted

— The DL Buffering Duration timer set to infinity

— The DL Buffering Suggested Packet Count IE set to 0

Paging is not performed.

Note: If the MME receives the Download Data Notification message when the MME is waiting for the UE Context Release Complete message in the S1 release procedure, the MME first sends the Download Data Notification Acknowledge message with the cause code Request Accepted to the SGW. After the S1 release procedure is completed, if the paging profile is configured with all the paging widths as 0 for the FWA device, the MME suppresses paging and sends the DDN Failure Indication message with the cause code Unable to page UE to the SGW.

For the UE restoration upon the DDN with the IMSI procedure, the Paging Suppression for Fixed Wireless Access feature is not used. For more information, see Geographically Redundant Pool.

4.6.2 Paging Suppression for FWA Devices in Other Procedures

Paging is also suppressed in other procedures and messages than the DDN procedure when a UE is in the ECM-IDLE state. The paging suppression for these procedures and messages is handled in the same way as for failed paging procedures. These procedures and messages are for example:

— The Dedicated Bearer Activation procedure

— The Bearer Modification procedure

— The Pool Move procedure

— The Networks Initiated (explicit) Detach procedure

— The SMS Received message sent from the SMS/VLR

— The Request for Positioning Received message sent from the GMLC

— The Insert Subscriber Data Request message sent from the HSS

5 Service Request

The UE-Initiated Service Request procedure is used when a UE in the ECM-IDLE state attempts to send user data or short messages. It can also be used when the UE in the ECM-IDLE state wants to send uplink signaling messages to re-establish one or several EPS bearers. The Service Request procedure is also used as a `Paging Response` message when preceded by a Paging procedure. For a description of the ECM-IDLE state, see Mobility and Connection Management States on page 2.

A successful UE-Initiated Service Request procedure changes the ECM state to ECM-CONNECTED, allowing the UE to send or receive data or perform signaling. Bearers that cannot be set up in the eNodeB or that cannot be updated in the SGW are removed. If default bearers cannot be set up in the eNodeB or be updated in the SGW, the PDN connections associated with them are removed. If no bearers are left, and the UE does not support EMM-REGISTERED without PDN Connection, the UE is detached with the cause **`Re-attach Required`**. For a description of the ECM-CONNECTED state, see Mobility and Connection Management States on page 2.

A UE using Data over NAS can transfer user data in NAS PDUs, without setting up user plane data radio bearers in the RAN. For more information, see Massive IoT.

5.1 Service Request Procedure

The Service Request procedure is shown in Figure 18.

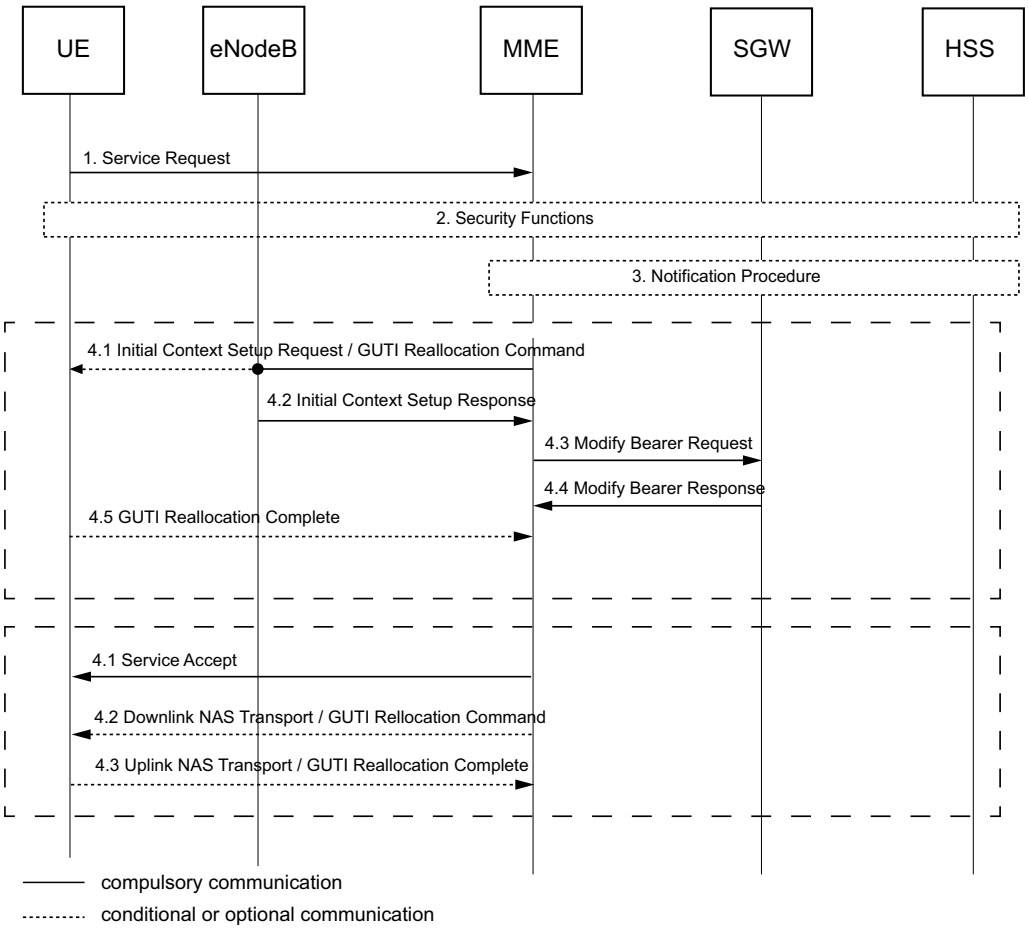


Figure 18 Service Request Procedure

The following steps describe the Service Request procedure:

1. The Service Request procedure is initiated when the UE sends a `Service Request` message through the eNodeB to the MME. `Service Request` messages that indicate emergency are prioritized in instances of resource limitation.

   If the APN or the APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, the PDN connection or connections are deleted towards the SGW after the `Service Request` procedure. For more information, see APN Resolve and Redirect for LTE Access.

2. Security functions can be performed and the subscriber is authenticated. A security context is established, and ciphering and integrity protection are negotiated. For IMS Emergency Service, if the integrity check is approved for the UE, selective authentication is not applied. For more information about the integrity check and selective authentication, see Security.

   If the Service Request procedure is rejected based on Diameter S6a errors received from the HSS, a configurable NAS cause code corresponding to the

Diameter S6a error code is sent to the UE. For the mapping of Diameter S6a error codes to NAS cause codes, see Diameter S6a Error Code to NAS Cause Code Mapping on page 147.

3. If the IMEISV received from the UE during the security functions procedure is different from the previous IMEISV, if it is available, the MME initiates a Notification procedure to the HSS with the updated terminal information. For an unauthenticated UE, no Notification procedure is triggered toward the HSS.

4. The subsequent procedure depends on whether the UE has PDN connections.

☐ If the UE has PDN connections, the following procedure applies:

1. The MME sends the `Initial Context Setup Request` message to the eNodeB. This message contains the TEID and the IP address of the SGW for user-plane traffic.

   GUTI reallocation is performed, and the MME includes a `GUTI Reallocation Command` message in the `Initial Context Setup Request` to the UE, if the following criteria are fulfilled:

   — `ServiceRequestGutiReallocationEnabled` for the UE IMSI number series is set to `true`.

   — The time elapsed since last GUTI reallocation is greater than the configured value for `MMEGutiReallocationTimeLimit`.

   For more information about the `Initial Context Setup Request` message, see LTE Session Management.

   For more information about GUTI reallocation, see Security.

2. The eNodeB performs the Radio Bearer Establishment procedure. When the user-plane radio bearers are set up, the EPS bearer state is synchronized between the UE and the network, that is, the UE removes the EPS bearers for which no radio bearers are set up. The eNodeB sends the `Initial Context Setup Response` message to the MME. This message contains the TEID and the IP address of the eNodeB for user-plane traffic.

3. The MME sends a `Modify Bearer Request` message to the SGW, containing the TEID of the eNodeB and the IP address of the eNodeB. If the parameter `S11UliAlwaysSent` is set to `on`, the MME includes the ULI in the `Modify Bearer Request` to the SGW, even if the previously sent ULI to the SGW has not changed. The MME can also send a `Modify Access Bearers Request` message to the SGW if the following criteria are met:

   — More than one PDN connection exists for the UE.

   — The SGW supports the `Modify Access Bearers Request` message.

— The UseModifyAccessBearers parameter is set to on.

4. The SGW acknowledges the request by sending the `Modify Bearer Response` message containing the identity of the bearers to the MME.
5. If a `GUTI Reallocation Command` message was sent, the UE acknowledges the GUTI by sending `GUTI Reallocation Complete` message. The UE can send a `GUTI Reallocation Complete` message.

☐ If the UE has no PDN connections, the following procedure applies:

1. The MME responds with a `Service Accept` message.
2. If GUTI Reallocation is required, the MME sends the `GUTI Reallocation Command` message in a `Downlink NAS transport` message.
3. The UE responds with the `GUTI Reallocation Complete` message in an `Uplink NAS transport` message.

6 S1 Release

The S1 Release procedure is used to release the logical S1-AP signaling connection and all S1 bearers for the UE. The procedure changes the state of the UE from ECM-CONNECTED to ECM-IDLE and all UE-related context information is deleted from the eNodeB.

6.1 MME- or eNodeB-Initiated S1 Release

The MME initiates an S1 Release procedure in several different situations. The following are a few examples of when the procedure is initiated:

— During Detach

— When an S1-AP signaling connection needs to be removed, for example, after a TAU without `Active` flag or `signalling active` flag being set

— A bearer mismatch in the E-RAB Modification Indication message

— In cases of CS-fallback

The eNodeB initiates an S1 Release procedure in several different situations. The following are a few examples of when the procedure is initiated:

— When the radio connection with the UE is lost

— When user inactivity occurs

— When an unspecified failure occurs

For possible causes for the S1 Release procedure, see section S1AP Cause Codes in EBM Cause Codes.

Note: S1 release history S1_RELEASE_HISTORY is recorded in EBM events L_SERVICE_REQUEST, L_TAU, L_ATTACH, and L_DETACH when the UE re-enters the ECM-CONNECTED state. For more details, see EBM Events and Parameters. The EBM information facilitates troubleshooting and eNodeB parameter tuning.

6.1.1 Traffic Case

The MME-Initiated or the eNodeB-Initiated S1 Release procedure is shown in Figure 19 and is described below the figure.

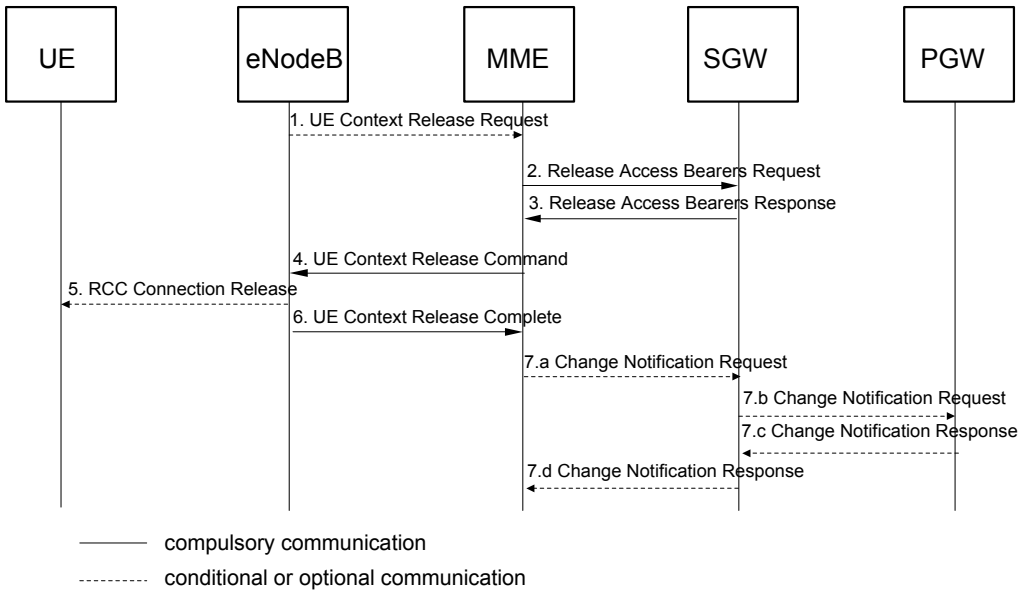


Figure 19 MME- or eNodeB-Initiated S1 Release Procedure

The following steps describe the MME-Initiated or the eNodeB-Initiated S1 Release procedure:

1. If the release is initiated by the eNodeB, the eNodeB sends a `UE Context Release Request` message to the MME. The `UE Context Release Request` message contains the cause for the release.

   If the NR Usage Data Reporting feature is configured, the eNodeB can include the `Secondary RAT Usage Report List` IE if data is received.

2. The MME sends a `Release Access Bearers Request` message to the SGW. The `Release Access Bearers Request` message optionally contains the `Indication Flags` IE. If the S1 release procedure is initiated by the eNodeB because of an abnormal release of radio link, the MME sets the `Abnormal Release of Radio Link` bit in the `Indication Flags` IE to **1**.

   The MME can include the `Secondary RAT Usage Data Report` IE in the `Release Access Bearers Request` message if data is received in step 1. The `IRSGW` and the `IRPGW` bits indicate if the usage data is to be reported to the SGW, the PGW or both.

3. The SGW releases all eNodeB related information for the UE and responds with a `Release Access Bearers Response` message to the MME.

4. The MME releases the S1 connection by sending the `UE Context Release Command` message containing the cause of the release to the eNodeB.

5. If the RRC connection is not already released, the eNodeB starts the RRC Connection Release procedure. Once the procedure is finished, the eNodeB deletes the UE context.

6. The eNodeB confirms the S1 release by returning a `UE Context Release Complete` message to the MME.

   The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Release Complete` message. For more information, see Massive IoT.

   The eNodeB can include the `Secondary RAT Usage Report List` IE. If this IE is included in step 1, it is not included in this message.

7. If the NR Usage Data Reporting feature is activated, and the `Secondary RAT Usage Report List` IE is included in step 1, with the PGW as the intended receiver, step 7 is performed before steps 4-6.

   If the eNodeB provides, and the MME accepts the Secondary RAT Usage Data in step 6, the MME sends the `Change Notification Request` message with the `Secondary RAT Usage Data Report` IE.

7 Connection Suspend

The Connection Suspend procedure is used to suspend a UE using User Plane CIoT EPS optimization. A successful Connection Suspend procedure moves a UE from the ECM-CONNECTED state to the ECM-IDLE state, while allowing the MME to store information needed to resume UE services.

For a description of the ECM-IDLE state, see Mobility and Connection Management States on page 2.

For more information about the Connection Suspend and Resume feature, see Massive IoT and Features and Functions Management.

7.1 Connection Suspend Procedure

The Connection Suspend procedure is shown in Figure 17 and is described below the figure.

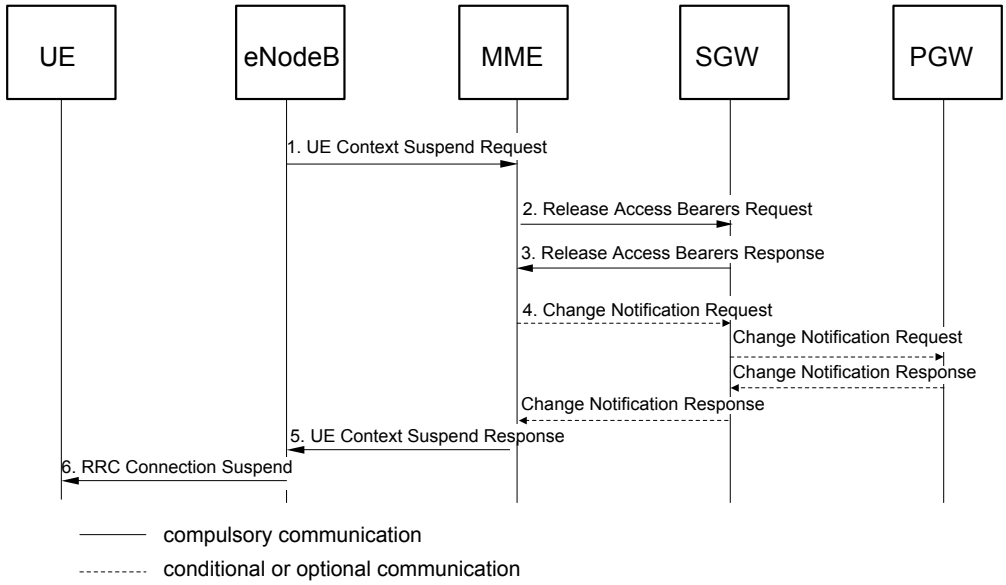


Figure 20 Connection Suspend Procedure

The following steps describe the Connection Suspend procedure:

1. The Connection Suspend procedure is initiated when the eNodeB sends a `UE Context Suspend Request` message to the MME.

   The eNodeB, the UE, and the MME store the information needed to resume the connection. For example, the MME stores the S1-AP association when moving to the ECM-IDLE state.

If the NR Usage Data Reporting feature is configured, the eNodeB can include the `Secondary RAT Usage Report List` IE.

The MME also stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Suspend Request` message.

For more information, see Massive IoT.

2. The MME sends a `Release Access Bearers Request` message to the SGW. If the Secondary RAT Usage Data was received in step 1, the Secondary RAT Usage Data is included in this message.
3. The SGW responds by sending a `Release Access Bearers Response` message to the MME.
4. If the eNodeB includes `Secondary RAT Usage Report List` IE in step 1, then the `Secondary RAT Usage Data Report` IE is included in the `Change Notification Request` and the `Change Notification Response`.
5. The MME suspends the UE by returning a `UE Context Suspend Response` message to the eNodeB.
6. The eNodeB sends an `RRC Connection Suspend` message to the UE to suspend the RRC Connection.

8 Connection Resume

The Connection Resume procedure is used to resume UE services for a UE using User Plane CIoT EPS optimization. The Connection Resume procedure is also used as a `Paging Response` message when preceded by a Paging procedure.

A successful Connection Resume procedure moves a UE from the ECM-IDLE state to the ECM-CONNECTED state without the MME having to resend the UE context and re-establish the S1-AP association.

The Connection Resume procedure can only be used if the MME has stored the UE context and the S1-AP association in a previous successful Suspend procedure.

A successful Mobile Originated Connection Resume procedure changes the ECM state to ECM-CONNECTED, allowing the UE to send or receive data or signaling. Bearers that cannot be set up in the eNodeB or that cannot be updated in the SGW are removed. If the default bearers cannot be set up in the eNodeB or be updated in the SGW, the PDN connections associated with them are removed. If no default bearers are left, the UE not supporting EMM-REGISTERED without PDN Connection is detached with the detach type Re-Attach Required.

For a description of the ECM-CONNECTED state, see Section 2.1 on page 5.

For more information on the Connection Suspend and Resume feature, see Massive IoT and Features and Functions Management.

8.1 Connection Resume Procedure

The Connection Resume procedure is shown in Figure 18 and is described below the figure.

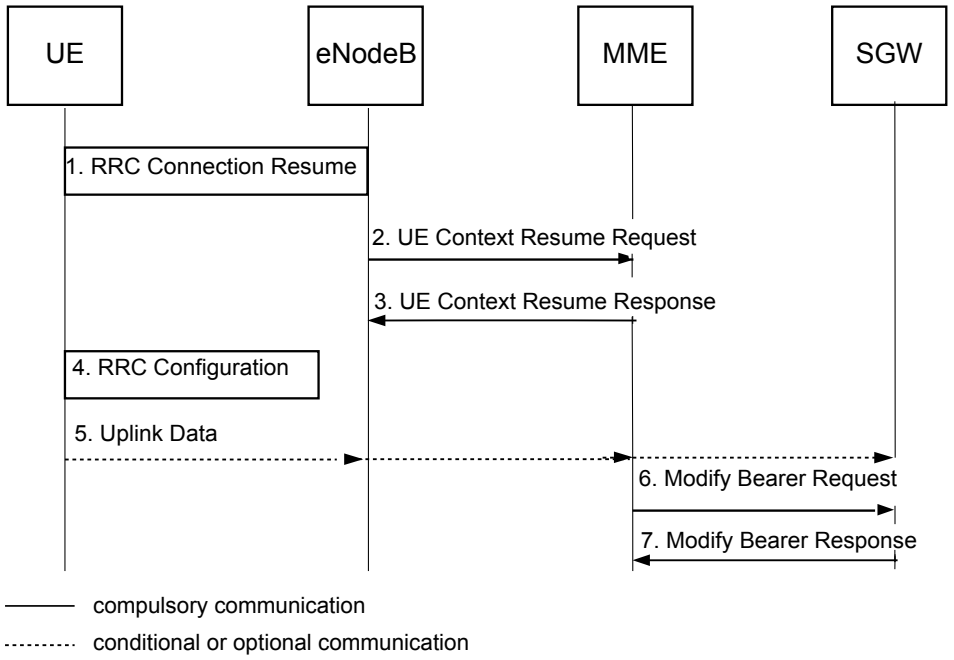


Figure 21 Connection Resume Procedure

The following steps describe the Connection Resume procedure:

1. The UE triggers the RRC Connection Resume procedure, including information needed by the eNodeB to access the AS context stored in the UE.

2. The eNodeB initiates the Connection Resume procedure by sending a `UE Context Resume Request` message to the MME.

   If the APN or the APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, the PDN connection or connections are deleted towards the SGW after the Connection Resume procedure. For more information, see APN Resolve and Redirect for LTE Access.

3. The MME responds by sending a `UE Context Resume Response` message to the eNodeB.

   If the MME cannot admit all suspended E-RABs, the MME indicates this in the `E-RABs Failed To Resume List` IE.

   If the eNodeB cannot admit all suspended bearers, the eNodeB indicates this in the list of rejected EPS bearers. If a default EPS bearer is not accepted by the eNodeB, all the EPS bearers associated with the default bearer are treated as non-accepted bearers. The MME releases the non-accepted and the non-established bearers by triggering the Bearer Release procedure.

4. Optionally, RRC Reconfiguration is initiated if any failed bearers are sent to the eNodeB in the `UE Context Resume Response` message.

5. Optionally, the UE sends `Uplink Data` to the SGW.
6. The MME sends a `Modify Bearer Request` message to the SGW, containing the TEID of the eNodeB and the IP address of the eNodeB. The MME can also send a `Modify Access Bearers Request` message to the SGW if the following criteria are met:
   - More than one PDN connection exists for the UE.
   - The SGW supports the `Modify Access Bearers Request` message.
   - The UseModifyAccessBearers parameter is set to `on`.
7. The SGW responds by sending a `Modify Bearer Response` message or a `Modify Access Bearers Response` message containing the identity of the bearers to the MME.

Note:
- The Connection Resume procedure can also be performed during the X2-based handover procedure by sending a `Path Switch Request` message with the RRC resume cause set. For more information, see Intra-MME X2-Based Handover without SGW Relocation and Intra-MME X2-Based Handover with SGW Relocation.
- The MME does not support simultaneous use of User Plane and Control Plane CIoT EPS optimization for a UE. Switching between User Plane and Control Plane CIoT EPS optimization for a UE is only possible when the UE is in the EMM-DEREGISTERED state after a Detach procedure.

9 Mobility without Dataflow

When the UE is in the ECM-IDLE mode, that is, without dataflow, a TAU procedure updates the MME with information on the tracking area in which the UE is located. The procedure is initiated by the UE when it enters a tracking area outside the current TAI list or the UE or when the periodic TAU timer has expired. For more information about TAU from an SGSN, see Inter-System Mobility Management.

The TAU procedure can also be performed after an X2-Based Handover procedure or an S1-Based Handover procedure. For more information on performing the TAU procedure after an X2-Based Handover procedure, see Mobility with X2-Based Handover on page 87. For more information on performing the TAU procedure after an S1-Based Handover procedure, see Mobility with S1-Based Handover on page 95.

The UE can also initiate an intra-MME TAU procedure by sending a `Combined TAU Request` message. For more information about combined procedures, see EPS Support for CS Services.

For information about TAI lists, see TAI List on page 141.

9.1 Mobility Within an MME Service Area

UE-initiated mobility management procedures are performed when a UE in ECM-IDLE mode moves within an MME service area. Since the MMEs belong to the same service area, it is not required to reselect the MME.

9.1.1 Periodic TAU

The periodic TAU procedure is used by the UE to notify the MME about the existence of the UE. A periodic TAU procedure is performed when the UE stays within tracking areas that belong to the same TAI list and the periodic TAU timer of the UE expires. The periodic TAU procedure is initiated when the MME receives a `TAU Request` message indicating a periodic update from the UE.

The Periodic TAU Timer (T3412) can be deduced from the HSS-subscribed, the IMSI-based or the S1MobileReachableTimer value. For PSM UEs, the Periodic TAU Timer (T3412) also can be deduced from the CBS-configured value or the UE-requested value. For more information, see Massive IoT.

If the Periodic TAU Timer (T3412) cannot be deduced from the CBS-configured (only for PSM), the UE-requested (only for PSM), or the HSS-subscribed timer value because of insufficient information, the Periodic TAU Timer (T3412) value is deduced in the following scenarios:

— If a PeriodicTAUTimer configured based on the IMSI number series exists for the UE, the Periodic TAU Timer (T3412) equals the PeriodicTAUTimer configured based on the IMSI number series.

— If no PeriodicTAUTimer configured based on the IMSI number series exists for the UE, the Periodic TAU Timer (T3412) equals the value of S1MobileReachableTimer minus 4 minutes.

For more information on this feature, see Configuring Session and Mobility Management.

9.1.1.1 Traffic Case

The periodic TAU procedure is shown in Figure 22 and is described below the figure.

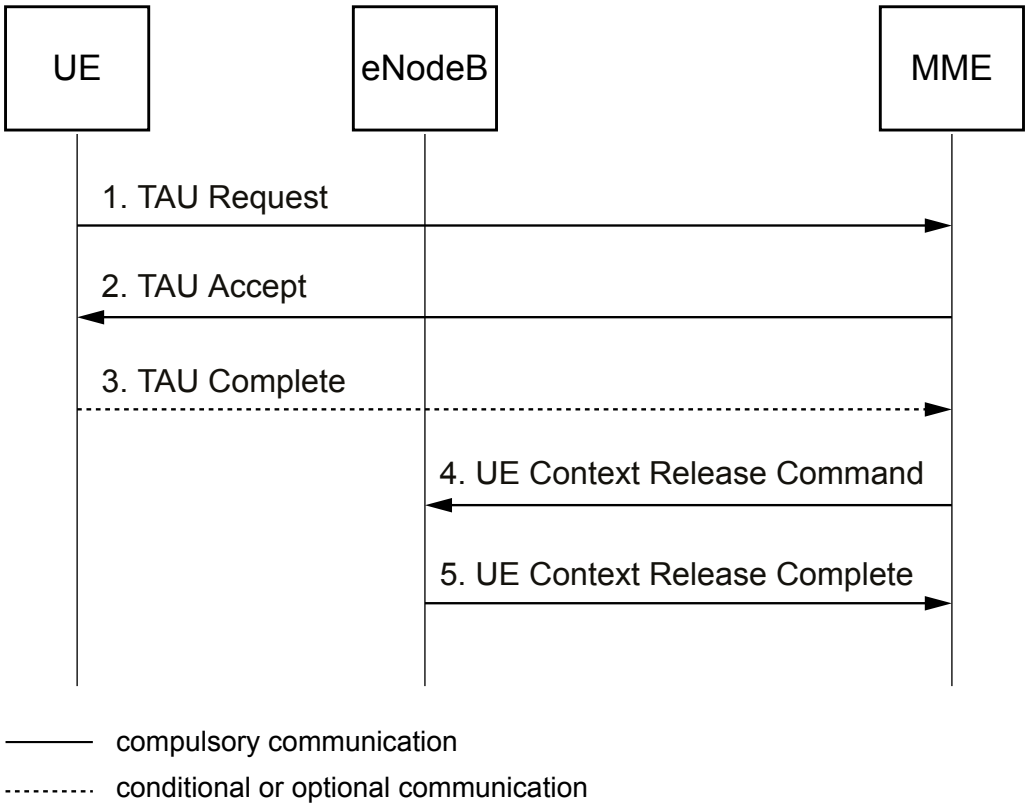


Figure 22 Periodic TAU Procedure

The following steps describe the periodic TAU procedure:

1. When the periodic TAU timer expires, the UE sends a TAU Request message to the MME.

The MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the TAU procedure is rejected, see Mobility without Dataflow Rejected on page 76. If the MME receives a periodic TAU request message from a UE with an emergency PDN connection, the emergency PDN connection is removed. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123.

2. The MME sends a `TAU Accept` message to the UE. If the time elapsed since last GUTI reallocation is greater than the configured value `MMEGutiReallocationTimeLimit`, GUTI reallocation is performed. The MME also includes an EPS bearer context status IE in the `TAU Accept` message, indicating which EPS bearer contexts are active in the MME. The UE locally deactivates all those EPS bearer contexts that are active in the UE, but are indicated by the MME as being inactive.

   If an Equivalent PLMN List exists in the MME for the target tracking area of the UE, the Equivalent PLMN IE is included in the `TAU Accept` message. For more information about Equivalent PLMN, see Selective EPL on page 15.

   The MME includes the `EPS Network Feature Support` IE in the accept message if the IMS-Based Telephony - MMTel feature is activated and the PLMN is configured to support IMS Voice Service or IMS Emergency Service. The `EPS Network Feature Support` IE includes `IMS VoPS` bit. See the Note for information about the `IMS VoPS` bit.

   For more information about IMS Voice Service or IMS Emergency Service, see Features and Functions Management and Configuring MMTel Service.

3. If the GUTI has been reallocated, the UE sends a `TAU Complete` message to the MME.

4. The MME sends a `UE Context Release Command` message to the eNodeB.

5. The eNodeB releases the resources related to the UE and responds with a `UE Context Release Complete` message.

   The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Release Complete` message. For more information, see Massive IoT.

9.1.2 Intra-MME TAU without SGW Relocation

An intra-MME TAU without SGW relocation procedure is performed when the UE moves to a tracking area not included in the TAI list of the UE, and the new tracking area is within the same SGW and MME service areas.

The MME analyzes the GUTI and verifies that it belongs to the same MME.

9.1.2.1 Traffic Case

The intra-MME TAU without SGW relocation procedure is shown in Figure 23 and is described below the figure.

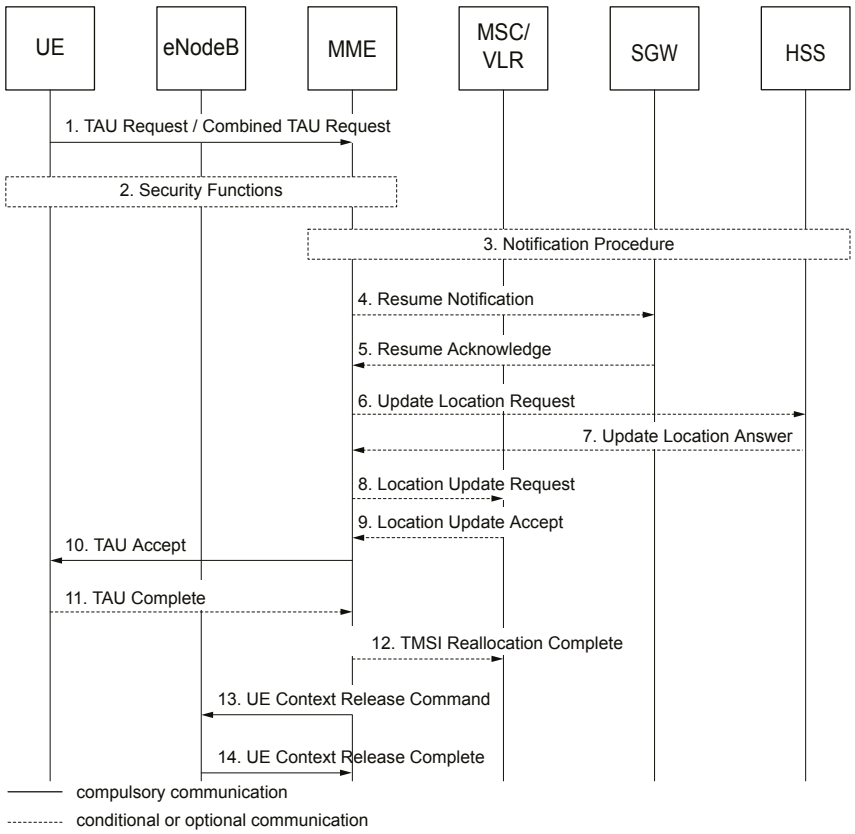


Figure 23 Intra-MME TAU without SGW Relocation Procedure

The following steps describe the intra-MME TAU procedure:

1. The intra-MME TAU procedure is initiated when the MME receives a `TAU Request` message from the UE, indicating a normal TAU.

   The MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the TAU procedure is rejected, see Mobility without Dataflow Rejected on page 76. For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information on IMS Emergency Service, see Configuring MMTel Service.

   The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target tracking area is restricted, non-emergency PDN connections are removed. For more

information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

The UE can also send a `Combined TAU Request` message. For more information on combined procedures, see EPS Support for CS Services.

If the `active` flag or the `signalling active` flag is set in the TAU Request message, the MME initiates EPS bearer re-establishment. For more information on TAU with the `active` flag set, see Intra-MME TAU and Inter-MME TAU with Active Flag Set on page 77. For more information on TAU with `signalling active` flag set, see Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set on page 79.

2. The MME can perform security functions to authenticate the subscriber. A security context is established, and ciphering and integrity protection are negotiated. The IMEI Check procedure can also be performed. For more information on security functions, see Security.

3. If the IMEISV that is received from the UE during the security functions procedure is different from the previous IMEISV, if available, and there is no Update Location Procedure later, the MME initiates a Notification Procedure to the HSS with the updated terminal information. For an unauthenticated UE performing a TAU procedure with an emergency PDN connection, no Notification Procedure is triggered toward the HSS.

4. If the MME detects that the UE is in the suspended status, and no `Modify Bearer Request` message is sent to the SGW, the MME sends a `Resume Notification` message to the SGW to resume the suspended non-GBR bearers for each PDN connection.

5. The SGW responds by sending a `Resume Acknowledge` message to the MME.

6. The MME sends an `Update Location Request` message to inform the HSS to get subscription data if the UE relocates to a different PLMN and the IMSI of the UE is part of the regional subscription feature configuration. The message contains the user state and location information if the `-aanh S6aAllowAdditionalNetLocHss` parameter in modify_s6a command is set to true.

   For an unauthenticated UE performing a TAU request with an emergency PDN connection, no Update Location Request message is sent to the HSS.

7. The HSS sends an `Update Location Answer` message to the MME, acknowledging the new location of the UE. The new MME checks if CSG restrictions apply. If the UE is restricted, the TAU procedure is rejected. The new MME updates the subscription data and sets up a context for the UE.

   If the Location Area has changed, a `Combined TAU Request` message was sent in , and the `PreventCombinedRegistration` parameter is set to false, continue with . Otherwise, continue with .

   For more information about CSG restrictions, see CSG Restrictions on page 131.

8. The MME sends a `Location Update Request` message to the MSC/VLR.
9. The MSC/VLR answers by sending a `Location Update Accept` message to the MME.
10. The MME sends a `TAU Accept` message to the UE. If the time elapsed since last GUTI reallocation is greater than the configured value `MMEGutiReallocationTimeLimit`, or if the UE moves to a different PLMN served by the same MME during Multiple PLMN Support, GUTI reallocation is also performed.

    The MME informs the UE of the supported features, such as IMS Voice Service or IMS Emergency Service, by sending the `EPS Network Feature Support` IE in the `TAU Accept` message. Supported features are based on the configuration of the MME. The `EPS Network Feature Support` IE includes the `IMS VoPS` bit. See the Note for information about the `IMS VoPS` bit.

    For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on how to configure IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).
11. If the GUTI has been reallocated, the UE acknowledges the new GUTI and returns a `TAU Complete` message to the MME.
12. If a `Combined TAU Request` message was sent in , the MME sends a `TMSI Reallocation Complete` message to the MSC/VLR.
13. The MME sends a `UE Context Release Command` message to the eNodeB.
14. The eNodeB releases the resources related to the UE and responds with a `UE Context Release Complete` message.

    The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Release Complete` message. For more information, see Massive IoT.

9.1.3 Intra-MME TAU with SGW Relocation

An intra-MME TAU with SGW relocation procedure is performed when the UE moves to a TA not included in the TAI list of the UE, and the new TA is within the same MME service area, but is served by a new SGW.

The MME analyses the GUTI and verifies that it belongs to the same MME.

9.1.3.1 Traffic Case

The intra-MME TAU with SGW relocation procedure is shown in Figure 24 and is described below the figure.

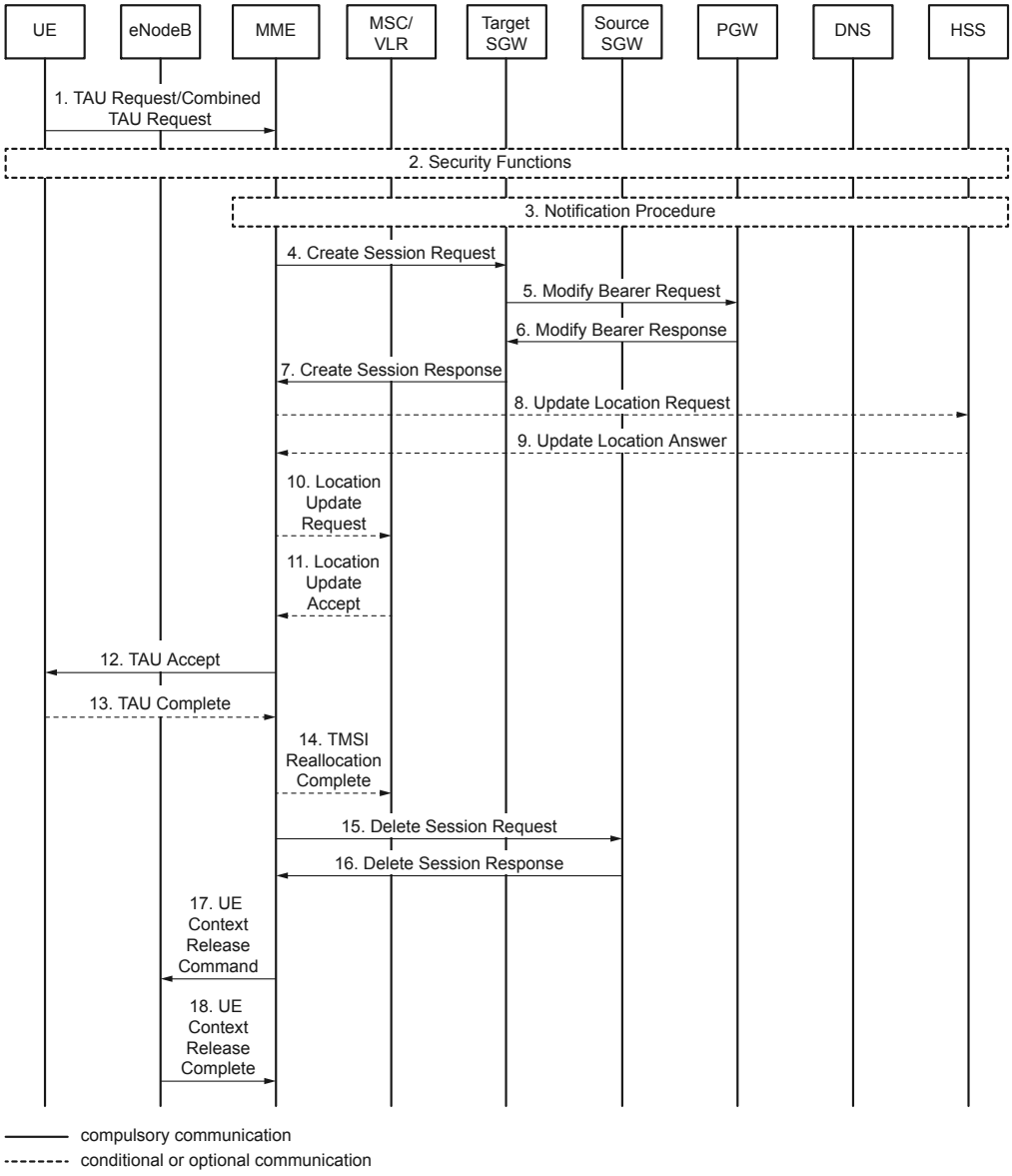


Figure 24

The following steps describe the intra-MME TAU with SGW relocation procedure:

1. The intra-MME TAU procedure is initiated when the MME receives a `TAU Request` message from the UE, indicating a normal TAU.

   The MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the TAU procedure is rejected, see Mobility without Dataflow Rejected on page 76. For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming

Restrictions, see Roaming Restrictions on page 123. For more information on IMS Emergency Service, see Configuring MMTel Service.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target TA is restricted, non-emergency PDN connections are removed. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

The UE can also send a `Combined TAU Request` message. For more information on combined procedures, see EPS Support for CS Services.

If the `active` flag or `signalling active` flag is set in the TAU Request message, the MME initiates EPS bearer re-establishment. For more information on TAU with the `active` flag set, see Intra-MME TAU and Inter-MME TAU with Active Flag Set on page 77. For more information on TAU with `signalling active` flag set, see Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set on page 79.

2. The MME can perform security functions to authenticate the subscriber. A security context is established, and ciphering and integrity protection are negotiated. The IMEI Check procedure can also be performed. For more information on security functions, see Security.

3. If the IMEISV that is received from the UE during the security functions procedure is different from the previous IMEISV, if available, and there is no Update Location Procedure later, the MME initiates a Notification Procedure to the HSS with the updated terminal information. For an unauthenticated UE performing a TAU procedure with an emergency PDN connection, no Notification Procedure is triggered toward the HSS.

4. The MME sends a `Create Session Request` message to the target SGW. One `Create Session Request` message is sent for each PDN connection. The target SGW begins to establish PDN connections. PDN connections that cannot be established are removed together with the bearers related to them. If all default bearers fail to be established in the SGW, the TAU is rejected.

5. The target SGW sends a `Modify Bearer Request` to the PGW.

6. The PGW returns a `Modify Bearer Response` message to the target SGW.

7. The target SGW sends a `Create Session Response` message to the MME.

8. The MME sends an `Update Location Request` message to inform the HSS to get subscription data if the UE relocates to a different PLMN and the IMSI of the UE is part of the regional subscription feature configuration. The message contains the user state and location information, if the `-aanh S6aAllowAdditionalNetLocHss` parameter in modify_s6a command is set to true.

   For an unauthenticated UE performing a TAU request with an emergency PDN connection, no Update Location Request message is sent to the HSS.

9. The HSS sends an `Update Location Answer` message to the MME, acknowledging the new location of the UE. The new MME checks if CSG restrictions apply. If the UE is restricted, the TAU procedure is rejected. The new MME updates subscription data and sets up a context for the UE.

   If the Location Area has changed, a `Combined TAU Request` message was sent in , and the `PreventCombinedRegistration` parameter is set to false, continue with . Otherwise, continue with .

   For more information about CSG restrictions, see CSG Restrictions on page 131.

10. The MME sends a `Location Update Request` message to the MSC/VLR.

11. The MSC/VLR answers by sending a `Location Update Accept` message to the MME.

12. The MME sends a `TAU Accept` message to the UE. The MME also includes an EPS bearer context status IE in the `TAU Accept` message, indicating which EPS bearer contexts are active in the MME.

    If the time elapsed since last GUTI reallocation is greater than the configured value `MMEGutiReallocationTimeLimit`, or if the UE moves to a different PLMN served by the same MME for Multiple PLMN Support, GUTI reallocation is also performed.

    The MME informs the UE of supported features, such as IMS Voice Service or IMS Emergency Service, by sending the `EPS Network Feature Support` IE in the `TAU Accept` message. Supported features are based on the configuration of the MME. The `EPS Network Feature Support` IE includes `IMS VoPS` bit. See the Note for information about the `IMS VoPS` bit.

    For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).

13. If the GUTI has been reallocated, the UE acknowledges the new GUTI and returns a `TAU Complete` message to the MME.

14. If a `Combined TAU Request` message was sent in , the MME sends a `TMSI Reallocation Complete` message to the MSC/VLR.

15. The MME sends a `Delete Session Request` message to the source SGW.

16. The source SGW responds to the MME with a `Delete Session Response` message.

17. The MME sends a `UE Context Release Command` message to the eNodeB.

18. The eNodeB releases the resources related to the UE and responds with a `UE Context Release Complete` message.

The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Release Complete` message. For more information, see Massive IoT.

9.2 Mobility between MME Service Areas

UE-initiated mobility management procedures are also performed when a UE in ECM-IDLE mode moves to a new MME service area. In this case, the MME is reselected.

If a UE supporting EMM-REGISTERED without PDN Connection initiates the inter-MME TAU procedure and the `Context Response` message received from the source MME does not include any PDN connections, the target MME handles the procedure without the session part.

9.2.1 Inter-MME TAU without SGW Relocation

An inter-MME TAU procedure without SGW relocation is performed when the UE moves to a TA not included in its TAI list, and the new TA is within the same SGW service area, but is served by a new MME.

9.2.1.1 Traffic Case

The inter-MME TAU without SGW relocation procedure is shown in Figure 25 and is described below the figure.

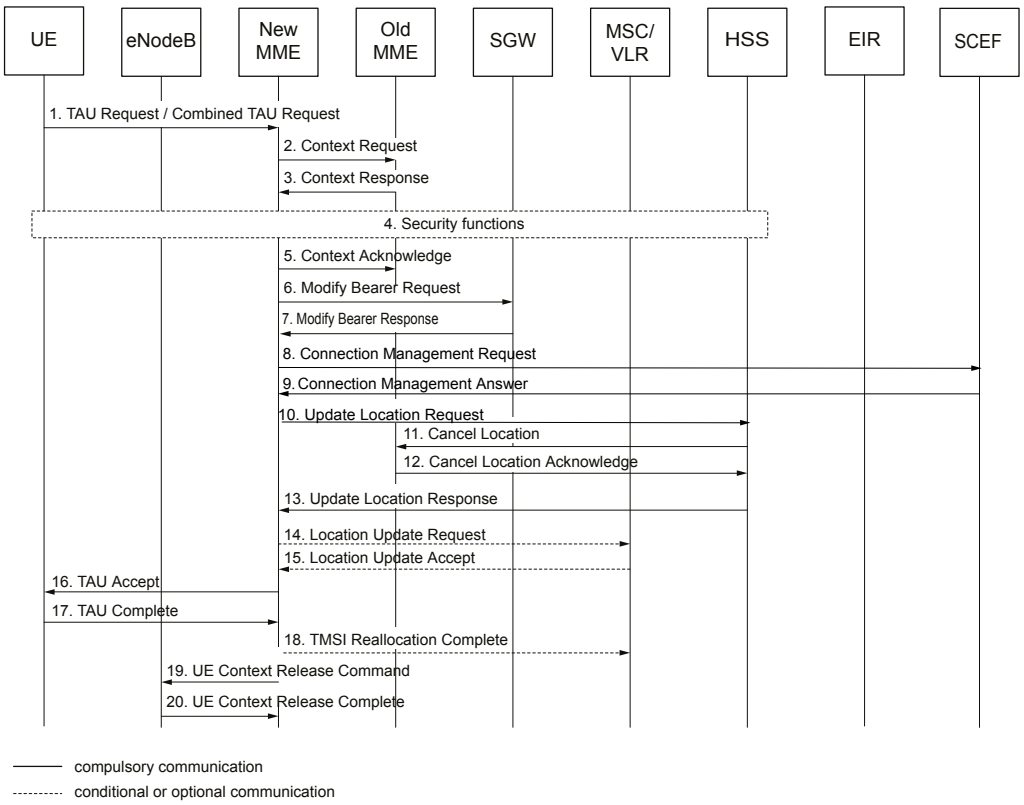


Figure 25 Inter-MME TAU without SGW Relocation Procedure

The following steps describe the inter-MME TAU without SGW relocation procedure:

1. The UE initiates the TAU procedure by sending a `TAU Request` to the new MME through the eNodeB. The MME performs a static selection or a DNS query to find the IP address of the old MME, depending on the configuration. For detailed information about the static selection, see Static and DNS-based SGSN or MME Selection on page 116. `TAU Request` messages that indicate emergency are prioritized if there is a resource limitation.

   The UE can also initiate an inter-MME TAU procedure by sending a `Combined TAU Request` message. For more information about combined procedures, see EPS Support for CS Services.

   If the `active` flag is set in the TAU Request message, the MME initiates EPS bearer re-establishment. For more information on TAU with the `active` flag set, see Intra-MME TAU and Inter-MME TAU with Active Flag Set on page 77. For more information on TAU with `signalling active` flag set, see Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set on page 79.

2. The new MME sends a `Context Request` message to the old MME to retrieve the UE information. The `Context Request` message includes the complete `TAU Request` message and the old GUTI from the UE.

If the licensed feature Data over NAS is activated, the CIoT Optimization Support Indication IE is included in the Context Request message. The flags can be set in the CIoT Optimization Support Indication IE as the following:

- If the UE supports EMM-REGISTERED without PDN connection, the flag AWOPDN, Attach without PDN Support Indication, is set in the IE.
- If the licensed feature DoNAS Non-IP over SGi is activated, the flag SGNIPDN, SGi Non IP PDN Support Indication, is set in the IE.
- If the license features DoNAS, PDN type Non-IP and DoNAS Non-IP over SCEF are activated, the flag SCNIPDN, SCEF Non IP PDN Support Indication, is set in the IE.

3. The old MME verifies the UE based on the information in the TAU Request message and sends a Context Response message containing the Mobility Management and EPS bearer contexts to the new MME. The old MME can be configured to send or not to send an emergency PDN connection if the new MME is in a different PLMN.

   Based on the CIoT EPS Optimization support indication in the Context Request message, the old MME sends the PDN connections over SGi or the SCEF PDN connections over T6a, depending on the available support of the new MME. If support for SGNIPDN is not indicated, PDN connections with PDN type Non-IP are not sent in the Context Response message. If support for SCNIPDN is not indicated, SCEF PDN connections are not sent in the Context Response message. The Context Response without any PDN connections are sent only if the support for AWOPDN is indicated in the new MME.

   A Context Response message is sent to the new MME in all cases regardless of whether it contains any PDN connections or not.

   The UE Radio Capability for Paging information can be included in the Context Response message and transferred from the old MME to the new MME. For more information, see Massive IoT.

   The new MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the TAU procedure is rejected, see Mobility without Dataflow Rejected on page 76.For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information on how to configure the MME to send an emergency PDN connection between PLMNs, see Configuring MMTel Service and IMS Emergency Service (CLI).

   The new MME checks if APN Restriction applies. If the APN or APNS contained in the EPS Bearer Context in the Context Response message matches the configured APN blacklist in the new MME, the PDN connection

or connections are deleted towards the SGW after TAU procedure. For more information, see Mobility without Dataflow Rejected on page 76.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target TA is restricted, non-emergency PDN connections are removed. If the new MME does not receive or cannot retain any PDN connections from the old MME, the TAU procedure is rejected. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

If any dedicated bearers are established for the UE, the new MME checks if the licensed feature, Network-initiated Dedicated Bearers, is activated. If the feature is activated, the dedicated bearers are allowed to continue. If the feature is not activated, the existing dedicated bearers are marked to be deleted. For more information, see Features and Functions Management.

4. The new MME can perform security functions to authenticate the subscriber. A security context is established, and ciphering and integrity protection are negotiated. The IMEI Check procedure can also be performed. For more information on security functions, see Security.

5. The new MME sends a `Context Acknowledge` message to the old MME, acknowledging the `Context Response` message and indicating that the SGW does not need to be reselected.

   The old MME starts a 20-second timer. When the 20-second timer expires in the old MME, the subscriber record is deleted in the old MME. If there are PDN connections that were not sent in the `Context Response` message in , the MME initiates the PDN Disconnection procedure for these PDN connections. For more information about the PDN Disconnection procedure, see LTE Session Management.

6. The new MME sends a `Modify Bearer Request` message to the SGW.

7. The SGW returns a `Modify Bearer Response` message to the new MME to acknowledge the request.

8. The new MME sends a `Connection Management Request` message to the SCEF to update T6a connection with action `CONNECTION_UPDATE`.

9. The SCEF sends a `Conncection Management Answer` message to the new MME to acknowledge the request.

10. The new MME sends an `Update Location Request` message to inform the HSS if the MME relocation and to get subscription data. For an unauthenticated UE performing a TAU request with an emergency PDN connection, no `Update Location Request` message is sent to the HSS. The message contains the user state and location information, if the `-aanh S6aAllowAdditionalNetLocHss` parameter in modify_s6a command is set to true.

11. The HSS identifies the old UE location in its database and sends a `Cancel Location` message to the old MME.

12. The old MME sends a `Cancel Location Acknowledge` message to the HSS.

13. The HSS sends an `Update Location Answer` message to the new MME, acknowledging the new location of the UE. The new MME checks if CSG restrictions apply. If the UE is restricted, the TAU procedure is rejected. The new MME updates subscription data and sets up a context for the UE. For more information about CSG restrictions, see CSG Restrictions on page 131

    If the Location Area has changed, a `Combined TAU Request` message was sent in , and the `PreventCombinedRegistration` parameter is set to false, continue with . Otherwise, continue with .

14. The new MME sends a `Location Update Request` message to the MSC/VLR.

15. The MSC/VLR responds with a `Location Update Accept` message.

16. The MME sends a `TAU Accept` message to the UE, including a new GUTI. The UE deactivates all EPS bearer contexts locally that are active in the UE, but that are indicated as inactive in the new MME. Dedicated bearers that were previously marked for deletion are deactivated.

    The MME informs the UE of the supported features, such as IMS Voice Service or IMS Emergency Service, by sending the `EPS Network Feature Support` IE in the `TAU Accept` message. Supported features are based on the configuration of the MME. The `EPS Network Feature Support` IE includes `IMS VoPS` bit. See the Note for information about the `IMS VoPS` bit.

    For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on how to configure IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).

17. The UE acknowledges the new GUTI and returns a `TAU Complete` message to the new MME.

18. If a `Combined TAU Request` message was sent in , the new MME sends a `TMSI Reallocation Complete` message to the MSC/VLR.

19. The new MME sends a `UE Context Release Command` message to the eNodeB.

20. The eNodeB releases the resources related to the UE and responds with a `UE Context Release Complete` message and the UE state changes into ECM-IDLE.

    The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the `UE Context Release Complete` message. For more information, see Massive IoT.

9.2.2 Inter-MME TAU with SGW Relocation

An inter-MME TAU procedure with SGW relocation is performed when the UE moves to a tracking area not included in its TAI list, and the new tracking area is served by a new MME and SGW.

9.2.2.1 Traffic Case

The inter-MME TAU with SGW relocation procedure is shown in Figure 26 and is described below the figure.

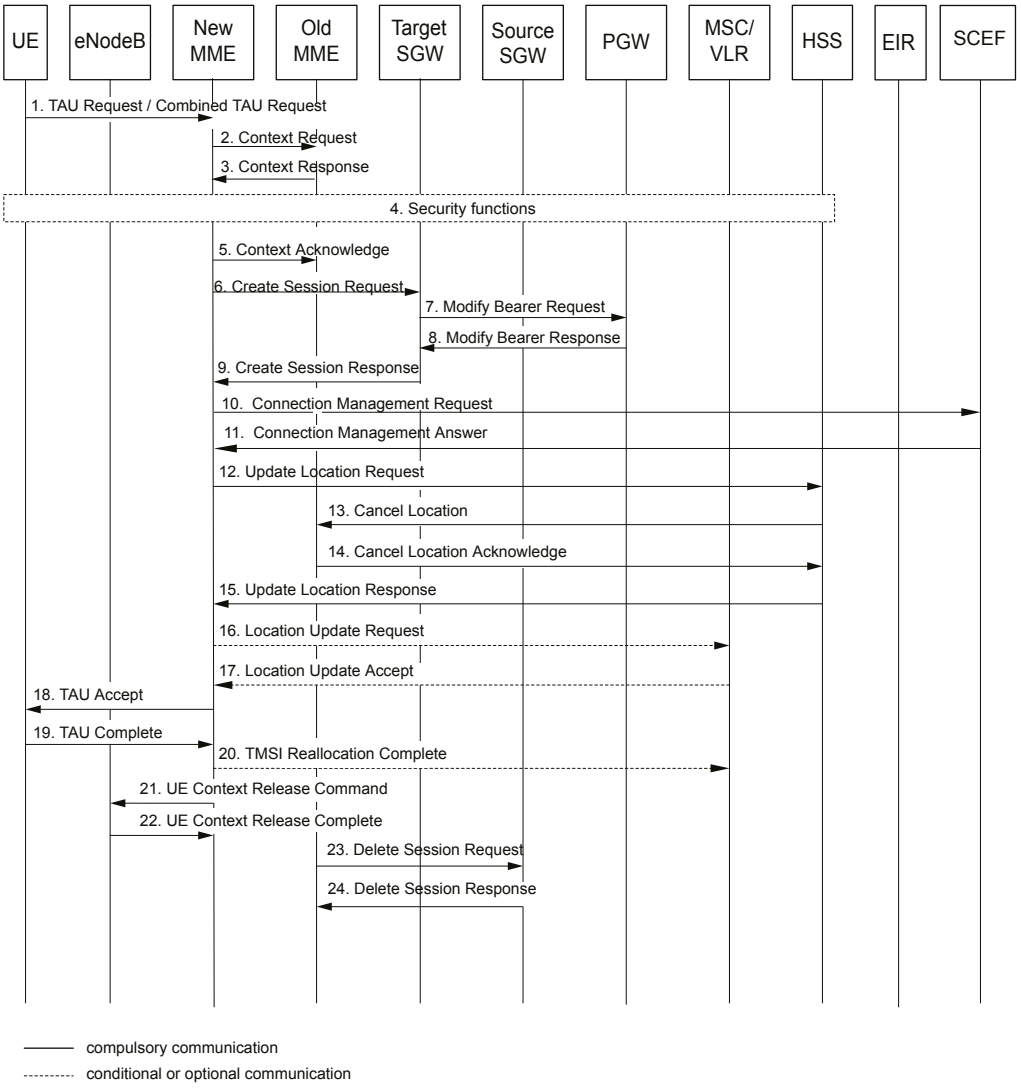


Figure 26 Inter-MME TAU with SGW Relocation Procedure

The following steps describe the inter-MME TAU with SGW relocation procedure:

1. The UE initiates the TAU procedure by sending a `TAU Request` to the new MME through the eNodeB. The MME performs static selection or a DNS query to find the IP address of the old MME, depending on the configuration. For detailed information about the static selection, see Static and DNS-based SGSN or MME Selection on page 116. `TAU Request` messages that indicate emergency are prioritized if there is a resource limitation.

   The UE can also initiate an inter-MME TAU procedure by sending a `Combined TAU Request` message. For more information about combined procedures, see EPS Support for CS Services.

   The new MME checks if the Inter-PLMN Mobility Restriction function applies. If the PLMN is restricted, the TAU procedure is rejected. For more information about Inter-PLMN Mobility Restriction, see Inter-PLMN Mobility Restriction on page 132.

   If the `active` flag is set in the TAU Request message, the MME initiates EPS bearer re-establishment. For more information on TAU with the `active` flag set, see Intra-MME TAU and Inter-MME TAU with Active Flag Set on page 77. For more information on TAU with `signalling active` flag set, see Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set on page 79.

2. The new MME sends a `Context Request` message to the old MME to retrieve the UE information. The `Context Request` message includes the complete `TAU Request` message and the old GUTI from the UE.

   If the licensed feature `Data over NAS` is activated, the `CIoT Optimization Support Indication` IE is included in the `Context Request` message. The flags can be set in the `CIoT Optimization Support Indication` IE as the following:

   - If the UE supports EMM-REGISTERED without PDN connection, the flag `AWOPDN`, Attach without PDN Support Indication, is set in the IE.
   - If the licensed feature `DoNAS Non-IP over SGi` is activated, the flag `SGNIPDN`, SGi Non IP PDN Support Indication, is set in the IE.
   - If the license features `DoNAS, PDN type Non-IP` and `DoNAS Non-IP over SCEF` are activated, the flag `SCNIPDN`, SCEF Non IP PDN Support Indication, is set in the IE.

3. The old MME verifies the UE based on the information in the `TAU Request` message and sends a `Context Response` message containing the Mobility Management and EPS bearer contexts to the new MME. The old MME can be configured to send or not to send an emergency PDN connection if the new MME is in a different PLMN.

   Based on the CIoT EPS Optimization support indication in the `Context Request` message, the old MME sends the PDN connections over SGi or the SCEF PDN connections over T6a, depending on the available support in the new MME. If support for SGNIPDN is not indicated, PDN connections with

PDN type Non-IP are not sent in the `Context Response` message. If support for SCNIPDN is not indicated, SCEF PDN connections are not sent in the `Context Response` message. The Context Response without any PDN connections are sent only if the support for AWOPDN is indicated in the new MME.

A `Context Response` message is sent to the new MME in all cases regardless of whether it contains any PDN connections or not.

The UE Radio Capability for Paging information can be included in the `Context Response` message and transferred from the old MME to the new MME. For more information, see Massive IoT.

The new MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the TAU procedure is rejected, see Mobility without Dataflow Rejected on page 76. For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information on how to configure the MME to send an emergency PDN connection between PLMNs, see Configuring MMTel Service and IMS Emergency Service (CLI).

The new MME checks if APN restriction applies. If the APN or APNS contained in the EPS Bearer Context in the `Context Response` message matches the configured APN blacklist in the new MME, and if all the APNs are blacklisted, the TAU procedure is rejected or accepted based on whether the UE supports EMM-REGISTERED without PDN Connection. For more information, see Mobility without Dataflow Rejected on page 76.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target tracking area is restricted, non-emergency PDN connections are removed. If the new MME does not receive or cannot retain any PDN connections from the old MME, the TAU procedure is rejected. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

If any dedicated bearers are established for the UE, the new MME checks if the licensed feature, Network-initiated Dedicated Bearers, is activated. If the feature is activated, the dedicated bearers are allowed to continue. If the feature is not activated, the existing dedicated bearers are marked to be deleted. For more information, see Features and Functions Management.

4. The new MME can perform security functions to authenticate the subscriber. A security context is established, and ciphering and integrity protection are negotiated. The IMEI Check procedure can also be performed. For more information on security functions, see Security.

5. The new MME sends a `Context Acknowledge` message to the old MME, including an SGW Change Indication, acknowledging the `Context Response` message and indicating that the SGW has been reselected.

The old MME starts a 20-second timer. When the 20-second timer expires in the old MME, the subscriber record is deleted in the old MME, see . If there are PDN connections that were not sent in the `Context Response` message in , the MME initiates the PDN Disconnection procedure for these PDN connections. For more information about the PDN Disconnection procedure, see LTE Session Management.

6. The new MME sends a `Create Session Request` message to the target SGW for each PDN connection. The target SGW begins to establish PDN connections. PDN connections that cannot be established are removed together with the bearers related to them. If all default bearers fail to be established in the SGW, the TAU is rejected.

7. The target SGW assigns one IP address and TEID for each bearer and sends a `Modify Bearer Request` message to the PGW for each PDN connection. The `Modify Bearer Request` message contains the following information for downlink traffic for the accepted EPS Bearers:

   - The SGW IP address and the TEIDs

8. The PGW updates the PGW context field and sends a `Modify Bearer Response` for each `Modify Bearer Request` received in .

9. The target SGW concludes the bearer activation by sending a `Create Session Response` for each `Create Session Request` received in .

10. The new MME sends a `Connection Management Request` message to the SCEF to update the T6a connection with the action `CONNECTION_UPDATE`.

11. The SCEF sends an `Connection Management Answer` message to the new MME to acknowledge the request.

12. The new MME sends an `Update Location Request` message to inform the HSS about the MME relocation and to get subscription data. For an unauthenticated UE performing a TAU request with an emergency PDN connection, no `Update Location Request` message is sent to the HSS. The message contains the user state and the location information if the `-aanh S6aAllowAdditionalNetLocHss` parameter in modify_s6a command is set to true.

13. The HSS identifies the old UE location in the HSS database and sends a `Cancel Location` message to the old MME.

14. The old MME sends a `Cancel Location Acknowledge` message to the HSS.

15. The HSS sends an `Update Location Answer` message to the new MME, acknowledging the new location of the UE. The new MME checks if CSG restrictions apply. If the UE is restricted, the TAU procedure is rejected. The new MME updates the subscription data and sets up a context for the UE. For more information about CSG restrictions, see CSG Restrictions on page 131.

If the Location Area has changed, a Combined TAU Request message was sent in , and the PreventCombinedRegistration parameter is set to false, continue with . Otherwise, continue with .

16. The new MME sends a Location Update Request message to the MSC/VLR.

17. The MSC/VLR responds with a Location Update Accept message.

18. The MME sends a TAU Accept message to the UE, including a new GUTI. The UE deactivates all local EPS bearer contexts that are active in the UE, but that are indicated as inactive in the new MME. Dedicated bearers that were previously marked for deletion are deactivated.

    The MME informs the UE of the supported features, such as IMS Voice Service or IMS Emergency Service, by sending the EPS Network Feature Support IE in the TAU Accept message. Supported features are based on the configuration of the MME. The EPS Network Feature Support IE includes IMS VoPS bit. See the Note for information about the IMS VoPS bit.

    For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on how to configure IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).

19. The UE acknowledges the new GUTI and returns a TAU Complete message to the new MME.

20. If a Combined TAU Request message was sent in , the new MME sends a TMSI Reallocation Complete message to the MSC/VLR.

21. The new MME sends a UE Context Release Command message to the eNodeB.

22. The eNodeB releases the resources related to the UE and responds with a UE Context Release Complete message and the UE state changes into ECM-IDLE.

    The MME stores the Coverage Enhancement related information, if the Coverage Enhancement related information is present in the UE Context Release Complete message. For more information, see Massive IoT.

23. When the 20-second timer that started in expires, the MME sends a Delete Session Request message for each PDN connection sent in the Context Response message in to the source SGW.

24. The source SGW responds to the MME with one Delete Session Response message for each Delete Session Request message in step 21.

9.3 Mobility without Dataflow Rejected

If the `TAU Request` message is not accepted, one of the following happens:

— The TAU procedure is ended without notifying the UE.

— A `TAU Reject` message, including a cause for rejection, is sent to the UE.

If the TAU procedure is rejected based on Diameter S6a errors received from the HSS, a configurable NAS cause code corresponding to the Diameter S6a error code is sent to the UE. For the mapping of Diameter S6a error codes to NAS cause codes, see Diameter S6a Error Code to NAS Cause Code Mapping on page 147.

If some of the dedicated bearers failed to setup in the eNodeB or could not be modified in the SGW, these bearers are deactivated.

If a default bearer failed to setup in the eNodeB or was not modified in the SGW, this particular PDN connection is disconnected. If all default bearers failed to setup in the eNodeB or is not modified in the SGW, the UE is explicitly detached with cause **`Re-attach Required`**.

If all the APN(s) contained in the EPS Bearer Context in the `Context Response` message matches the configured APN blacklist in the new MME, and the UE does not support EMM-REGISTERED without PDN connection, the TAU procedure is rejected. For more information, see APN Resolve and Redirect for LTE Access.

10 Mobility with Dataflow

A UE can request user plane establishment in the following scenarios:

— The UE sets the `active` flag or `signalling active` flag to request EPS bearer re-establishment. For example, TAU with the `active` flag set can be performed in cases where the UE is in the ECM-CONNECTED state and a handover procedure cannot be performed.

— When the UE performs an Intra-MME TAU or an Inter-MME TAU procedure with SGW relocation, the Indirect Data Forwarding Function allows the data delivery if there is buffered payload in the source SGW.

A successful Mobility with Dataflow procedure changes the ECM state to ECM-CONNECTED, allowing the UE to send or receive data or perform signaling. For a description of the ECM-CONNECTED state, see ECM-CONNECTED on page 5.

10.1 Mobility Within and between MME Service Areas

This section describes the intra-MME TAU and the inter-MME TAU procedures with the `active` flag or the `signalling active` flag set.

10.1.1 Intra-MME TAU and Inter-MME TAU with Active Flag Set

The NAS signaling connection is kept when the `active` flag is set in the TAU Request. The additional signaling to the intra-MME TAU and the inter-MME TAU is shown in Figure 24 and described below the figure.

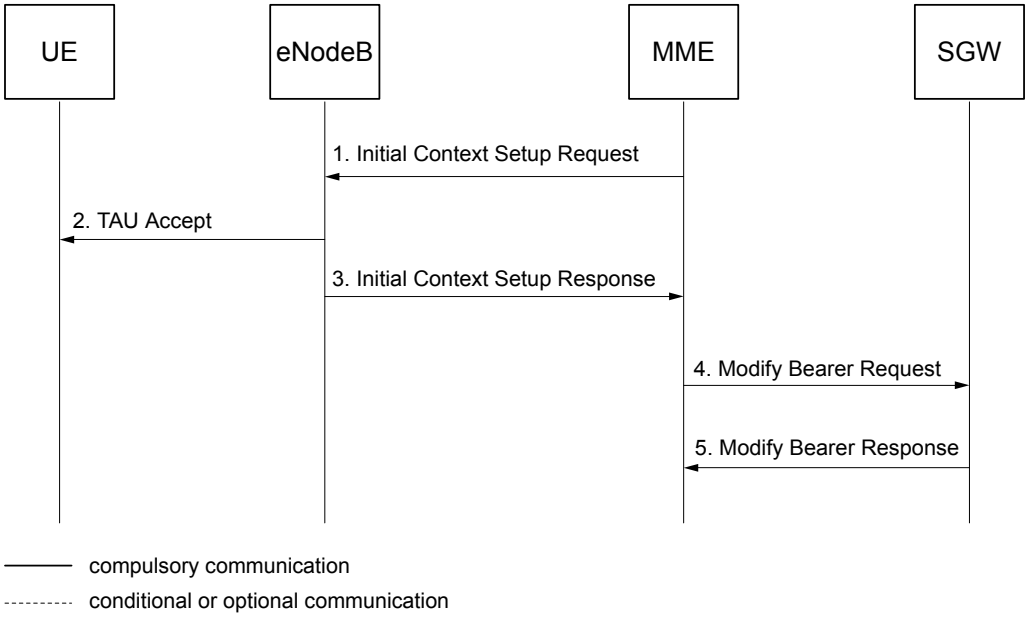


Figure 27 Intra- and Inter-MME TAU with Active Flag Set

The following steps describe the intra- and inter-MME TAU with `active` flag set procedure:

1. The MME sends an `Initial Context Setup Request` message to the eNodeB.
2. The `Initial Context Setup Request` message contains a `TAU Accept` message that the eNodeB forwards to the UE.
3. The eNodeB responds by sending the `Initial Context Setup Response` message to the MME.
4. The MME sends one `Modify Bearer Request` message for each PDN connection to the SGW.

   The `Modify Bearer Request` message contains the following:

   - The identity of the bearers
   - The IP address and TEID for user-plane traffic
   - The ULI, if the parameter `S11UliAlwaysSent` is set to `on`
5. The SGW responds with a `Modify Bearer Response` message to the MME.

Bearers that cannot be set up in the eNodeB or that cannot be updated in the SGW are removed. If default bearers cannot be set up in the eNodeB or be updated in the SGW, the PDN connections associated with them are removed. If no default bearers can be set up, the UE is detached with cause Re-attach Required.

For intra-MME TAU with Active Flag:

If the APN or the APNs contained in the EPS Bearer Context stored for the UE match the configured APN blacklist in the MME, the PDN connection or connections are deleted towards the SGW,the SCEF or both after the TAU procedure. For more information, see APN Resolve and Redirect for LTE Access.

10.1.2 Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set

For UEs using DoNAS, when the `signalling active` flag is set in the TAU Request message, the NAS signaling connection is kept and S11-U connection is established.

Note: Signalling active flag is supported only for UEs using DoNAS. For UEs not using DoNAS, TAU Requests with signalling active flag are rejected.

The additional signaling to the intra-MME TAU and the inter-MME TAU with `signalling active` flag set is shown in Figure 25 and described after Figure 25.

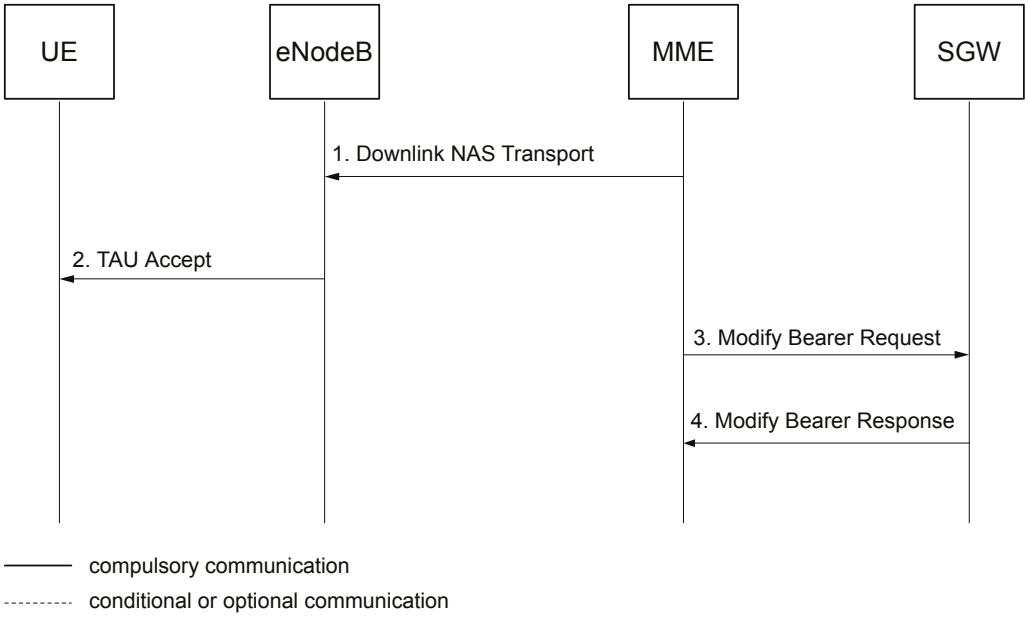


Figure 28 Intra-MME TAU and Inter-MME TAU with Signalling Active Flag Set

The following steps describe the additional signaling for the intra-MME TAU and the inter-MME TAU with `signalling active` flag set procedure:

1. The MME sends a `Downlink NAS Transport` message, which contains the `TAU Accept` message, to the eNodeB.
2. The eNodeB forwards the `TAU Accept` message to the UE.
3. The MME sends one `Modify Bearer Request` message. The `Modify Bearer Request` message contains the following:

- Indication of S11-U tunneling of NAS user data
- The MME S11-GTP-U IP address and the S11-GTP-U F-TEID
- The ULI, if the parameter `S11UliAlwaysSent` is set to `on`

4. The SGW responds with a `Modify Bearer Response` message to the MME.

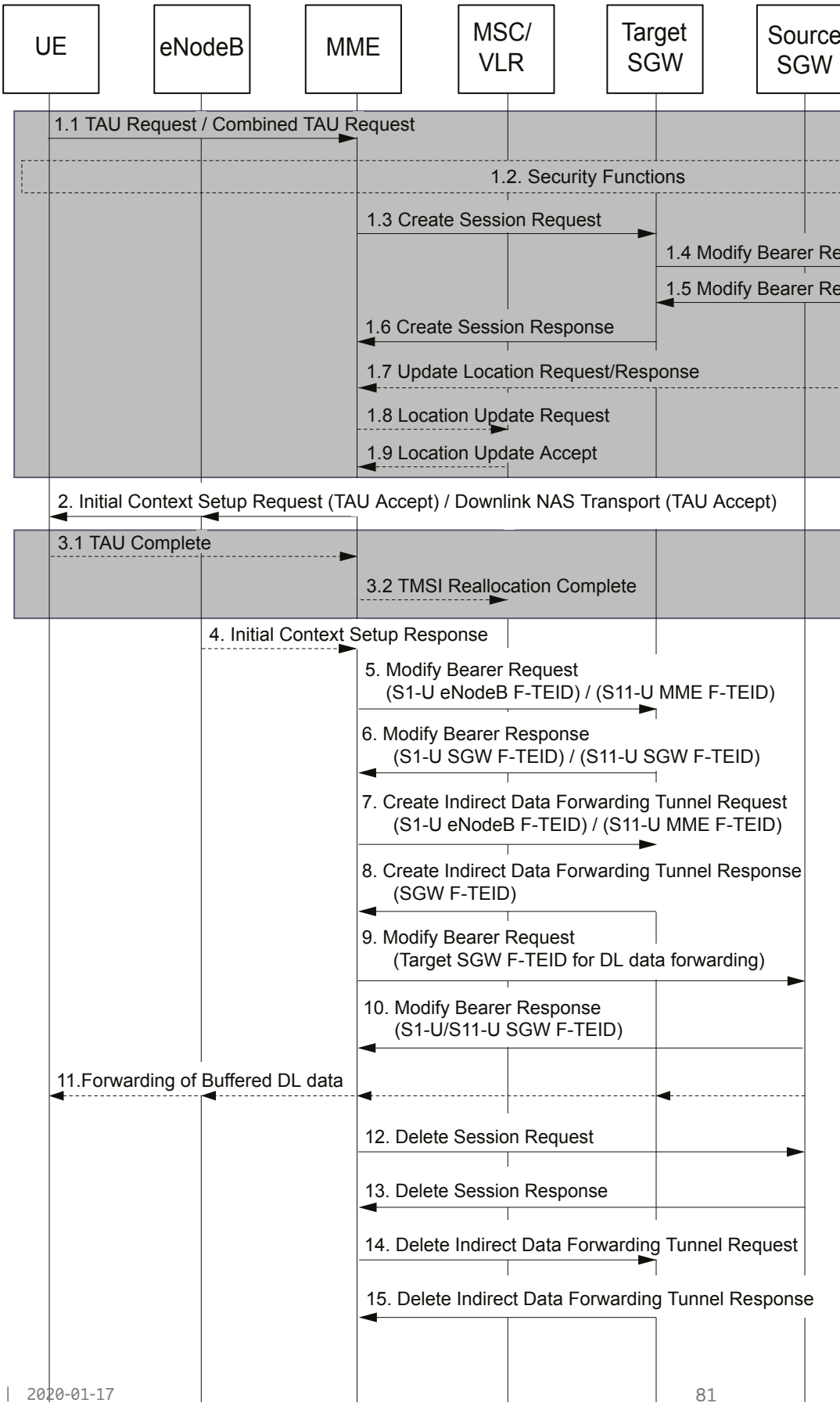
If the default bearer cannot be updated in the SGW, the PDN connection associated with the default bearer is removed and the UE is detached with cause Re-attach Required.

For intra-MME TAU with Signalling Active Flag:

If the APN or the APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, the PDN connection or connections are deleted towards the SGW, theSCEF or both after the TAU procedure. For more information, see APN Resolve and Redirect for LTE Access.

10.1.3 Intra-MME TAU with SGW Relocation and Indirect Data Forwarding

When a UE using eDRX or PSM moves within the same MME service area, resulting in an Intra-MME TAU with SGW Relocation procedure, the Indirect Data Forwarding function allows the data delivery if there is pending payload buffered in the source SGW. The Intra-MME TAU with SGW Relocation and Indirect Data Forwarding function is shown in Figure 29 and described below the figure.



compulsory communication

1. This step includes step 1.1 to step 1.9 from Figure 29.. For more information, see to in Traffic Case on page 62.

2. If S1-U is used, the MME sends an `Initial Context Setup Request` message to the eNodeB. The `Initial Context Setup Request` message contains a `TAU Accept` message that the eNodeB forwards to the UE.

   If S11-U is used, the MME sends a `Downlink NAS Transport` message to the eNodeB. The `Downlink NAS Transport` message contains a `TAU Accept` message that the eNodeB forwards to the UE.

3. This step includes step 3.1 and step 3.2 from Figure 29. For more information, see and in Traffic Case on page 62.

4. The eNodeB responds by sending the `Initial Context Setup Response` message with the S1-U eNodeB F-TEID to the MME.

   This step is only applicable for S1-U.

5. If S1-U is used, the MME sends a `Modify Bearer Request` message containing the S1-U eNodeB F-TEID to the target SGW.

   If S11-U is used, the MME sends a `Modify Bearer Request` message containing the S11-U MME F-TEID to the target SGW.

6. If S1-U is used, the target SGW responds with a `Modify Bearer Response` message containing the S1-U SGW F-TEID to the MME.

   If S11-U is used, the target SGW responds with a `Modify Bearer Response` message containing the S11-U SGW F-TEID to the MME.

7. If S1-U is used, the MME sends a `Create Indirect Data Forwarding Tunnel Request` message containing the S1-U eNodeB F-TEID to the target SGW.

   If S11-U is used, the MME sends a `Create Indirect Data Forwarding Tunnel Request` message containing the S11-U MME F-TEID to the target SGW.

8. The target SGW responds with a `Create Indirect Data Forwarding Tunnel Response` message containing the SGW F-TEID to the MME.

9. The MME sends a `Modify Bearer Request` message containing the target SGW F-TEID for downlink data forwarding to the source SGW.

10. If S1-U is used, the source SGW responds with a `Modify Bearer Response` message containing the S1-U SGW F-TEID to the MME.

    If S11-U is used, the source SGW responds with a `Modify Bearer Response` message containing the S11-U SGW F-TEID to the MME.

11. If S1-U is used, after receiving the buffered downlink data forwarded by the source SGW, the target SGW sends the data to the eNodeB, and then the eNodeB sends the data to the UE.

    If S11-U is used, after receiving the buffered downlink data forwarded by the source SGW, the target SGW sends the data to the MME, and then the MME sends the data to the UE over the NAS Interface.

12. The MME sends a `Delete Session Request` message to the source SGW.

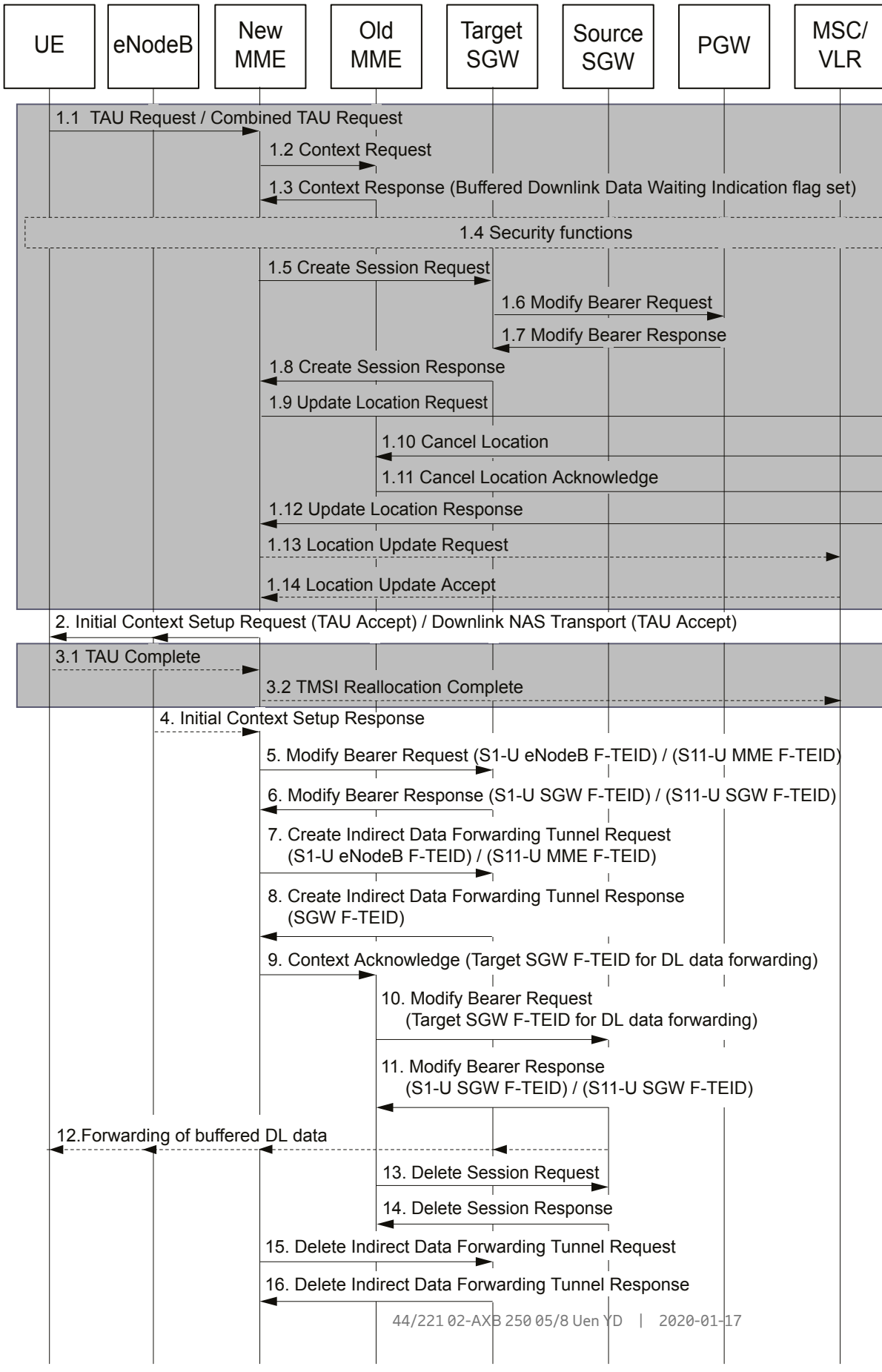
13. The source SGW responds with a `Delete Session Response` message to the MME.

14. The MME sends a `Delete Indirect Data Forwarding Tunnel Request` message to the target SGW.

15. The target SGW sends a `Delete Indirect Data Forwarding Tunnel Response` message to the MME.

10.1.4 Inter-MME TAU with SGW Relocation and Indirect Data Forwarding

When a UE using eDRX or PSM moves between Tracking Areas, resulting in an Inter-MME TAU with SGW Relocation procedure, the Indirect Data Forwarding function allows the data delivery if there is pending payload buffered in the source SGW. The Inter-MME TAU with SGW Relocation and Indirect Data Forwarding function is shown in Figure 30 and described below the figure.


UE
eNodeB
New MME
Old MME
Target SGW
Source SGW
PGW
MSC/ VLR
1.1 TAU Request / Combined TAU Request
1.2 Context Request
1.3 Context Response (Buffered Downlink Data Waiting Indication flag set)
1.4 Security functions
1.5 Create Session Request
1.6 Modify Bearer Request
1.7 Modify Bearer Response
1.8 Create Session Response
1.9 Update Location Request
1.10 Cancel Location
1.11 Cancel Location Acknowledge
1.12 Update Location Response
1.13 Location Update Request
1.14 Location Update Accept
2. Initial Context Setup Request (TAU Accept) / Downlink NAS Transport (TAU Accept)
3.1 TAU Complete
3.2 TMSI Reallocation Complete
4. Initial Context Setup Response
5. Modify Bearer Request (S1-U eNodeB F-TEID) / (S11-U MME F-TEID)
6. Modify Bearer Response (S1-U SGW F-TEID) / (S11-U SGW F-TEID)
7. Create Indirect Data Forwarding Tunnel Request (S1-U eNodeB F-TEID) / (S11-U MME F-TEID)
8. Create Indirect Data Forwarding Tunnel Response (SGW F-TEID)
9. Context Acknowledge (Target SGW F-TEID for DL data forwarding)
10. Modify Bearer Request (Target SGW F-TEID for DL data forwarding)
11. Modify Bearer Response (S1-U SGW F-TEID) / (S11-U SGW F-TEID)
12.Forwarding of buffered DL data
13. Delete Session Request
14. Delete Session Response
15. Delete Indirect Data Forwarding Tunnel Request
16. Delete Indirect Data Forwarding Tunnel Response

1. This step includes step 1.1 to step 1.14 from Figure 30. For more information, see to in Traffic Case on page 71.

   The Indirect Data Forwarding function in step 1.3 is enabled only if the Buffered Downlink Data Waiting Indication (BDWI) flag is set as below:

   If there is downlink data buffered in the source SGW, the old MME sends a `Context Response` message containing the BDWI flag to the new MME. The old MME starts the `T3ResponseAcknowledgeContext` timer and the additional `T3AdditionalValueForAcknowledgeContext` timer to wait for the `Context Acknowledge` message from the new MME, see .

   For more information, see in Traffic Case on page 71.

2. If S1-U is used, the new MME sends an `Initial Context Setup Request` message to the eNodeB. The `Initial Context Setup Request` message contains a `TAU Accept` message that the eNodeB forwards to the UE.

   If S11-U is used, the new MME sends a `Downlink NAS Transport` message to the eNodeB. The `Downlink NAS Transport` message contains a `TAU Accept` message that the eNodeB forwards to the UE.

3. This step includes step 3.1 and step 3.2 from Figure 30. For more information, see and in Traffic Case.

4. The eNodeB responds by sending the `Initial Context Setup Response` message with the S1-U eNodeB F-TEID to the new MME.

   This step is only applicable for S1-U.

5. If S1-U is used, the new MME sends a `Modify Bearer Request` message containing the S1-U eNodeB F-TEID to the target SGW.

   If S11-U is used, the new MME sends a `Modify Bearer Request` message containing the S11-U MME F-TEID to the target SGW.

6. If S1-U is used, the target SGW responds with a `Modify Bearer Response` message containing the S1-U SGW F-TEID to the new MME.

   If S11-U is used, the target SGW responds with a `Modify Bearer Response` message containing the S11-U SGW F-TEID to the new MME.

7. If S1-U is used, the new MME sends a `Create Indirect Data Forwarding Tunnel Request` message containing the S1-U eNodeB F-TEID to the target SGW.

   If S11-U is used, the new MME sends a `Create Indirect Data Forwarding Tunnel Request` message containing the S11-U MME F-TEID to the target SGW.

8. The target SGW responds with a `Create Indirect Data Forwarding Tunnel Response` message containing the SGW F-TEID to the new MME.

The new MME starts the TDeleteIDFTunnel timer.

9. The new MME sends a Context Acknowledge message containing the target SGW F-TEID for downlink data forwarding to the old MME. After receiving the Context Acknowledge message, the old MME stops the T3ResponseAcknowledgeContext timer and the T3AdditionalValueForAcknowledgeContext timer started in , and starts a 20-second timer.

   When the 20-second timer expires in the old MME, the subscriber record is deleted in the old MME, see .

10. The old MME sends a Modify Bearer Request message containing the target SGW F-TEID for downlink data forwarding to the source SGW.

11. If S1-U is used, the source SGW responds with a Modify Bearer Response message containing the S1-U SGW F-TEID to the old MME.

    If S11-U is used, the source SGW responds with a Modify Bearer Response message containing the S11-U SGW F-TEID to the old MME.

12. If S1-U is used, after receiving the buffered downlink data forwarded by the source SGW, the target SGW sends the data to the eNodeB, and then the eNodeB sends the data to the UE.

    If S11-U is used, after receiving the buffered downlink data forwarded by the source SGW, the target SGW sends the data to the new MME, and then the new MME sends the data to the UE over the NAS Interface.

13. When the 20-second timer that started in expires, the old MME sends a Delete Session Request message to the source SGW.

14. The source SGW responds with a Delete Session Response message to the old MME.

15. When the TDeleteIDFTunnel timer that started in expires, the new MME sends a Delete Indirect Data Forwarding Tunnel Request message to the target SGW.

16. The target SGW sends a Delete Indirect Data Forwarding Tunnel Response message to the new MME.

11 Mobility with Seamless Dataflow

When the UE moves within a tracking area or between tracking areas while there are ongoing data sessions and the RAN detects the move before the UE has initiated a TAU procedure, the RAN initiates a handover procedure between the eNodeBs to avoid service interruption. The RAN also initiates a handover in case there is insufficient radio coverage. The UE is in the EMM-REGISTERED and the ECM-CONNECTED states.

Handover over the X2 interface is preferred, and occurs if there is an X2 interface between the eNodeBs. For more information, see Mobility with X2-Based Handover on page 87.

In case there is no X2 interface between the eNodeBs, a handover is performed over the S1 interface. For more information, see Mobility with S1-Based Handover on page 95.

The MME handles handover interference, which can happen between X2-based or S1-based handovers and MME-originated signaling. For more information on handover procedures, see SoC with 3GPP TS 23.401.

11.1 Mobility with X2-Based Handover

An X2-based handover procedure occurs when the UE moves between two cells, and an X2 interface exists between the source eNodeB and the target eNodeB. An X2-based handover procedure is initiated by the RAN and is divided into three phases:

— Handover preparation

— Execution

— Completion

In the first two phases, the source eNodeB and target eNodeB have already prepared and executed the handover through control signaling over the X2 interface before informing the MME that the handover has taken place. The third phase is described in the X2-based handover without SGW relocation procedure, see Intra-MME X2-Based Handover without SGW Relocation on page 88, and X2-based handover with SGW relocation procedure, see Intra-MME X2-Based Handover with SGW Relocation on page 91.

For more information about CSG restrictions, see CSG Restrictions on page 131.

Note: Handover to a CSG cell in another PLMN always fails.

11.1.1 Intra-MME X2-Based Handover without SGW Relocation

An intra-MME X2-based handover without SGW relocation procedure is performed when the UE moves between cells within the same MME and SGW serving areas.

11.1.1.1 Traffic Case

The intra-MME X2-based handover without SGW relocation procedure is shown in Figure 31 and described below the figure.

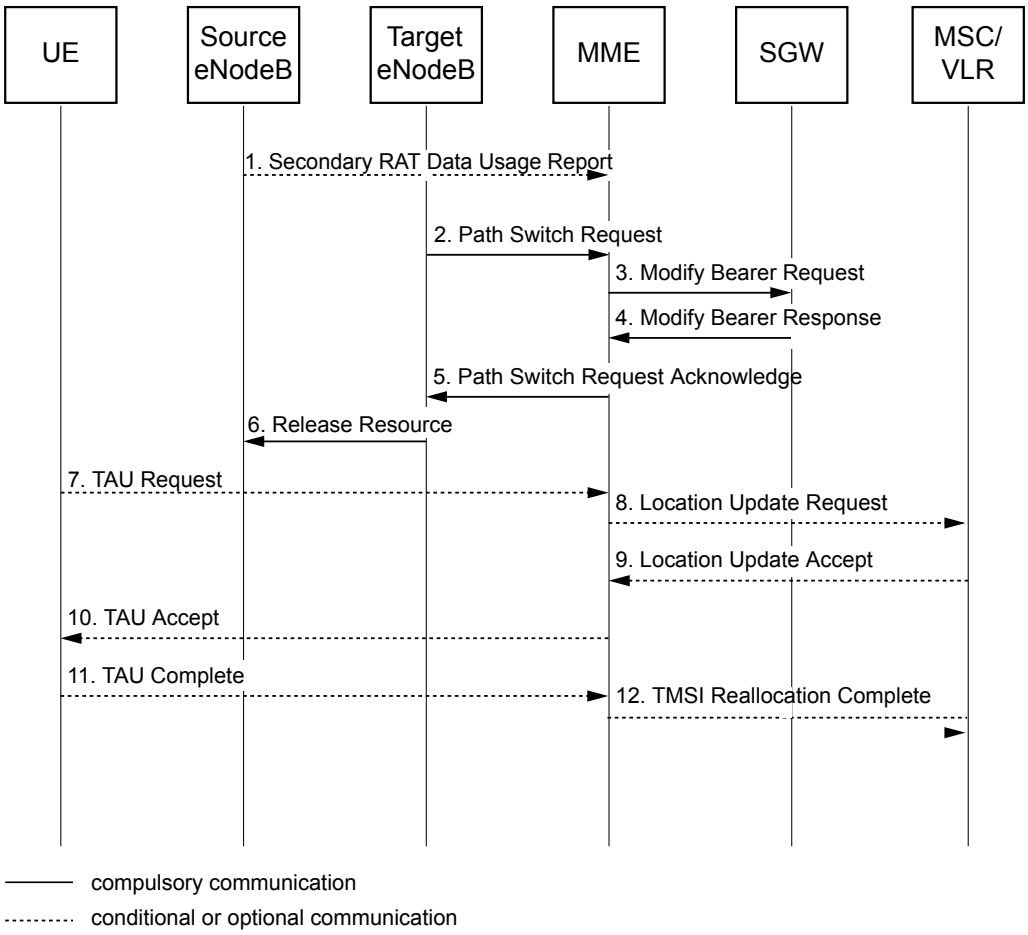


Figure 31 Intra-MME X2-Based Handover without SGW Relocation Procedure

The following steps describe the intra-MME X2-based handover without SGW relocation procedure:

1. If the NR Usage Data Reporting feature is activated, the eNodeB can send the `Secondary RAT Data Usage Report` message, which contains the `Secondary RAT Usage Report List` IE and `Handover Flag` IE.

2. The target eNodeB sends a `Path Switch Request` message to inform the MME that the UE has changed eNodeBs. This message contains a list of EPS bearers, eNodeB IP addresses, and TEIDs. The MME does the following:

   - Validates the information
   - Releases the connection to the source eNodeB implicitly

   If the tracking area has changed, the MME checks if access restrictions or roaming restrictions apply. The MME also checks if CSG restrictions apply. If the UE is restricted, the X2-Based Handover fails, see Failure in the X2-Based Handover without SGW Relocation on page 91.For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

   The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target tracking area is restricted, non-emergency PDN connections are removed. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service.

   Note: If the UE triggers a resume procedure by including the RRC resume cause in the `Path Switch Request` message, the connection with the UE can be resumed using User Plane CIoT EPS optimization. For more information, see Connection Resume Procedure.

   If all the APN or APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, a `Path Switch Request Failure` is sent to the target eNodeB. For more information, see APN Resolve and Redirect for LTE Access.

3. The MME sends a `Modify Bearer Request` message to the SGW for each PDN connection. The `Modify Bearer Request` message contains the following information for the accepted EPS bearers:

   - The eNodeB IP addresses and the TEIDs from the target eNodeB

   If the NR Usage Data Reporting feature is activated and the MME has received the `Secondary RAT Usage Report List` IE from the eNodeB, the MME includes the `Secondary RAT Usage Data Report` IE.

4. The SGW starts sending downlink packets to the target eNodeB, and also sends a `Modify Bearer Response` message to the MME.

5. The MME confirms the handover by sending a `Path Switch Request Acknowledge` message to the target eNodeB. If the Aggregated Maximum Bit Rate of the UE (UE-AMBR) is changed, the MME provides the updated value to the target eNodeB in the `Path Switch Request Acknowledge` message. This message can also contain the EPS bearers that failed to be

established. The MME releases the failed dedicated bearers by triggering the Bearer Release procedure in the SGW. Failed PDN connections are removed through the SGW.

If the ErabToBeSwitchedInUplinkListAlwaysIncluded parameter is set to true, the Path Switch Request Acknowledge message also contains the SGW IP addresses and the TEIDs for uplink traffic.

6. The successful handover triggers the target eNodeB to send a Release Resources message to the source eNodeB. EPS bearers in source eNodeB are released.

7. If the UE moves to a tracking area not included in the TAI list of the UE, the MME receives a TAU Request message from the UE.

   The UE can also send a Combined TAU Request message. If the Location Area has changed, a Combined TAU Request message is sent, and the PreventCombinedRegistration parameter is set to false, continue with . Otherwise, continue with .

8. The MME sends a Location Update Request message to the MSC/VLR.

9. The MSC/VLR responds by sending a Location Update Accept message to the MME.

10. The MME sends a TAU Accept message encapsulated in an S1-AP Downlink NAS Transport message to the UE. If the time elapsed since last GUTI reallocation is greater than the configured value MMEGutiReallocationTimeLimit, or if the UE moves to a different PLMN served by the same MME for Multiple PLMN Support, GUTI reallocation is performed.

    The MME informs the UE of the supported features, such as IMS Voice Service or IMS Emergency Service by sending the EPS Network Feature Support IE in the Attach Accept message. Supported features are based on the configuration of the MME. The EPS Network Feature Support IE includes IMS VoPS bit. See the Note for information about the IMS VoPS bit.

    For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on how to configure IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).

11. If the GUTI has been reallocated, the UE sends a TAU Complete message to the MME.

12. If the TAU Request message in was a Combined TAU Request, the MME sends a TMSI Reallocation Complete message to the MSC/VLR.

11.1.1.2 Failure in the X2-Based Handover without SGW Relocation

The following are examples of when `Path Switch Request Failure` messages are sent to the target eNodeB:

— No default bearers were set up in the target eNodeB

— All `Modify Bearer Request` messages sent to the SGW are unsuccessful, that is, no default bearers can be modified in the SGW

— Failure in the X2-based handover procedure caused by roaming restrictions

The MME sends the `Path Switch Request Failure` message to the target eNodeB if the MME cannot determine the specific UE.

If the X2-based handover procedure fails because of roaming restrictions, the MME sends a `Path Switch Request Failure` message to the target eNodeB with the default cause code `Handover failure in Target EPC/eNodeB or Target System`. The MME sends a `Detach Request` message with an operator-configured cause code between #11 - #15 to the UE.

11.1.2 Intra-MME X2-Based Handover with SGW Relocation

An intra-MME X2-based handover with SGW relocation procedure is performed when the UE moves between cells within the same MME service area, but the cells are served by different SGWs.

A prerequisite for this procedure is that there must be IP connectivity between the target eNodeB and the source SGW. If there is no IP connectivity, an S1-based handover procedure is performed.

11.1.2.1 Traffic Case

The Intra-MME X2-based handover with SGW relocation procedure is shown in Figure 32 and is described below the figure.

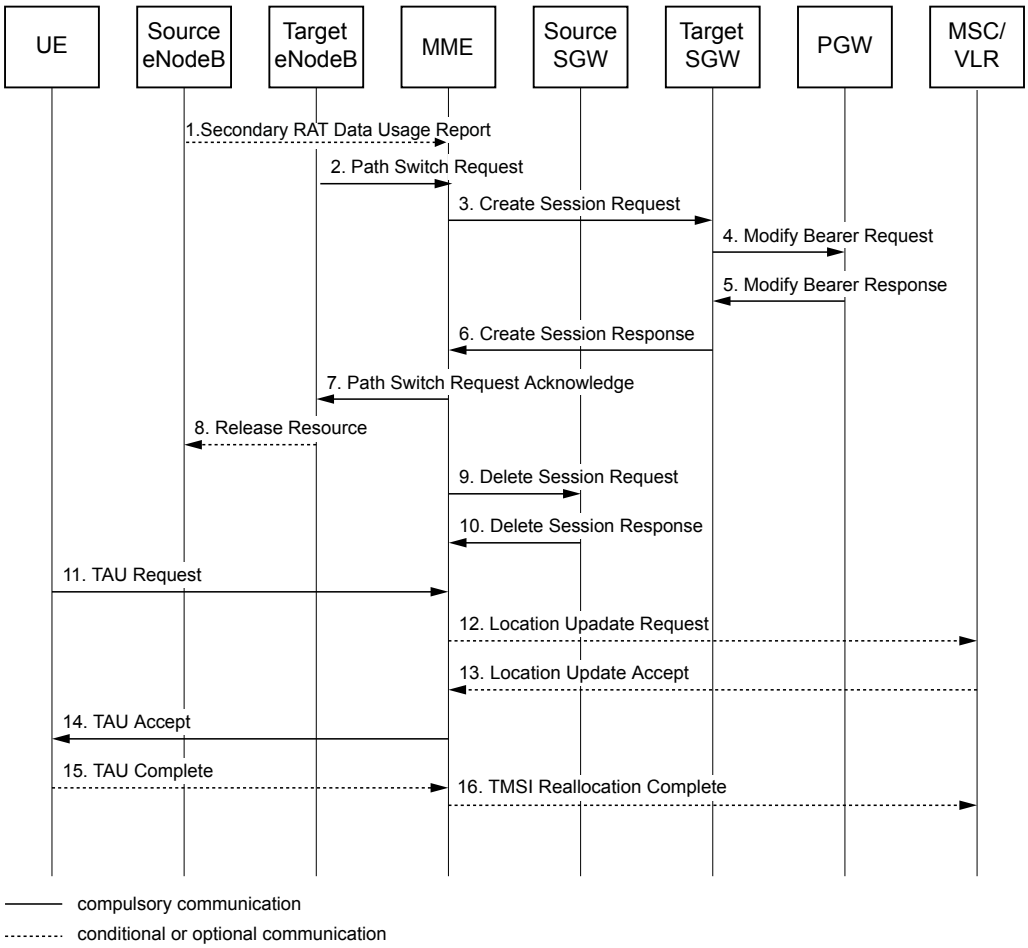


Figure 32 Intra-MME X2-Based Handover with SGW Relocation Procedure

The following steps describe the intra-MME X2-based handover with SGW relocation procedure:

1. If the NR Usage Data Reporting feature is activated, the eNodeB can send the `Secondary RAT Data Usage Report` message which contains the `Secondary RAT usage report list` IE and `Handover Flag` IE.

2. The target eNodeB sends a `Path Switch Request` message to inform the MME that the UE has changed eNodeBs. This message contains a list of EPS bearers, eNodeB IP addresses, and TEIDs for user-plane traffic. The MME performs the following:

   - Validates the information
   - Determines that the SGW needs to be relocated
   - Selects a new SGW
   - Releases the connection to the source eNodeB implicitly

If the tracking area has changed, the MME checks if access restrictions or roaming restrictions apply. The MME also checks if CSG restrictions apply. If the UE is restricted, the X2-Based Handover fails, see Failure in the X2-Based Handover with SGW Relocation on page 95. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target tracking area is restricted, non-emergency PDN connections are removed. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service.

Note: If the UE triggers a resume procedure by including the RRC resume cause in the `Path Switch Request` message, then connection with the UE can be resumed using User Plane CIoT EPS optimization. For more information, see Connection Resume Procedure.

If the APN(s) contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, a `Path Switch Request Failure` is sent to the target eNodeB. For more information, see APN Resolve and Redirect for LTE Access.

3. The MME sends one `Create Session Request` message to the target SGW for each of the remaining PDN connections. The `Create Session Request` message contains the following:

   - The PGW IP addresses and TEIDs for uplink traffic
   - The eNodeB IP addresses and TEIDs for downlink traffic

   If the NR Usage Data Reporting feature is activated and the MME has received the `Secondary RAT usage report list` IE from the eNodeB, the MME includes the `Secondary RAT usage data report` IE.

4. The target SGW assigns one IP address and TEID for each bearer and sends a `Modify Bearer Request` message to the PGW for each PDN connection. The `Modify Bearer Request` message contains the following information for downlink traffic for the accepted EPS Bearers:

   - The SGW IP addresses and TEIDs

5. The PGW updates its context field and sends a `Modify Bearer Response` message to the target SGW.

6. The target SGW sends a `Create Session Response` message to the MME, containing the following information for uplink user-plane traffic:

   - SGW IP addresses and TEIDs

The MME releases the failed dedicated bearers by triggering the bearer release procedure in the SGW. Failed PDN connections are removed through the SGW. The MME starts a timer for the release of bearers.

7. The MME confirms the handover by sending a `Path Switch Request Acknowledge` message to the target eNodeB, containing the following information for uplink traffic:

   - SGW IP addresses and TEIDs

   If the UE-AMBR is changed, the MME provides the updated value to the target eNodeB in this message. This message also contains the EPS bearers that failed to establish.

8. The successful handover triggers the target eNodeB to send a `Release Resources` message to the source eNodeB. EPS bearers in source eNodeB are released.

9. The MME sends the `Delete Session Request` message to the source SGW to release bearers locally when the timer, previously set by the MME, has expired.

   If the NR Usage Data Reporting feature is activated and the MME has received the `Secondary RAT usage report list` IE from the eNodeB, the MME includes the `Secondary RAT usage data report` IE.

10. The source SGW acknowledges this by sending the `Delete Session Response` message to the MME. The source SGW deletes the bearers without notifying the PGW.

11. The UE sends a `TAU Request` message to the MME. The UE can also send a `Combined TAU Request` message to the MME. If a `Combined TAU Request` message is sent and the `PreventCombinedRegistration` parameter is set to false, continue with . Otherwise, continue with .

12. The MME sends a `Location Update Request` message to the MSC/VLR.

13. The MSC/VLR responds with a `Location Update Accept` message.

14. The MME answers with a `TAU Accept` message encapsulated in an `S1-AP Downlink NAS Transport` message to the UE. If the time elapsed since last GUTI reallocation is greater than the configured value `MMEGutiReallocationTimeLimit`, or if the UE moves to a different PLMN served by the same MME for Multiple PLMN Support, a GUTI reallocation is performed.

    The MME informs the UE about supported features, such as IMS Voice Service or IMS Emergency Service by sending the `EPS network feature support` IE in the `TAU Accept` message. Supported features are based on the configuration of the MME. The `EPS network feature support` IE includes `IMS VoPS` bit. See the Note for information about the `IMS VoPS` bit.

For more information on the IMS Voice Service and the IMS Emergency Service feature, see Features and Functions Management. For more information on configuring IMS Voice Service and IMS Emergency Service, see Configuring MMTel Service and IMSI Number Series (CLI).

15. If the GUTI has been reallocated, the UE sends a `TAU Complete` message to the MME.

16. If the `TAU Request` message in was a `Combined TAU Request` message, the MME sends a `TMSI Reallocation Complete` message to the MSC/VLR. This only occurs when a new TMSI is reallocated.

11.1.2.2 Failure in the X2-Based Handover with SGW Relocation

The following are examples of when `Path Switch Request Failure` messages are sent to the target eNodeB:

— No default bearers were set up in the target eNodeB

— All `Create Session Request` messages sent to the target SGW are unsuccessful, and no default bearers can be set up in the target SGW

— Failure in the X2-based handover procedure caused by roaming restrictions

The MME sends the `Path Switch Request Failure` message to the target eNodeB if the MME cannot determine the specific UE.

If the X2-based handover procedure fails because of roaming restrictions, the MME sends a `Path Switch Request Failure` message to the target eNodeB with the default cause code `Handover failure in Target EPC/eNodeB or Target System`. The MME sends a `Detach Request` message with an operator-configured cause code between #11 - #15 to the UE.

11.2 Mobility with S1-Based Handover

Although handover over the X2 interface is preferred, this is not possible if no X2 interface exists between the eNodeBs. In this case, the RAN initiates a handover preparation over the S1 interface to avoid service disruption. The S1 handover can involve a relocation of the MME, the SGW, or both, along with eNodeB relocation.

The handover is initiated by the source eNodeB when the eNodeB detects UE movement between Tracking Areas.

For more information about CSG restrictions, see CSG Restrictions on page 131.

Note: Handover to a CSG cell in another PLMN always fails.

11.2.1 Inter-MME S1-Based Handover without SGW Relocation

An inter-MME S1-based handover without SGW relocation procedure is performed when the UE moves between cells and the new cell is within the same SGW service area, but served by a different MME.

11.2.1.1 Traffic Case

The inter-MME S1-based handover without SGW relocation procedure is shown in Figure 33 and is described below the figure.

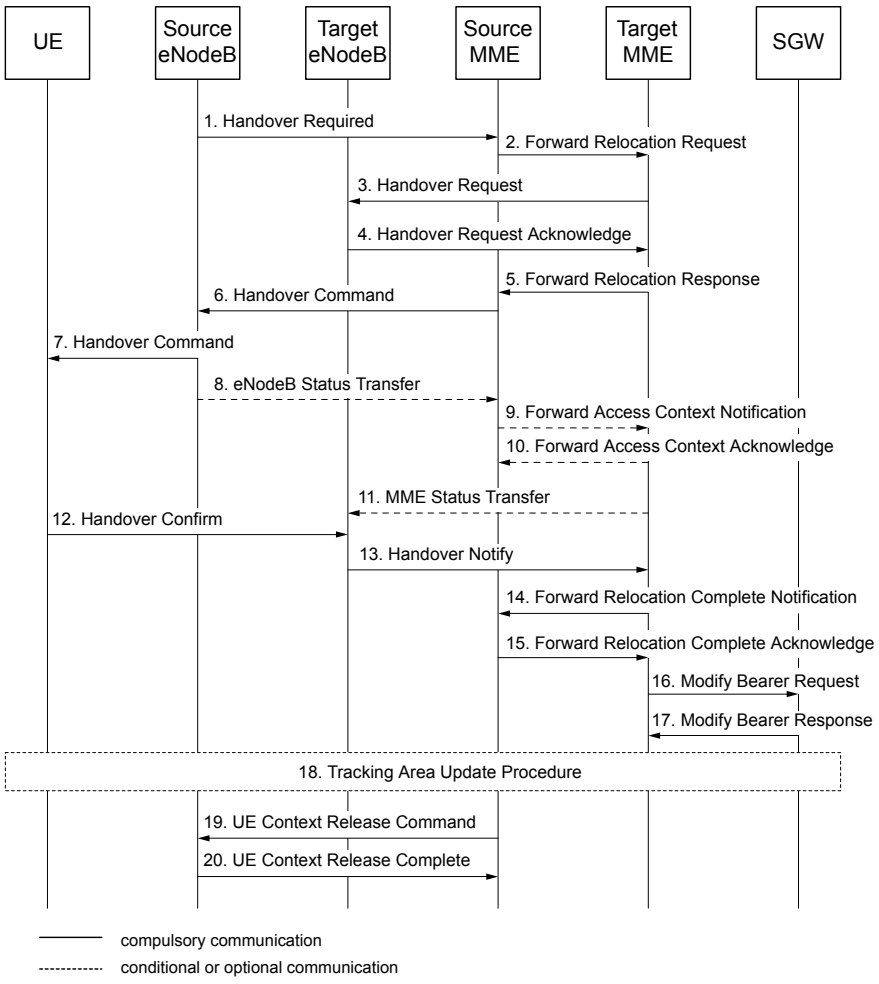


Figure 33 Inter-MME S1-Based Handover without SGW Relocation Procedure

The following steps describe the inter-MME S1-based handover without SGW relocation procedure:

1. The source eNodeB sends a `Handover Required` message to the source MME. The source MME checks if access restrictions or roaming restrictions

apply. The source MME also checks if CSG restrictions apply. If the UE is restricted, the S1-based handover procedure fails, see Failure in the Inter-MME S1-Based Handover without SGW Relocation on page 99. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile. If the target TA is restricted, non-emergency PDN connections are removed. For more information on the removal of non-emergency PDN connections, see . For more information on how to configure IMS Emergency Service, see Configuring MMTel Service.

2. The source MME sends a `Forward Relocation Request` message to the selected target MME. The source MME selects the target MME either through static selection or a DNS query, depending on the configuration. For detailed information about the static selection, see Static and DNS-based SGSN or MME Selection on page 116.

   Note: The MME can be configured to blacklist temporarily unavailable target nodes during inter-MME S1-Based PS Handover, see Target SGSN-MME Selection and Blacklisting during PS Handover on page 118 .

   The UE Radio Capability for Paging information can be included in the `Forward Relocation Request` message and transferred from the source MME to the target MME. For more information, see Massive IoT.

   The target MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the S1-based handover procedure fails, see Failure in the Inter-MME S1-Based Handover without SGW Relocation on page 99. For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information on how to configure an MME to send an emergency PDN connection between PLMNs, see Configuring MMTel Service and IMS Emergency Service (CLI).

   The target MME checks if APN restriction applies. If the APN or the APNS contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, the Handover Preparation Phase fails. For more information, see APN Resolve and Redirect for LTE Access.

   The target MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target TA is restricted, non-emergency PDN connections are removed. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

3. The target MME sends the `Handover Request` message to the target eNodeB. The `Handover Request` message creates the UE context in the

target eNodeB, including information about the bearers and the security context.

If the optional feature MME Support of HeNB is enabled and the MME fails to find the target eNodeB, the MME uses the TAI to search for the HeNB GW that serves this TAI. If the TAI is served by both macro eNodeB, or eNodeBs, and a HeNB GW, the MME selects the HeNB GW that serves the same TAI from the configured HeNB GW table. In this case, the MME sends the `Handover Request` message to the HeNB GW instead of the eNodeB.

If multiple HeNB GWs match the target TAI, and the Global eNodeB ID in the target ID IE has 28 bits, the MME uses the 20 most significant bits as the Global eNodeB ID to look for a directly connected HeNB GW, whose Global eNodeB ID is 20bits, same as the 20 most significant bits of the Global eNodeB ID in the target ID IE.

- If the MME finds a HeNB GW, the MME treats that HeNB GW as the target eNodeB.
- If the MME cannot find a HeNB GW, the MME randomly selects a HeNB from the HeNB GWs that match the target TAI as the target eNodeB.

If the HeNB is connected to the MME directly, the MME searches for the HeNB in the same way as it searches for a traditional macro eNodeB.

4. The target eNodeB acknowledges this request by sending a `Handover Request Acknowledge` message to the target MME. If the HeNB is deployed with an HeNB GW, the HeNB responds to the target MME through the HeNB GW with a `Handover Request Acknowledge` message after establishing the bearers. If the HeNB is connected to the target MME directly, it responds to the target MME without the HeNB GW.

   The list of bearers to set up must contain at least one default bearer. If no default EPS bearers are accepted by the target eNodeB, the inter-MME S1-based handover without SGW relocation procedure is rejected, see Failure in the Inter-MME S1-Based Handover without SGW Relocation on page 99.

5. The target MME sends a `Forward Relocation Response` message to the source MME, in response to .

6. The source MME sends a `Handover Command` message to the source eNodeB.

7. The eNodeB forwards the `Handover Command` message to the UE. This message can contain a list of bearers to release.

8. The source eNodeB can send an `eNodeB Status Transfer` message to the source MME. In case this message is not sent, continue with .

9. The source MME forwards the information in the `eNodeB Status Transfer` message to the target MME in a `Forward Access Context Notification` message.

10. The target MME responds by sending a `Forward Access Context Acknowledge` message to the source MME.

11. The target MME forwards the `MME Status Transfer` message to the target eNodeB. If the HeNB is deployed with an HeNB GW, the target MME sends the `MME Status Transfer` message to the HeNB through the HeNB GW. If the HeNB is connected to the target MME directly, the target MME sends the message to the HeNB without HeNB GW.

12. When the UE and the target cell have synchronized successfully, the UE sends a `Handover Confirm` message to the target eNodeB in response to .

13. The target eNodeB sends a `Handover Notify` message to the target MME. The `Handover Notify` message informs the target MME that the UE has arrived to the target cell and that the S1-based handover was successfully completed. If the HeNB is deployed with an HeNB GW, the target MME receives the `Handover Notify` message from the HeNB GW that serves the HeNB. If the HeNB is connected to the target MME directly, the target MME receives the message from the HeNB without HeNB GW.

14. The target MME sends a `Forward Relocation Complete Notification` message to the source MME.

15. The source MME responds by sending a `Forward Relocation Complete Acknowledge` message to the target MME.

16. The target MME performs the S-NAPTR query to select an SGW based on the current TAI of the UE and the old PGW. The target MME determines if the SGW relocation happens by comparing the selected SGW name with the SGW node name received in the Forward Relocation Request message. If the SGW node name is not included in the Forward Relocation Request message, the target MME determines if the SGW relocation happens. The target MME compares the IP address of the selected SGW with the SGW IP address received in the Forward Relocation Request message. In this case, the SGW relocation does not happen, and the target MME sends one `Modify Bearer Request` message for each PDN connection to the SGW.

17. The SGW responds by sending a `Modify Bearer Response` message to the target MME.

18. A Tracking Area Update Procedure is performed.

19. The source MME sends a `UE Context Release Command` message to the source eNodeB.

20. The source eNodeB releases its resources related to the UE and responds with the `UE Context Release Complete` message.

11.2.1.2 Failure in the Inter-MME S1-Based Handover without SGW Relocation

The target eNodeB sends a `Handover Failure` message when it fails to allocate any resources for any of the requested non-GBR bearers, that is, resource

allocation fails for all the requested non-GBR bearers. The MME sends the `Handover Preparation Failure` message to the source MME with an applicable cause code.

The following are examples of when `Handover Preparation Failure` messages are sent:

— No UE context is established in the target MME and target eNodeB, and no resources are allocated.

— No default bearers can be set up in the target eNodeB.

— The S1-based handover procedure fails because of roaming restrictions.

  For example, the MME sends a `Handover Preparation Failure` message with the cause code `Handover Failure in Target EPC/eNodeB or Target System` to the source eNodeB.

11.2.2 Inter-MME S1-Based Handover with SGW Relocation

An inter-MME S1-based handover with SGW relocation procedure is performed when the UE moves between cells, and the new cell is served by a new MME and a new SGW.

11.2.2.1 Traffic Case

The inter-MME S1-based handover with SGW relocation procedure is shown in Figure 34 and is described below the figure.

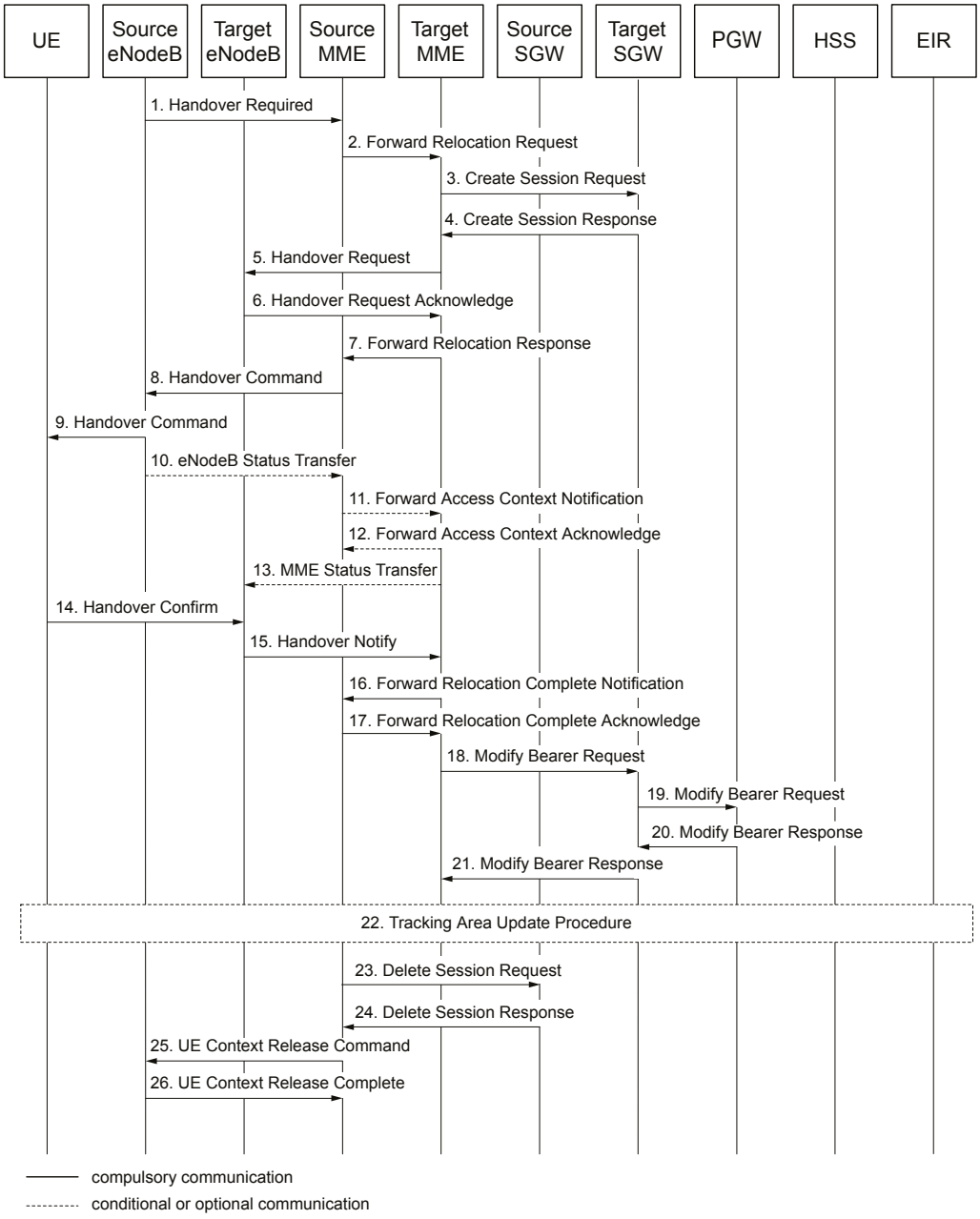


Figure 34 Inter-MME S1-Based Handover with SGW Relocation Procedure

The following steps describe the inter-MME S1-based handover with SGW relocation procedure:

1. The source eNodeB sends a `Handover Required` message to the source MME. The source MME checks if access restrictions or roaming restrictions apply. The source MME also checks if CSG restrictions apply. If the UE is restricted, the S1-based handover procedure fails, see Failure in the Inter-MME S1-Based Handover with SGW Relocation on page 105. For IMS

Emergency Service, access, CSG, and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile. If the target TA is restricted, non-emergency PDN connections are removed. For more information on the removal of non-emergency PDN connections, see . For more information on how to configure IMS Emergency Service, see Configuring MMTel Service.

2. The source MME sends a `Forward Relocation Request` message to the selected target MME. The source MME selects the target MME either through static selection or a DNS query, depending on the configuration. For detailed information about the static selection, see Static and DNS-based SGSN or MME Selection on page 116.

   The UE Radio Capability for Paging information can be included in the `Forward Relocation Request` message and transferred from the source MME to the target MME. For more information, see Massive IoT.

   The target MME checks if access restrictions or roaming restrictions apply. If the UE is restricted, the S1-based Handover procedure fails, see Failure in the Inter-MME S1-Based Handover with SGW Relocation on page 105.For IMS Emergency Service, access and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information on how to configure an MME to send an emergency PDN connection between PLMNs, see Configuring MMTel Service and IMS Emergency Service (CLI).

   The target MME checks if APN Restriction applies. If all the APN or APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, a `Handover Preparation Failure` is sent to source eNodeB. For more information, see APN Resolve and Redirect for LTE Access.

   The target MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If the target TA is restricted, non-emergency PDN connections are removed. For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

   If the UE has set up any dedicated bearers, the target MME checks if the licensed feature Network-initiated Dedicated Bearers is activated. If the feature Network-initiated Dedicated Bearers is activated, the dedicated bearers are allowed to continue. If the feature is not activated, the existing dedicated bearers are marked to be deleted. For more information on the feature Network-initiated Dedicated Bearers, see Features and Functions Management.

3. The target MME performs the S-NAPTR query to select an SGW based on the current TAI of the UE and the old PGW. The target MME determines if the SGW relocation happens by comparing the selected SGW name with the SGW node name received in the Forward Relocation Request message. If the SGW node name is not included in the Forward Relocation Request message, the target MME determines if the SGW relocation happens. The target MME compares the IP address of the selected SGW with the SGW IP address received in the Forward Relocation Request message. In this case, the SGW relocation happens, and the target MME sends a `Create Session Request` message to the target SGW.

4. The target SGW sends the `Create Session Response` message to the target MME.

5. The target MME sends the `Handover Request` message to the target eNodeB. The `Handover Request` message creates the UE context in the target eNodeB, including information about the bearers and the security context.

   If the optional feature MME Support of HeNB is enabled and the MME fails to find the target eNodeB, the MME uses the TAI to search for the Home eNodeB Gateway (HeNB GW) that serves that TAI. If the TAI is served by both macro eNodeB, or eNodeBs, and a HeNB GW, the MME selects the HeNB GW that serves the same TAI from the configured HeNB GW table. In this case, the MME sends the `Handover Request` message to the HeNB GW instead of the eNodeB.

   If multiple HeNB GWs match the target TAI, and the Global eNodeB ID in the target ID IE has 28 bits, the MME uses the 20 most significant bits as the Global eNodeB ID to look for a directly connected HeNB GW, whose Global eNodeB ID is 20bits, same as the 20 most significant bits of the Global eNodeB ID in the target ID IE.

   - If the MME finds a HeNB GW, the MME treats that HeNB GW as the target eNodeB.
   - If the MME cannot find a HeNB GW, the MME randomly selects a HeNB from the HeNB GWs matching the target TAI as the target eNodeB.

   If the HeNB is connected to the MME directly, the MME searches for the HeNB in the same way as it searches for a traditional macro eNodeB.

6. The target eNodeB acknowledges this request by sending a `Handover Request Acknowledge` message to the target MME. If the HeNB is deployed with an HeNB GW, the HeNB responds to the target MME through the HeNB GW with a `Handover Request Acknowledge` message after establishing the bearers. If the HeNB is connected to the target MME directly, it responds to the target MME without the HeNB GW.

7. The target MME sends the `Forward Relocation Response` message to the source MME with the cause **`Request Accepted`**. Only the successful bearers are listed for each PDN connection.

8. The source MME sends the `Handover Command` message to the source eNodeB.
9. The source eNodeB forwards the `Handover Command` message to the UE.
10. The source eNodeB can also send the `eNodeB Status Transfer` message to the source MME. In case this message is not sent, continue with .
11. The source MME forwards the `eNodeB Status Transfer` message in a `Forward Access Context Notification` message to the target MME.
12. The target MME responds with a `Forward Access Context Acknowledge` message.
13. The target MME sends an `MME Status Transfer` message to the target eNodeB. If the HeNB is deployed with an HeNB GW, the target MME sends the `MME Status Transfer` message to the HeNB through the HeNB GW. If the HeNB is connected to the target MME directly, the target MME sends the message to the HeNB without HeNB GW.
14. The UE detaches from the old cell and synchronizes with the target cell. The UE sends a `Handover Confirm` message to the target eNodeB. This can happen anytime after .
15. The target eNodeB sends a `Handover Notify` message to the target MME when the UE is identified in the target cell and the S1-based handover procedure has been successfully completed. If the HeNB is deployed with an HeNB GW, the target MME receives the `Handover Notify` message from the HeNB GW that serves the HeNB. If the HeNB is connected to the target MME directly, the target MME receives the message from the HeNB without HeNB GW.
16. The target MME sends a `Forward Relocation Complete Notification` message to the source MME and deactivates the dedicated bearers that were previously marked for deletion.
17. The source MME sends a `Forward Relocation Complete Acknowledge` message to the target MME.
18. The target MME sends one `Modify Bearer Request` message for each PDN connection to the target SGW.
19. The target SGW forwards the `Modify Bearer Request` message to the PGW.
20. The PGW responds with a `Modify Bearer Response` message to the target SGW.
21. The target SGW forwards the `Modify Bearer Response` message to the target MME.
22. A Tracking Area Update Procedure is performed.

23. If an indication of SGW relocation was sent to the source MME in the `Forward Relocation Response` message, the source MME sends the `Delete Session Request` message to the source SGW.

24. The source SGW responds to the source MME with a `Delete Session Response` message. The source SGW deletes the bearer resources locally.

25. The source MME releases the EPS bearer resources when the handover procedure is completed by sending a `UE Context Release Command` message to the source eNodeB.

26. The source eNodeB releases the UE contexts and responds to the source MME with the `UE Context Release Complete` message.

11.2.2.2 Failure in the Inter-MME S1-Based Handover with SGW Relocation

The target eNodeB sends a `Handover Failure` message when the target eNodeB fails to allocate any resources for any of the requested non-GBR bearers, that is, resource allocation fails for all the requested non-GBR bearers. The MME clears the reserved resources in the SGW for the UE on receiving the `Handover Failure` message from the target eNodeB. The MME sends the `Handover Preparation Failure` message to the source MME with an applicable cause code.

The following are examples of when `Handover Preparation Failure` messages are sent:

— No target SGW is selected or found.

— No UE context is established in the target SGW or target eNodeB, and no resources are allocated.

— No default bearers can be established in the target SGW.

— The S1-based handover procedure fails because of roaming restrictions.

11.2.3 Intra-MME S1-Based Handover without SGW Relocation

An intra-MME S1-based handover without SGW relocation procedure is performed when the UE moves between cells within the same MME and SGW serving areas.

11.2.3.1 Traffic Case

The intra-MME S1-based handover without SGW relocation procedure is shown in Figure 35 and is described below the figure.

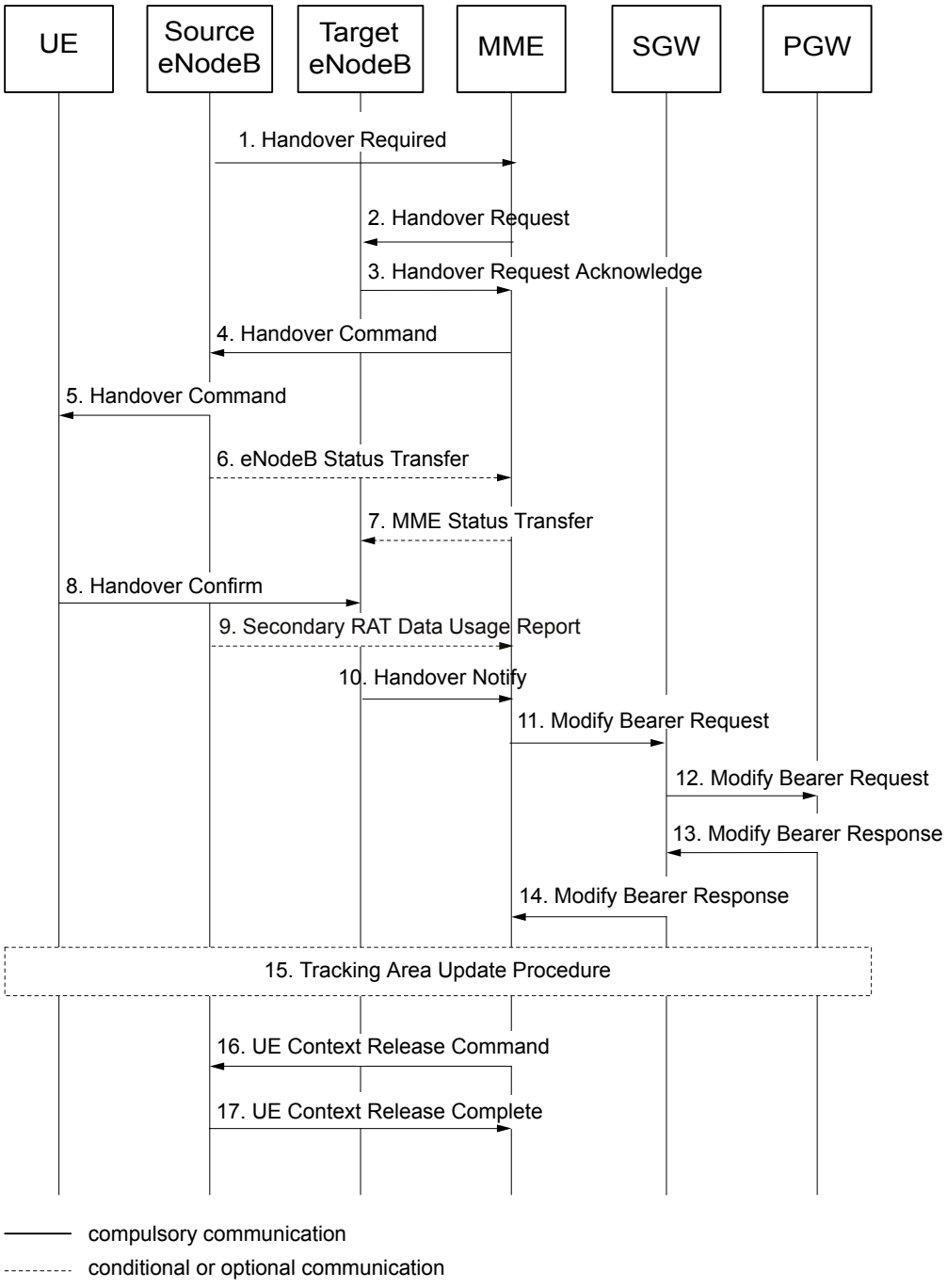


Figure 35 Intra-MME S1-Based Handover without SGW Relocation Procedure

The following steps describe the intra-MME S1-based handover without SGW relocation procedure:

1. The source eNodeB sends a `Handover Required` message to the MME.

The MME checks if access or roaming restrictions apply. The source MME also checks if CSG restrictions apply. If the UE is restricted, the S1-based handover procedure fails, see Failure in the Intra-MME S1-Based Handover with SGW Relocation on page 113. For IMS Emergency Service, access, CSG, and roaming restrictions are ignored. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

The MME checks if APN Restriction applies. If the APN or the APNs contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, a `Handover Preparation Failure` is sent to source eNodeB. For more information, see APN Resolve and Redirect for LTE Access.

The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If restrictions apply, non-emergency PDN connections are removed. For more information on the removal of non-emergency PDN connections, see . For more information on how to configure IMS Emergency Service, see Configuring MMTel Service and IMS Emergency Service (CLI).

2. The MME sends a `Handover Request` message to the target eNodeB, which creates the UE context in the target eNodeB.

   If the licensed feature MME Support of HeNB is enabled and the MME fails to find the target eNodeB, the MME uses the TAI to search for the HeNB GW that serves that TAI. If the TAI is served by both macro eNodeB, or eNodeBs, and a HeNB GW, the MME selects the HeNB GW that serves the same TAI from the configured HeNB GW table. In this case, the MME sends the `Handover Request` message to the HeNB GW instead of the eNodeB.

   If multiple HeNB GWs match the target TAI, and the Global eNodeB ID in the target ID IE has 28 bits, the MME uses the 20 most significant bits as the Global eNodeB ID to look for a directly connected HeNB GW, whose Global eNodeB ID is 20bits, same as the 20 most significant bits of the Global eNodeB ID in the target ID IE.

   - If the MME finds a HeNB GW, the MME treats that HeNB GW as the target eNodeB.
   - If the MME cannot find a HeNB GW, the MME randomly selects a HeNB from the HeNB GWs that match the target TAI as the target eNodeB.

   If the HeNB is connected to the MME directly, the MME searches for the HeNB in the same way as it searches for a traditional macro eNodeB.

3. The target eNodeB responds with a `Handover Request Acknowledge` message to the MME. If the HeNB is deployed with an HeNB GW, the HeNB responds to the MME through the HeNB GW with a `Handover Request Acknowledge` message after establishing the bearers. If the HeNB is connected to the MME directly, it responds to the MME without the HeNB GW.

4. The MME sends a `Handover Command` message to the source eNodeB.
5. The eNodeB forwards the `Handover Command` message to the UE. The `Handover Command` message can contain a list of bearers to release.
6. The source eNodeB can send an `eNodeB Status Transfer` message to the MME. In case this message is not sent, continue with .
7. The MME forwards the `MME Status Transfer` message to the target eNodeB. If the HeNB is deployed with an HeNB GW, the MME sends the `MME Status Transfer` message to the HeNB through the HeNB GW. If the HeNB is connected to the MME directly, the MME sends the message to the HeNB without the HeNB GW.
8. When the UE and the target cell have synchronized successfully, the UE sends a `Handover Confirm` message to the target eNodeB.
9. If the NR Usage Data Reporting feature is activated, the eNodeB can send the `Secondary RAT Usage Data Report` message which includes the `Secondary RAT Usage Report List` IE. A handover indication flag is included.
10. The target eNodeB sends a `Handover Notify` message to the MME. The `Handover Notify` message informs the MME that the UE has arrived to the target cell and that the S1 handover was successfully completed. If the HeNB is deployed with an HeNB GW, the MME receives the `Handover Notify` message from the HeNB GW that serves the HeNB. If the HeNB is connected to the MME directly, the MME receives the message from the HeNB without the HeNB GW.
11. The MME sends one `Modify Bearer Request` message for each PDN connection to the SGW.

    If the NR Usage Data Reporting feature is activated and the MME has received the `Secondary RAT Usage Report List` IE from the eNodeB, the MME includes the `Secondary RAT Usage Data Report` IE.
12. The SGW forwards the `Modify Bearer Request` message to the PGW.
13. The PGW responds by sending a `Modify Bearer Response` message to the SGW.
14. The SGW forwards the `Modify Bearer Response` message to the MME.
15. A Tracking Area Update Procedure is performed.
16. The MME sends a `UE Context Release Command` message to the source eNodeB.
17. The source eNodeB releases the resources related to the UE and responds with a `UE Context Release Complete` message.

11.2.3.2 Failure in the Intra-MME S1-Based Handover without SGW Relocation

The target eNodeB sends a `Handover Failure` message when the target eNodeB fails to allocate any resources for any of the requested non-GBR bearers, that is, resource allocation fails for all the requested non-GBR bearers. The MME sends the `Handover Preparation Failure` message to the source MME with an applicable cause code.

The following are examples of when `Handover Preparation Failure` messages are sent:

— No UE context is established in the target eNodeB, and no resources are allocated.

— No default bearers can be set up in the target eNodeB.

— The S1-based handover procedure fails because of roaming restrictions.

  For example, the MME sends a `Handover Preparation Failure` message with cause code `Handover Failure in Target EPC/eNodeB or Target System` to the source eNodeB.

11.2.4 Intra-MME S1-Based Handover with SGW Relocation

An intra-MME S1-based handover with SGW relocation procedure is performed when the UE moves between cells, and the new cell is within the same MME service area, but the cell is served by a new SGW.

11.2.4.1 Traffic Case

The intra-MME S1-based handover with SGW relocation procedure is shown in Figure 36 and is described below the figure.

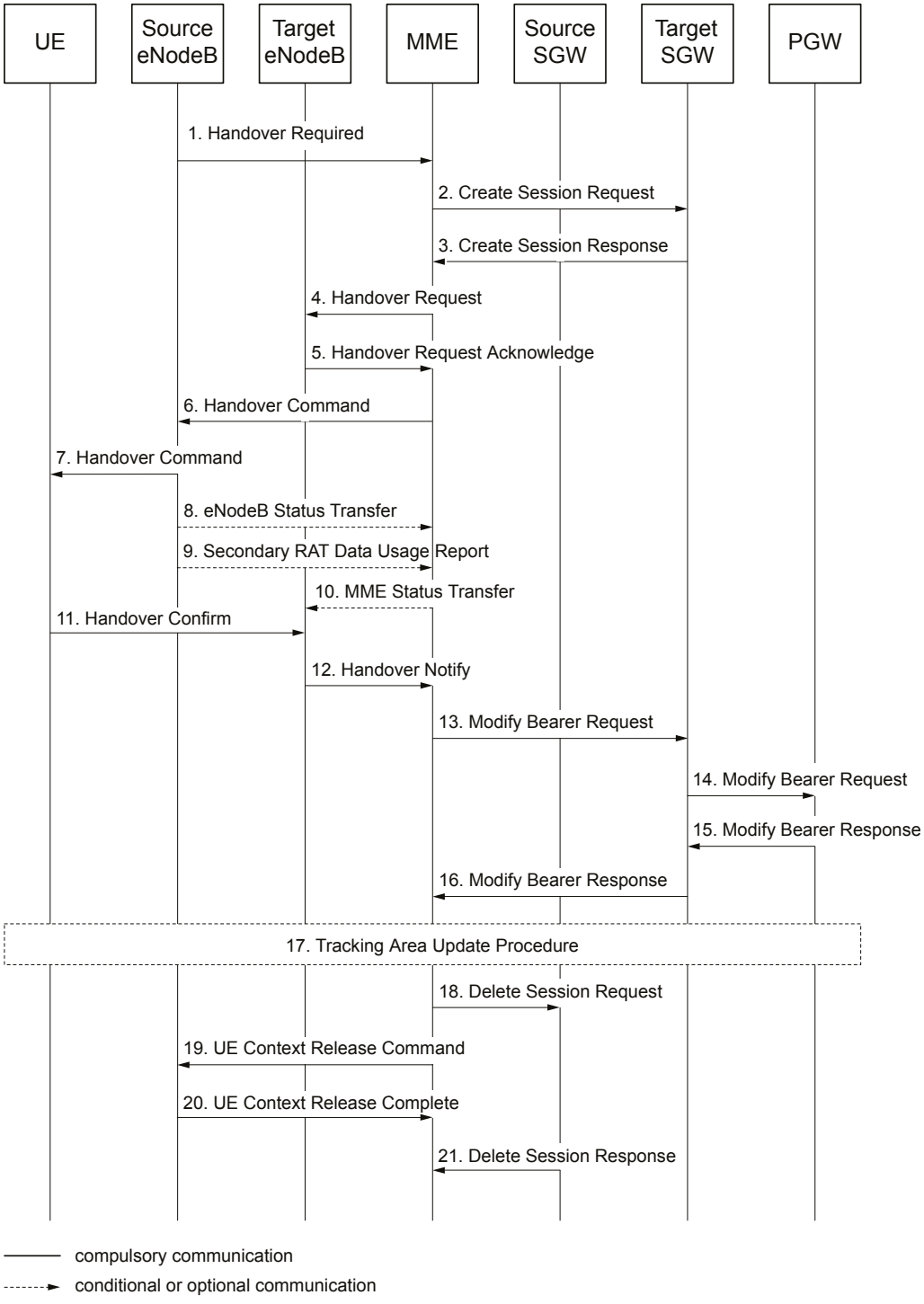


Figure 36 Intra-MME S1-Based Handover with SGW Relocation Procedure

The following steps describe the intra-MME S1-based handover with SGW relocation procedure:

1. The source eNodeB sends a `Handover Required` message to the MME.

   The MME checks if access or roaming restrictions apply. The source MME also checks if CSG restrictions apply. If the UE is restricted, the S1-based handover procedure fails, see Failure in the Intra-MME S1-Based Handover with SGW Relocation on page 113. For more information about Access Restrictions, see Access Restrictions on page 126. For more information about Roaming Restrictions, see Roaming Restrictions on page 123. For more information about CSG restrictions, see CSG Restrictions on page 131.

   The MME checks if APN Restriction applies. If the APN or the APNS contained in the EPS Bearer Context stored for the UE matches the configured APN blacklist in the MME, a `Handover Preparation Failure` is sent to source eNodeB. For more information, see APN Resolve and Redirect for LTE Access.

   The MME keeps an emergency PDN connection based on the configuration of the emergency profile in the target PLMN. If restrictions apply, non-emergency PDN connections are removed. For more information on the removal of non-emergency PDN connections, see . For more information on how to configure IMS Emergency Service, see Configuring MMTel Service.

2. The MME selects a target SGW based on the TAI and the old PGW. The MME sends a `Create Session Request` message to the target SGW.

3. The target SGW responds with a `Create Session Response` message to the MME.

4. The MME sends a `Handover Request` message to the target eNodeB, which creates the UE context in the target eNodeB.

   If the licensed feature MME Support of HeNB is enabled and the MME fails to find the target eNodeB, the MME uses the TAI to search for the HeNB GW that serves that TAI. If the TAI is served by both macro eNodeB, or eNodeBs, and a HeNB GW, the MME selects the HeNB GW that serves the same TAI from the configured HeNB GW table. In this case, the MME sends the `Handover Request` message to the HeNB GW instead of the eNodeB.

   If multiple HeNB GWs match the target TAI, and the Global eNodeB ID in the target ID IE has 28 bits, the MME uses the 20 most significant bits as the Global eNodeB ID to look for a directly connected HeNB GW, whose Global eNodeB ID is 20bits, same as the 20 most significant bits of the Global eNodeB ID in the target ID IE.

   - If the MME finds a HeNB GW, the MME treats that HeNB GW as the target eNodeB.
   - If the MME cannot find a HeNB GW, the MME randomly selects a HeNB from the HeNB GWs that match the target TAI as the target eNodeB.

   If the HeNB is connected to the MME directly, the MME searches for the HeNB in the same way as the MME searches for a traditional macro eNodeB.

5. The target eNodeB responds with a `Handover Request Acknowledge` message to the MME. If the HeNB is deployed with an HeNB GW, the HeNB responds to the MME through the HeNB GW with a `Handover Request Acknowledge` message after establishing the bearers. If the HeNB is connected to the MME directly, it responds to the MME without the HeNB GW.

6. The MME sends a `Handover Command` message to the source eNodeB.

7. The eNodeB forwards the `Handover Command` message to the UE. The `Handover Command` message can contain a list of bearers to release.

8. The source eNodeB can send an `eNodeB Status Transfer` message to the MME. In case this message is not sent, continue with .

9. If the NR Usage Data Reporting feature is activated, the eNodeB can send the `Secondary RAT Data Usage Report` message which includes the `Secondary RAT Usage Report List` IE.

10. The MME forwards the `MME Status Transfer` message to the target eNodeB. If the HeNB is deployed with an HeNB GW, the MME sends the `MME Status Transfer` message to the HeNB through the HeNB GW. If the HeNB is connected to the MME directly, the MME sends the message to the HeNB without the HeNB GW.

11. When the UE and the target cell have synchronized successfully, the UE sends a `Handover Confirm` message to the target eNodeB.

12. The target eNodeB sends a `Handover Notify` message to the MME. The `Handover Notify` message informs the MME that the UE has arrived to the target cell and that the S1 handover was successfully completed. If the HeNB is deployed with an HeNB GW, the MME receives the `Handover Notifyy` message from the HeNB GW which serves the HeNB. If the HeNB is connected to the MME directly, the MME receives the message from the HeNB without the HeNB GW.

13. The MME sends one `Modify Bearer Request` message for each PDN connection to the target SGW.

    If the NR Usage Data Reporting feature is activated, the MME can include the `Secondary RAT Usage Data Report` IE. A handover indication flag is included.

14. The target SGW forwards the `Modify Bearer Request` message to the PGW.

15. The PGW responds by sending a `Modify Bearer Response` message to the target SGW.

16. The target SGW forwards the `Modify Bearer Response` message to the MME.

17. A Tracking Area Update Procedure is performed.

18. The MME sends the `Delete Session Request` messages to the source SGW to release the EPS bearer resources. It is indicated in the messages that the source SGW must not initiate a delete procedure toward the PGW.

    If the NR Usage Data Reporting feature is activated, the MME can include the `Secondary RAT Usage Data Report` IE. The `IRSGW` bit is set to 1 and `IRPGW` bit is set to `0`.

19. The MME sends a `UE Context Release Command` message to the source eNodeB.

20. The source eNodeB releases the resources related to the UE and responds with the `UE Context Release Complete` message.

21. The source SGW responds to with the `Delete Session Response` message.

11.2.4.2 Failure in the Intra-MME S1-Based Handover with SGW Relocation

The target eNodeB sends a `Handover Failure` message when the requested non-GBR bearers cannot be allocated any resources by the target eNodeB, that is, resource allocation fails for all the requested non-GBR bearers. The MME clears the reserved resources in the SGW for the UE on receiving the `Handover Failure` message from the target eNodeB. The MME sends the `Handover Preparation Failure` message to the source MME with an applicable cause code.

The following are examples of when `Handover Preparation Failure` messages are sent:

— No target SGW is selected or found

— No UE context is established in the target SGW or target eNodeB and no resources are allocated

— No default bearers can be established in the target SGW

— Failure in the S1-based handover procedure caused by roaming restrictions

If the S1-based handover procedure fails caused by roaming restrictions, the MME sends a `Handover Preparation Failure` message to the source eNodeB with the cause code `Handover failure in Target EPC/eNodeB or Target System`.

12 Cell Change Reporting

When the licensed-controlled Cell Change Reporting feature is enabled, the MME subscribes to cell change events for the UE from the eNodeB. This is applicable for all UE devices in the ECM-CONNECTED state. The location information is then forwarded to the SGW.

Note: Enabling the feature increases signaling on the S1, S11, and the S5/S8 interfaces. The feature can also increase the overall load in the SGSN-MME in systems with many simultaneously attached users.

12.1 Traffic Case

The Cell Change Reporting procedure is shown in Figure 37 and is described below the figure.

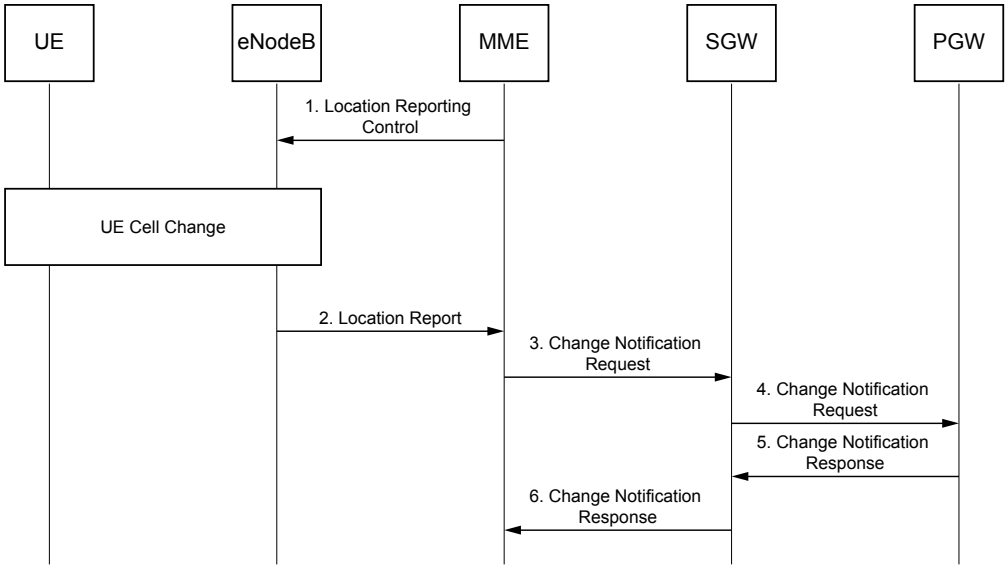


Figure 37 Cell Change Reporting Procedure

The following steps describe the Cell Change Reporting procedure:

1. When the UE changes state to ECM-CONNECTED, the MME sends a `Location Reporting Control` message to the eNodeB. In this message, the MME requests the eNodeB to send a location report whenever the UE changes cells.

2. The eNodeB sends a `Location Report` message to inform the MME about the location of the UE, including the TAI and ECGI, whenever the UE changes cells.

3. The MME sends one `Change Notification Request` message, including the TAI and ECGI, to the SGW for each PDN connection.

4. The SGW forwards the `Change Notification Request` message to the PGW. If dynamic policy and charging control are deployed, the PGW forwards the ECGI changes to the PCRF, if necessary.

5. The PGW sends the `Change Notification Response` message to the SGW.

6. The SGW forwards the `Change Notification Response` message to the MME.

13 Static and DNS-based SGSN or MME Selection

Note: The static SGSN or MME Selection is a customer specified solution.

The static SGSN or MME selection function enables the MME to select the old or the target SGSN or MME through the preconfigured selection tables. The static selection occurs during the Attach, TAU, Inter-MME S1 Handover, IRAT PS Handover, and RIM procedures. Both the combined SGSN-MMEs and the pure MMEs support the static selection. For detailed information about the preconfigured SGSN and MME selection tables, see Configuring Static SGSN or MME Selection in MME.

The static selection function is enabled by setting the node function `static_mme_sgsn_selection` to `ON`. If the node function is set to `OFF`, only the DNS query is used to select the nodes.

Note: For a TAU procedure from a GSM or a WCDMA SGSN, if the old RAI is in the own pool of the SGSN, the SGSN selection table created by the CLI command create_nri is used to find the old SGSN instead of a DNS query. The node function static_mme_sgsn_selection is only used when the MME searches for a cooperating SGSN outside the own pool or in a remote pool, that is, the SGSN selection in own pool is independent of the node function static_mme_sgsn_selection.

If the static selection is successful, the MME gets the IP address of the old or the target node. If the static selection fails, the DNS query is used only if the node function `static_mme_sgsn_selection_snaptr_dns_fallback` is set to `ON`. If the DNS query is successful, the MME gets both the hostname and the IP address of the old or the target node. The S-NAPTR procedure is used to query the DNS to select the MME. The S-NAPTR procedure or type A/AAAA is used to query the DNS to select the SGSN.

During the Attach and the TAU procedures, the MME resolves the old side using the old GUTI in the Attach request and the TAU request messages. If the old GUTI is native, the old side is an MME. If the old GUTI is mapped from P-TMSI, the old side is an SGSN.

When the TAU Request with the `old GUTI type` IE is received, the old GUTI is either native or mapped, which depends on what it is indicated in the old GUTI type.

When the TAU Request without the `old GUTI type` IE is received, the old GUTI is native in the following cases:

— The TAU procedure is integrity protected and the `Additional GUTI` IE is not present.

— The TAU procedure is integrity protected and the `Additional GUTI` IE matches the old GUTI.

Otherwise, the old GUTI is considered as mapped.

13.1 Static SGSN Selection

This section describes the static SGSN selection in MMEs.

During the Attach or the TAU procedure, the new MME queries different selection tables to select the old SGSN. The new MME extracts the RAI and NRI from the old GUTI. One RAI is associated with only one SGSN pool. If the RA is served by SGSNs in the same pool as the new MME, the MME uses the RAI and the NRI as the input to query the SGSN selection table for SGSNs in the own pool. If the combined SGSN-MME is the only SGSN in the pool, the combined SGSN is selected as the old SGSN. Otherwise, the SGSN matched by the RAI and the NRI in the pool is selected as the old SGSN. For SGSNs outside a pool or in a remote pool, the new MME uses the RAI and the NRI as inputs to query the SGSN selection table for a cooperating SGSN. If there is a matched SGSN, the SGSN is selected as the old SGSN. Otherwise, any SGSN that serves the cooperating RA is selected.

During the IRAT Handover or the RIM procedures, the source MME acquires the information of the target RAI from the Target RNC Identifier IE or the RIM Routing Address IE. If the target RA is served by SGSNs outside a pool or by a remote SGSN pool, the MME queries the SGSN selection table for a cooperating SGSN. The MME uses the RAI as input to query the selection table to get a list of SGSNs that serve the RA. If such a list is available, the MME sorts the list by capacity using the Weighted Round Robin (WRR) algorithm. The MME gets the IP address of the SGSN at the top of the list.

If the old or the target SGSN has both an S3IPAddress and a GnIPAddress or a GnIPv4v6Address, the new or the source MME prefers to select the S3IPAddress. In that case, the MME uses the GTPv2 to interwork with the old SGSN. If the GnIPAddress or the GnIPv4v6Address is selected, the MME uses the GTPv1 to interwork with the old SGSN.

13.2 Static MME Selection

During the Attach or the TAU procedures, the new MME queries the MME selection table to select the old MME. The new MME uses the GUMMEI as input. The GUMMEI, extracted from the old GUTI, consists of a PLMN-ID, an MME Group ID (MMEGI), and an MME Code (MMEC). If the query is successful, the new MME gets the IP address of the old MME.

During the Handover procedure, the source MME queries the MME selection table to select the target MME. The source MME uses the TAI as the input to get a candidate list of the target MMEs which serve the target TA. If such a list is available, the source MME sorts the candidate list by capacity using the

Weighted Round Robin (WRR) algorithm. The MME at the top of the sorted list is selected as the target MME.

13.3 Target SGSN-MME Selection and Blacklisting during PS Handover

The temporary blacklisting feature is applicable during Inter-MME S1-Based Handover and IRAT PS Handover from LTE to WCDMA over S3. The temporary blacklisting of the unavailable target nodes during S1-based inter-MME or IRAT PS Handover procedures is an optimization over the existing static or a DNS query-based target SGSN-MME selection.

If the target peer MME or S4-SGSN nodes are temporarily unavailable to the source MME queries during the inter-MME or IRAT PS Handover procedures, the source MME blacklists these temporarily unavailable peer nodes when the psho_target_blacklisting parameter is set to on using the modify_node_function CLI command.

Entering a Target Node to the Blacklist

The source MME considers a target MME or S4-SGSN temporarily unavailable during a PS Handover procedure, if the handover target does not send any `Forward Relocation Response` message during the time specified in the `T3ResponseForwardRelocation` parameter multiplied with the duration specified in the `N3RequestForwardRelocation` parameter.

Monitoring a Blacklisted Target and Clearing the Blacklist

— The source MME can blacklist the unavailable nodes for a configurable duration, see the PshoTargetTempUnavailableDuration parameter. The maximum duration for which an unavailable node can be blacklisted is 360 minutes.

— The MME monitors the blacklisted nodes using the GTPV2-C echo procedure.

— The source MME can use the blacklisted nodes again as targets for inter-MME or IRAT PS Handover procedures only after they are removed from the blacklist. The MME removes blacklisted nodes from the blacklist when any of the following happens:

  - The configured Temporarily Unavailable Duration timer expires, see the PshoTargetTempUnavailableDuration parameter.
  - The MME receives an `Echo Response` message from the blacklisted node.
  - The source MME receives the `Forward Relocation Response` message from the blacklisted node. This happens only when all the target nodes from both the SGSN and the MME selection table are temporarily unavailable and the source MME has to select a target anyway. For more

information, see Static SGSN Selection on page 117 and Static MME Selection on page 117.

- The psho_target_blacklisting parameter is set to `off` using the modify_node_function CLI command, which removes all the entries from the blacklist.

— The counters that monitor the number of times the target nodes are added and removed from the blacklist are the following:

- VS.HO.S10NbrTempBlockedTargetMme.E
- VS.IRATHO.S3NbrTempBlockedTargetS4sgsn.E
- VS.HO.S10NbrUnblockedTargetMme.E
- VS.IRATHO.S3NbrUnblockedTargetS4sgsn.E

SGSN-MME Target Selection with Temporary Unavailable Blacklisting

Blacklisting uses the sorted candidate list of target MMEs or S4-SGSNs returned to the target nodes through the DNS query and the static MME or SGSN selection procedure. To prevent a possible PS Handover, blacklisting ensures that the unavailable nodes are not selected as target nodes from the sorted candidate list of target MMEs or S4-SGSNs, for the subsequent PS Handover procedure. For more information, see Configuring SGSN-MME Selection and Blacklisting during PS Handover.

— When the psho_target_blacklisting parameter is set to `on` using the modify_node_function CLI command, the MME returns the first candidate in the sorted candidate list of target MMEs or S4-SGSNs that is not in the blacklist. If all the target nodes are blacklisted, the MME returns the first candidate in the sorted candidate list of target MMEs or S4-SGSNs.

Note: In case of static SGSN-MME selection with active DNS fallback, if all the candidates from the static configuration are blacklisted, no DNS query is triggered to find new candidates. Instead the first candidate in the sorted candidate list of target MMEs or S4-SGSNs is selected as the target node.

— When the node function psho_target_blacklisting parameter is set to `off` using the modify_node_function CLI command, the MME returns the first candidate in the sorted candidate list of target MMEs or S4-SGSNs.

14 Mobility-Based Policy Selection

The MME and the SAPC can communicate directly through the Smp interface when the Mobility-Based Policy feature is enabled. The MME uses policies from the SAPC for RFSP selection, also called SPID selection.

The MME selects the RFSP for the UE from the RFSP received from the SAPC, the subscribed RFSP, and the locally configured RFSP according to the following rules:

— For home subscribers, the RFSP value received from the SAPC takes precedence over the subscribed one. The RFSP value received from the SAPC is used if available and the Mobility-Based Policy feature is enabled. Otherwise, the subscribed RFSP value is used.

— For roaming subscribers, the locally configured RFSP value of the MME is used if available.

The selected RFSP is sent to the eNodeB for the UE through the following S1AP messages:

— Initial Context Setup Request

— UE Context Modification Request

— Downlink NAS Transport

Note: The RFSP is sent to the eNodeB in the Downlink NAS Transport message carrying certain NAS messages when the s1_include_spid_in_dl_nas_transport parameter is set to on.

15 Mobility Event Log

All `Attach Reject` messages that occur because of network failure are stored in the Mobility Event Log. The `Attach Reject` messages are stored for both GPRS and EPS subscribers.

For more information on the Mobility Event Log file, see Mobility Event Log.

16 Multiple PLMN Support

The SGSN-MME supports multiple PLMNs, that is, one SGSN-MME can serve several PLMNs. This makes it possible to share an SGSN-MME between networks in different countries or regions. It is also possible for several operators to share an SGSN-MME to support their individual RANs.

The Multiple PLMN Support feature allows up to 32 local PLMNs to share an SGSN-MME. Each PLMN is distinguished by a unique PLMN identity, consisting of an MCC and an MNC.

Multiple PLMN Support can be combined with the optional feature Roaming Restrictions to enable specific roaming restrictions for different roaming subscribers. For more information on the Roaming Restrictions feature, see Roaming Restrictions on page 123.

17 Restrictions

Restrictions enable the MME to restrict the access of certain subscribers.

17.1 Roaming Restrictions

The license-controlled feature Roaming Restrictions enables the MME to restrict or permit access for certain UEs to one or several tracking areas. Exempted areas can optionally be configured for roaming restrictions.

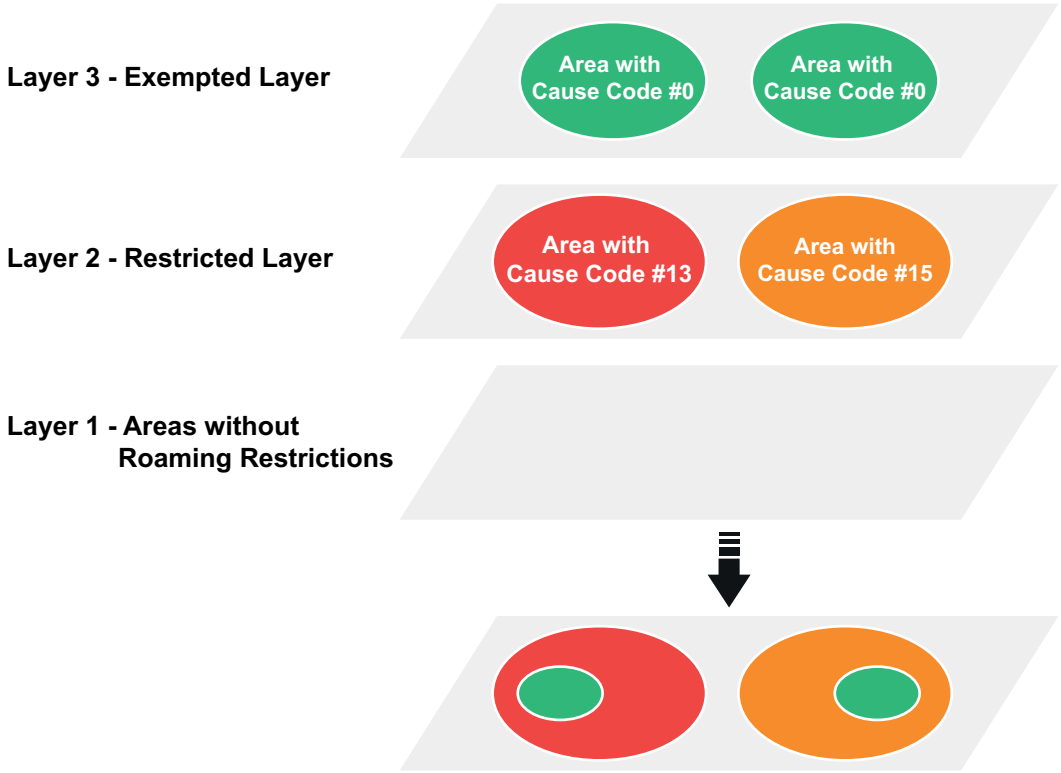


Figure 38 Roaming Restrictions with Exempted Areas

Layer 1 is the geographical area without roaming restriction configuration.

If a tracking area within layer 2 has been set with an RrCauseCode (#11-#15), this tracking area is configured as a restricted area. In Figure 38, two areas have been set with RrCauseCode #13 and RrCauseCode #15 respectively, making these two areas restricted areas.

The configuration of layer 3 is on top of the configuration of layer 2. If one or more tracking areas on layer 3 have been set with RrCauseCode #0, this area is configured as an exempted area on top of the restricted area.

Note: Cause Code #0 is used to configure roaming restrictions with exempted areas.

The Roaming Restrictions feature applies to the Attach, TAU, Handover, and CP Relocation procedures. Roaming Restrictions enable the MME to restrict or permit access for roaming subscribers to a tracking area within a geographical area based on the following conditions:

— IMSI number series

— UE device type (IMEI-TAC or IMEI-TAC SV)

— Both IMSI number series and UE device type (IMEI-TAC or IMEI-TAC SV)

Note: The MME primarily checks the configured roaming restrictions based on IMSI number series. If the roaming restrictions based on IMSI number series do not apply, for example, because they are not restricted or exempted, the MME checks the roaming restrictions based on the IMEI-TAC or the IMEI-TAC SV.

When a UE subject to roaming restrictions enters a restricted tracking area or geographical area, a configured cause code is sent to the UE in the Reject message. The cause code indicates to the UE that the service is denied or that the area is not allowed, which depends on the IMSI number series, the IMEI-TAC, or the IMEI-TAC SV that the UE belongs to.

Roaming Restrictions Based on IMEI-TAC or IMEI-TAC SV

For roaming restrictions based on IMEI-TAC or IMEI-TAC SV, the IMEI-TAC or the IMEI-TAC SV list can be associated with a cause code (#0, #11-#15) and configured as a blacklist or a whitelist.

If the IMEI-TAC or IMEI-TAC SV list is configured as a blacklist, the associated cause code (#0, #11-#15) is applied to the UEs in the IMEI-TAC or IMEI-TAC SV list in the geographical area. If the cause code configured for the geographical area is one of the roaming restriction cause codes (#11-#15), the roaming restriction cause code is sent to the UEs in the Reject messages. If the cause code configured for the geographical area is #0, the UEs are allowed to access the geographical area.

If the IMEI-TAC or IMEI-TAC SV list is configured as a whitelist, the associated cause code (#11-#15) is applied to the UEs that do not match the IMEI-TAC or IMEI-TAC SV whitelist in the geographical area. If the cause code configured for the geographical area is one of the roaming restriction cause codes (#11-#15), the roaming restriction cause code is sent to the UEs that do not match the IMEI-TAC or IMEI-TAC SV whitelist in the reject messages. If the cause code configured for the geographical area is #0, the UEs that are not matched are allowed to access the geographical area while the matched UEs are rejected. This check is applied only if a device is rejected because either of the cause codes #11-#15 are configured.

If several UE device groups are mapped to the same geographical area, the UE device groups specified by the IMEI-TAC or IMEI-TAC SV lists are not allowed to configure as different list roles.

For each geographical area, one whitelist can be configured for roaming restriction cause codes (#11-#15) and one whitelist for the exemption cause code (#0).

The exempted IMEI list can be configured to not apply the associated cause code for the UEs in the exempted IMEI list, even if the IMEI-TAC of the UEs is configured in the blacklist.

If a UE device type is specified by the IMEI-TAC in one device group, and is also specified by the IMEI-TAC SV in another device group, this results in the following:

— The associated cause code is sent based on the configuration of the IMEI-TAC SV.

— The exempted IMEI or IMEISV list is based on the configuration of the IMEI-TAC SV.

Roaming Restrictions Based on IMSI Number Series

Roaming restrictions based on IMSI number series and roaming restrictions based on IMEI-TAC or IMEI-TAC SV can also be used separately.

For a UE with an emergency PDN connection, the Roaming Restrictions feature is bypassed. When a UE with an emergency PDN connection enters the restricted areas, all non-emergency PDN connections are removed, and the emergency PDN connection is kept.

For more information on how to configure Roaming Restrictions, see Configuring Roaming Restrictions.

Roaming Restriction Cause Codes

Table 5 shows the operator-configured cause codes that are returned to the UE when an Attach, TAU, or X2-Based Handover procedure is rejected.

Table 5 Roaming Restriction Cause Codes for Rejected Attach, TAU, or X2-Based Handover Procedures

Cause code #11	PLMN not allowed
Cause code #12	Tracking area not allowed
Cause code #13	Roaming not allowed in this tracking area
Cause code #14	EPS services not allowed in this PLMN
Cause code #15	No suitable cells in tracking area

Table 6 shows the default cause code that is returned to the source MME when an S1-Based Handover procedure is rejected.

Table 6 Roaming Restriction Cause Code for Rejected S1-Based Handover Procedures

GTPv2 Cause code #81	`Relocation failure`

Table 7 shows the default cause code that is sent to the source eNodeB when an S1-Based Handover procedure is rejected, or to the target eNodeB when an X2-Based Handover procedure is rejected.

Table 7 Roaming Restriction Cause Code for Rejected S1-Based Handover Procedures or X2-Based Handover Procedures

S1-AP Cause Code	`Handover failure in target EPC/eNodeB or target system`

For IMS Emergency Service, roaming restrictions are ignored.

17.2 Access Restrictions

The license-controlled feature Access Restriction ensures that subscribers that are not allowed to access the LTE or the NB-IoT network are restricted from access. There are two ways to achieve this:

— Analyzing the Access Restriction Data IE received from the HSS

— Analyzing the IMSI number received from the UE

Note: Access restriction control requires that the HSS has coherent support for the `Access Restriction Data` IE.

Access restrictions are ignored for a UE with an emergency PDN connection if IMS emergency service is allowed for this UE. However, during mobility procedures, non-emergency PDN connections are removed if the UE is access-restricted.

Access restriction control is performed in the following cases:

— When the MME receives an `Update Location Answer` message including the `Access Restriction Data` IE during a UE-initiated Attach or Inter-MME TAU procedure.

  If a subscriber is restricted from accessing the requested network, the MME sends an appropriate Reject message to the UE with a cause code.

— When the MME receives an `Insert Subscriber Data Request` message, including the `Access Restriction Data` IE from the HSS.

If a subscriber is restricted from accessing the requested network, the MME sends a Detach message to the UE with a cause code.

— When a UE is accessing the MME.

  It is possible to define an IMSI number series to restrict a UE from accessing the LTE or the NB-IoT network. The MME analyzes the IMSI number of the UE to check if the IMSI number is allowed.

— When the MME receives a `UE CAPABILITY INFO INDICATION` message, the Cat-M UE is indicated, and MME decides to block this Cat-M UE according to the configuration of the `CatMCauseCode` parameter.

  It is possible to define an IMSI number series to restrict a Cat-M UE from accessing the LTE network. The MME analyzes the IMSI number of the UE to check if the IMSI number is allowed.

If the UE is restricted from accessing the LTE or the NB-IoT network, or if the Cat-M UE is restricted from accessing the LTE network, the MME sends an appropriate reject message to the UE with a configured cause code. For more information on the cause codes that are sent with a Reject or a Detach message, see Troubleshooting.

The MME can be configured to handle an emergency PDN connection from an unknown UE depending on the emergency profile configuration of the MME. This behavior is related to the IMEI Check feature. For more information, see IMEI Check (CLI) and Security.

17.3 Subscription-Based Restrictions

The licensed feature Subscription-Based Restrictions allows operators to regulate access to the LTE network on a subscriber level, and consists of the following two functions:

— ODB Support for PS Service

— Regional Subscription

17.3.1 ODB Support for PS Service

The barring of PS services is applied to the subscribers when the subscription restriction control is performed. The subscription restriction control is performed when the MME receives a message carrying the ODB category `All Packet Oriented Services Barred`:

— When the MME receives an `Update Location Answer` message carrying the ODB category from the HSS during a UE-initiated Attach procedure, the MME rejects the Attach procedure with a cause code.

— When the MME receives an `Update Location Answer` message carrying the ODB category during an Inter-MME TAU procedure, the MME accepts the

TAU procedure first and then immediately detaches the UE with a cause code.

— When the MME receives an `Insert Subscriber Data Request` message carrying the ODB category from the HSS, the MME detaches the UE with a cause code.

Table 8 presents the cause code that is used for subscription restriction control for a home subscriber and a roaming subscriber.

Table 8 Cause Codes Used for Subscription Restriction Control

Subscriber	Configuration of the node function odb_attach_reject_nas_cc_remap(1)	Cause Code	Description
Home subscriber	on	Cause code #15	No suitable cells in tracking area
	off	Cause code #14	EPS services not allowed in this PLMN
Roaming subscriber	N/A	Cause code #14	EPS services not allowed in this PLMN

(1) The `odb_attach_reject_nas_cc_remap` node function is applicable only for ATTACH reject caused by ODB for home subscribers.

For ODB subscribers whose access to PS services is regulated, all APNs are blocked. An ODB-free APN list can be configured to define up to 50 APNs that ODB subscribers can access. The ODB subscribers can still access the APNs in the ODB-free APN list when the following conditions are met:

— When the subscription_restriction parameter is activated using the modify_feature_state CLI command.

— When the odb_allowed_apn_list parameter is enabled using the modify_node_function CLI command.

— The APNs that are configured in the ODB-free APN list also exist in the HSS subscription data.

The MME blocks all APNs except the APNs that are configured in the ODB-free APN list. When the ODB-free APN list is empty, all APNs are blocked. The ODB-free APN list is applicable for both home subscribers and roaming subscribers.

Note: To apply the ODB-free APN list to roaming subscribers, enable the odb_allowed_apn_list_for_roaming_subscriber parameter using the modify_node_function CLI command.

The ODB function is not applicable to the emergency service.

For more information on configuring ODB, see Configuring Session and Mobility Management.

17.3.2 Regional Subscription

The Regional Subscription feature defines regional subscription areas, or regions, where access is either allowed or restricted for a specific subscriber. The regions are identified by regional subscription zone identities, containing zone codes, configured for each subscriber in the HSS. In the MME, each zone code is associated with one or several geographical areas, where each geographical area represents a tracking area, a set of tracking areas, or a complete PLMN, defining the regions where the subscriber is allowed or restricted.

The subscription data requested from the HSS by the MME for a subscriber contains a list of zone codes that apply to the subscriber within the current PLMN. If the SGSN-MME does not receive any zone code information in the subscription data, or receives a zone code that does not correspond to the zone code configured for the regional subscription area, regional subscriptions do not apply.

Note: Regional subscription restrictions are not applicable to emergency services, and are only applicable to the S6a interface.

Regional Subscription allows the user to perform the following actions:

— Restrict parts of a PLMN, and allow the rest of the PLMN implicitly

— Allow part of a PLMN, and restrict the rest of the PLMN implicitly

— Override roaming restrictions in a PLMN

— Prevent access to an external PLMN

For more information on configuring Regional Subscription, see Configuring Regional Subscription.

Regional subscription control is performed when the UE performs a mobility procedure, for example, Attach, TAU, Handover, or CP Relocation procedures. If the UE is restricted by regional subscription control, and the RsCauseCode parameter is not configured, the mobility procedure is rejected and a hardcoded cause code is returned to the UE. Table 9 presents the hardcoded cause codes that are used for regional subscription control for a home subscriber and a roaming subscriber. If a cause code is configured through the RsCauseCode parameter, it replaces the hardcoded cause code to be sent to the UE. For more information about the RsCauseCode parameter, see Regional Subscription (CLI).

Table 9 Hardcoded Cause Codes Used for Regional Subscription Control

Subscriber	Cause Code	Description
Home subscriber	Cause code #15	`No suitable cells in tracking area`
Roaming subscriber	Cause code #13	`Roaming not allowed in this tracking area`

The MME requests regional subscription data from the HSS according to the following:

— When the MME receives an `Update Location Answer` message from the HSS, the message can include zone codes. If the MME receives zone codes from the HSS, the MME compares the received the zone codes with any zone codes in the regional subscription configuration in the MME, and decides if the subscriber gets access.

— When the MME receives an `Insert Subscriber Data Request` message from the HSS, the message can include zone codes. If the MME receives zone codes from the HSS, the MME compares the received zone codes with any zone codes in the regional subscription configuration in the MME, and decides if the subscriber gets access.

— When the MME receives a `Delete Subscriber Data Request` message with the `Regional Subscription Withdrawal` bit `0` set to `1`, the MME deletes the zone codes stored in the subscription data.

Note: The list of forbidden tracking areas in the Handover Restriction List (HRL) is based on the Roaming Restriction configuration. If the eNodeB initiates a Handover procedure based on the HRL at any time, the handover is managed by the MME in an appropriate manner.

If the licensed feature Subscription-Based Restrictions is granted, the SGSN-MME sets the `Regional Subscription` feature bit in the `Feature-List` AVP, regardless of the feature state of `regional_subscription`.

17.4 Handover Restriction List

The `Handover Restriction List` IE can be included in `Initial Context Setup Request`, `Handover Request`, and `S1-AP Downlink NAS Transport` messages, which steers a UE in the ECM-CONNECTED state into selecting a target PLMN during Handover procedures.

The `Handover Restriction List` IE can include the following IEs:

Serving PLMN IE

This IE is mandatory and contains the current PLMN for the UE.

Equivalent PLMNs IE

This IE is included only if it is configured in the MME.

Forbidden TAs IE

This IE is included only if it is configured in the MME, and the Roaming Restrictions feature and the Regional Subscription feature are activated.

Forbidden LAs IE

This IE is included only if it is configured in the MME, and the Roaming Restrictions feature and the Regional Subscription feature are activated.

Forbidden inter-RATs IE

This IE is included if the Access Restriction feature is activated and the access restriction data is available in the subscription data.

NR Restriction IE

This IE is included if the UE is restricted from using NR as secondary RAT.

For information on the configuration of Allowed PLMNs, Forbidden TAs and Forbidden LAs, see Configuring a Handover Restriction List for LTE Access.

17.5 Reject Cause Code for Undefined IMSI Number Series

It is possible to configure the Reject Cause Code sent to the UE during initial Attach and TAU procedures when the IMSI number series is not defined in the MME. For more information, see Configuring Session and Mobility Management.

17.6 CSG Restrictions

The MME checks if CSG restrictions apply when the license-controlled feature MME Support for Closed Subscriber Group is enabled and the UE is accessing a CSG cell. If the `CSG ID` for the CSG cell is included in the CSG subscription data for the UE and the `CSG ID` does not expire, the UE is permitted to access the CSG cell. Otherwise, the UE is rejected. If the UE is using IMS Emergency Service or emergency is indicated in the Extended Service request message, the UE is not rejected because of CSG restrictions. If the UE is using IMS Emergency Service, non-emergency bearers are deleted.

CSG restrictions apply to the following procedures:

— Attach

— Detach

— Service Request

— Extended Service Request

— TAU

— Handover

Note: The MME does not support retrieving CSG subscription data from the HSS for another PLMN than the registered PLMN.

Therefore, during X2-Based Handover, if the target cell for the handover is located in another PLMN, the CSG check fails and a Path Switch Request Failure message is sent to the target Home eNodeB. The UE is detached with reattach required. The UE is CSG-restricted if applicable in the following Attach based on the CSG subscription data valid for the new PLMN.

During the same conditions, for S1-Based Handover, the source MME sends a Handover Preparation Failure message to the source Home eNodeB.

Table 10 presents the cause code sent to the UE when a mobility procedure is rejected because of CSG restrictions.

Table 10 CSG Restriction Cause Code Sent to the UE

Cause code #25	NOT_AUTHORIZED_FOR_THIS_CSG

Table 11 presents the cause code sent to the HeNB/HeNB gateway when a mobility procedure is rejected because of CSG restrictions.

Table 11 CSG Restriction Cause Code Sent to the HeNB or HeNB Gateway

Cause code #38	INVALID_CSG_ID

For more information on CSG restrictions, see Closed Subscriber Group and EBM Cause Codes.

17.7 Inter-PLMN Mobility Restriction

The Inter-PLMN Mobility Restriction function blocks the received TAU requests during Inter-MME TAU procedures. The Inter-PLMN Mobility Restriction function also applies to the ISC SGSN-MME TAU procedures. For more information, see Inter-System Mobility Management.

When the MME receives a TAU Request from the UE, the MME checks if the Inter-PLMN Mobility Restriction applies and derives the PLMN from the old GUTI that is included in the TAU Request message. If the PLMN is restricted in the following scenarios, the MME rejects the TAU Request with a reject message

containing the EMM cause code `UE_identity_cannot_be_derived_by_the_network`:

— The old PLMN is not native to the SGSN-MME and the old PLMN is in the Inter-PLMN Mobility Restriction blacklist.

— The old PLMN is not native to the SGSN-MME and the old PLMN is not in the Inter-PLMN Mobility Restriction whitelist.

— The old PLMN is not native to the SGSN- MME and no PLMN is configured for the Inter-PLMN Mobility Restriction.

Note: It is not possible for the user to configure a PLMN both in the local PLMN list and the Inter-PLMN Restriction list.

For information on the configuration of Inter-PLMN Mobility Restriction, see Configuring Session and Mobility Management.

17.8 IMS Emergency Service Restrictions

It is possible to restrict specific users from using IMS Voice services or IMS Emergency Service in a tracking area. If a UE is subjected to this restriction and initiates an emergency Attach within the radius of the restricted tracking area, the UE initiated mobility procedures are also denied access to the MME. For information on configuring IMS Emergency Restrictions, see Configuring MMTel Service.

18 Serving Network Change Report to GW

The `Serving Network` IE contains the serving PLMN. If the `ServingNetworkChangeReport` parameter is set to **on**, and the UE-serving PLMN is changed during the TAU without SGW Relocation, Service Request, and Handover procedures, the MME includes the `Serving Network` IE, containing the current UE-serving PLMN, in the Modify Bearer Request message to notify the SGW of the serving PLMN change.

During an Inter-MME Handover procedure, the source MME includes the `Serving Network` IE, containing the current UE-serving PLMN, and the selected PLMN-ID in the Forward Relocation Request message. The target MME includes the `Serving Network` IE in the Modify Bearer Request message to inform the SGW of the change of the serving network if the following conditions are met:

— The `ServingNetworkChangeReport` parameter is set to **on**.

— The current serving network for the PDN has not yet been reported to the SGW.

19 Network-Provided Location

As the IMS requests the ULI information of UE, that is the last known ULI, the ULI time stamp, and the UE time zone, the session management messages sent from the MME to SGW contain the `ULI`, `ULI Timestamp`, and `UE Time Zone` IEs in the following procedures:

— LTE Mobility Management

— LTE Session Management

— SRVCC

That is, the MME notifies the SGW of the last known ULI, ULI time stamp, and UE time zone. Then the ULI information is forwarded to the PGW, the PCRF, and the IMS, as described in Figure 39.

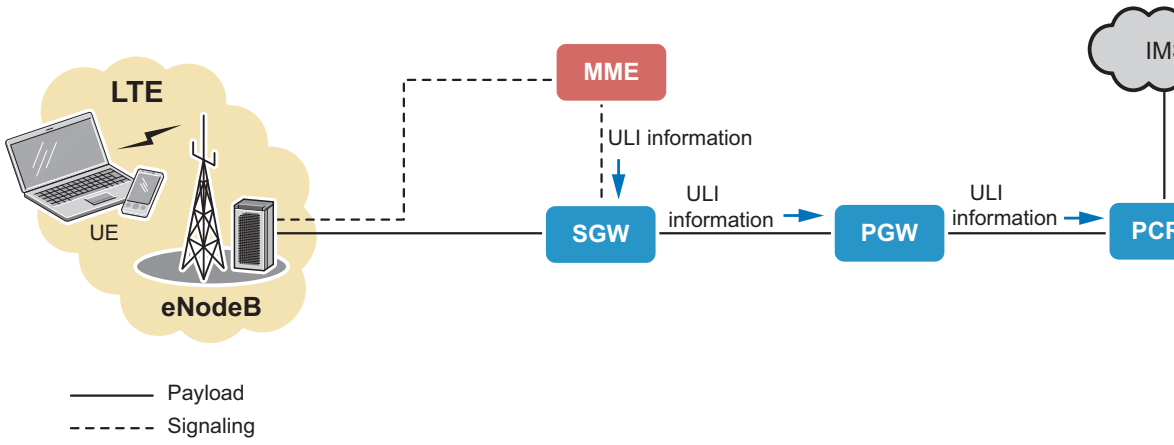


Figure 39 ULI Information

The ULI information provided in PCC-based network locations has the following benefits:

— Determines the network location of the UE during emergency calls

— Provides location-based charging for IMS voice services

— Reduces HSS interactions and minimizes the additional signaling

19.1 Network-Provided Location in Mobility Management Procedures

The MME notifies the SGW of the last known ULI, the ULI time stamp, and the UE time zone through the `Create Session Request` and the `Delete Session Request` messages in the following mobility management procedures:

— UE-Initiated Attach

— UE-Initiated Detach

— MME-Initiated Detach

— HSS-Initiated Detach

— TAU with SGW Relocation

— X2-Based Handover with SGW Relocation

— S1-Based Handover with SGW Relocation

— RAU to S4-SGSN with SGW Relocation

— IRAT Handover from LTE to WCDMA over Gn

— IRAT Handover from LTE to WCDMA with SGW Relocation

Note: The `Create Session Request` message does not include the `ULI Timestamp` IE. The `Create Session Request` message in the S1-based Handover with SGW Relocation procedure only includes the `UE Time Zone` IE.

If the ULI information (ECGI and TAI) is included in the `UE Context Release Complete` message in the S1 release procedure, the MME stores the ULI information.

19.2 Network-Provided Location in Session Management Procedures

The MME notifies the SGW of the last known ULI, the ULI time stamp, and the UE time zone through the `Create Bearer Response`, `Update Bearer Response`, `Delete Bearer Response`, `Delete Bearer Command`, `Create Session Request`, and `Delete Session Request` messages in the following session management procedures:

- Activation of dedicated bearers
- PGW-Initiated Bearer Modification with Bearer QoS Update
- HSS-Initiated Subscribed QoS Modification
- PGW-Initiated Bearer Modification without Bearer QoS Update
- MME-Initiated Deactivation of Bearers
- PGW-Initiated Deactivation of Bearers
- MME-Initiated PDN Disconnection
- UE-Initiated PDN Disconnection
- UE-Requested PDN Connectivity

Note: The `Create Session Request`, `Create Bearer Response`, and `Update Bearer Response` messages only include the `ULI` and the `UE Time Zone` IEs. The `UE Time Zone` is included in the `Delete Session Request` message only if the operation indication is set and the UE time zone is changed.

If the ULI information (ECGI and TAI) is included in the `E-RAB Release Response` or the `E-RAB Release Indication` message in the following procedures, the MME stores the ULI information:

- MME-Initiated Deactivation of Bearers
- PGW-Initiated Deactivation of Bearers
- MME-Initiated PDN Disconnection

For more information about session management procedures, see LTE Session Management.

19.3 Network-Provided Location in SRVCC Procedures

The MME notifies the SGW of the last known ULI, the ULI time stamp, and the UE time zone through the `Delete Bearer Command`, `Delete Bearer Response`,

and the `Delete Session Request` messages in the following SRVCC procedures:

— SRVCC procedure to UTRAN with PS Handover

— SRVCC procedure to UTRAN/GERAN with DTM Support

For more information about SRVCC procedures, see EPS Support for CS Services.

20 Network Names and Time Zones

Network Names is a basic function that allows sending both full and short network names to the UE. For information about configuring the network names, see PLMN Identification (CLI). For information on how to configure customized network names based on IMSI number series and geographical areas, see Configuring Session and Mobility Management.

The Time Zones function sends the UE local time zone to the SGW, which enables time-based charging in the SGW, the PGW, or both. For information on how to configure the Time Zones function, see Configuring GSM and WCDMA Time Zones and Configuring LTE Time Zones.

20.1 Time Zones

The tracking areas of a PLMN can be deployed over a geographically large area which can span over more than one time zone. The Time Zones function provides the UE with the local time of the geographical area where the UE is located, for example, at Attach.

The local time is defined by assigning a time zone to a geographical area in the local MME configuration. When the UE moves between tracking areas, the MME checks if there is a change in the local time zone of the UE and updates the UE if it has changed.

The MME can send the UE local time zone to the SGW or another MME by including the `UE Time Zone` IE in the following GTPv2 messages:

- `Create Session Request`
- `Create Bearer Response`
- `Modify Bearer Request`
- `Update Bearer Response`
- `Delete Bearer Response`
- `Context Response`
- `Forward Relocation Request`

During the TAU and Service Request procedures, the MME includes the `UE time zone` IE in the `Modify Bearer Request` message sent to the SGW when the UE local time zone changes.

When the DST flag changes for a time zone, the MME starts the `ServiceReqDeferredDuration` timer for the time zone if the `ServiceReqDeferredReport` is set to `on`. Before this timer expires, the MME tries

to defer the DST change reporting in the service request procedure for UEs in the geographical area with the time zone. When the first `Service Request` message from a UE is received and the UE ULI does not change, the MME generates a randomized time stamp between the current time and the DST change time plus the `ServiceReqDeferredDuration` value for the UE. If the randomized time stamp equals the current time, the MME reports the DST changes immediately to the SGW through the `Modify Bearer Request` message in the first service request procedure. Otherwise, the MME defers the DST reporting to the SGW until the randomized time stamp has reached, the UE sends another `Service Request` message, and the DST change has not been reported in other procedures.

The DST change reporting in other procedures, such as the Attach, TAU, and Handover procedures, is not affected by the deferring DST change reporting function.

When the `ServiceReqDeferredDuration` timer expires, the MME handles the DST change reporting in the Service Request procedure in the normal way.

The deferring DST change reporting function is also applicable for the UE Restoration upon the Service Request procedure. For more information, see Geographically Redundant Pool.

21 TAI List

A TAI list consists of TAIs, representing the tracking areas that the UE can enter without initiating a TAU procedure. Based on the configuration, the TAI list is created based on either the visited TAIs (see TAI List Based on Visited TAIs on page 141) or the TAC list received from the DNS (see TAI List Based on TAC List from DNS on page 142).

The SGSN-MME creates a TAI list and sends it to the UE, included in the `Attach Accept` and `TAU Accept` messages. If the TAI list is changed, the new version is sent to the UE at periodic TAU procedures.

For more information on how to configure TAI list options, see Configuring Session and Mobility Management.

21.1 TAI List Based on Visited TAIs

The TAI list includes the current TAI and the previously visited TAIs. At an Attach or TAU, the current TAI, and if received, the last visited TAI, are added to the list, if not yet included. If the current and last visited TAI are already included, the time stamp is updated. The time stamp indicates the last time the UE visited a specific TAI. The time stamp is also updated when there is signaling from the UE.

The maximum number of TAIs on a TAI list is 16, including the current TAI. If the list has reached the maximum number, the oldest TAI is removed from the list.

The maximum length of the TAI list can be changed by giving the MaxTaiListLength parameter a new value (1-16). If the MaxTaiListLength parameter is set to '1', only the current TAI is included in the list ('1' is the default value of the parameter). If the parameter is set to '2', the last visited TAI is also included in the list.

A TAI is removed from the TAI list if its age, based on the time stamp, exceeds the value defined by the MaxTaiAge parameter. In this case, the TAI is removed when the next TAU or Attach procedure is performed. The TAI list is not updated during a Paging procedure.

The SGSN-MME creates and updates the TAI list and checks it for inconsistency using the current TAI as reference. The TAI list must meet the following criteria:

— All TAs must be served by the same SGSN-MME.

— All tracking areas with configured Wi-Fi UE Locator information must be served by the same Wi-Fi UE Locator.

Note: This is only applicable if the Wi-Fi Integration feature is enabled. For more information, see Wi-Fi Integration.

— The location area selected for the current TAI must be selected for all the other TAIs in the TAI list.

  Note: This is only applicable if the SGs interface is used. For more information, see EPS Support for CS Services.

— All tracking areas must belong to the same PLMN.

— All tracking areas must have the same Time Zone name.

— All tracking areas must have the same set of Equivalent PLMNs for the actual UE.

  Note: This is only applicable if the Selective Equivalent PLMN feature is used.

— If customized network names have been enabled, the UE must have the same customized network name for all tracking areas in the TAI list.

— The UE must have roaming access to all tracking areas on the list.

— All tracking areas must be served by the currently used SGW.

— All tracking areas must belong to the same location-based IP address allocation area or to a normal area.

  Note: This is only applicable if the Location Based IP Address Allocation feature is used.

If no inconsistencies are found, the SGSN-MME sends a TAI List IE to the UE. If inconsistencies are found, the faulty TAIs are removed from the TAI list before the list is sent to the UE.

21.2 TAI List Based on TAC List from DNS

The TAC list is defined in the DNS. The SGSN-MME performs a DNS U-NAPTR query to retrieve a TAC list for the current tracking area. The SGSN-MME converts the TAC list into a TAI list. Duplicate TACs in the TAC list are removed. For information on the U-NAPTR procedure, see the following:

— IETF RFC3402

— IETF RFC3403

— IETF RFC4848 (an extension of IETF RFC3958)

The maximum allowed length for the TAC list is 14 entries. If the TAC received from the DNS is longer than 14 entries, the list is truncated. This leaves two free entries on the TAI list, which are used for the current TAI and the last visited TAI if they are not included in the list of TACs received from the DNS.

22 T-ADS Procedure

T-ADS procedures are used for 3GPP mobility when the IMS-Based Telephony - MMTel feature is used on the LTE side.

To determine whether to route a voice call to circuit-switched or to packet-switched access, the SCCAS must be informed whether the UE that is registered in the IMS is camping on an IMS Voice over PS-capable access. For this purpose, network-based T-ADS is used. The T-ADS procedures provide the HSS with the time stamp of the UE current tracking area and the associated RAT Type, and an indication of whether IMS Voice over PS is supported in the current tracking area.

23 ADD for LTE

The ADD function for LTE enables a timely update of the latest IMEISV of a UE in the MME.

If the security functions are not performed, even with an IMEISV stored in the UE context, the MME fetches the latest IMEISV by using the `Identity Request` and `Identity Response` messages. The ADD function for LTE is performed during the Attach procedure, and can also be performed during the following mobility procedures, depending on the configuration of the `ImeiRefetchEnabled` parameter:

— Inter-MME TAU

— Inter-MME handover

— IRAT Handover from WCDMA to LTE over S3

— IRAT Handover from WCDMA to LTE over Gn

Once the MME detects that the IMEISV of a UE changes, the MME updates the HSS and the SGW with the new IMEISV. The HSS is updated by an `Update Location Request` or a `Notify Request` message. The SGW is updated by the `Modify Bearer Request` and the `Create Session Request` messages.

For information about how to configure the ADD function for LTE, see Configuring Session and Mobility Management.

Network Impact

When the ADD function is enabled, the `MEI` IE is added in the `Modify Bearer Request` message during the affected procedures when both of the following conditions are met:

— The `MeiInModifyBearerReq` parameter is set to `on`.

— The IMEISV of a UE changes.

The SGW must also support the `MEI` IE in the `Modify Bearer Request message` over the S11 interface.

24 Multiple SIM Subscription

24.1 Multiple SIM Support

The SGSN-MME supports mobile subscribers with multiple devices and IMSI numbers using the same MSISDN during a mobility management procedure.

24.2 Additional MSISDN Support

The SGSN-MME supports Additional MSISDN (A-MSISDN), which is available for Multiple SIM Subscriptions. For SRVCC procedures, a unique A-MSISDN can be defined in the subscription data in the HSS for each SIM, in addition to the common MSISDN.

The SGSN-MME indicates support for A-MSISDN by setting bit 31 in the Feature-List-ID 1 AVP in the following messages sent to the HSS over the S6a interface:

— `Update Location Request`

— `Insert Subscriber Data Answer`

— `Delete Subscriber Data Answer`

The HSS sends the A-MSISDN in a Subscription Data AVP in `Update Location Answer` and `Insert Subscriber Data Request` messages.

If an A-MSISDN is available, the source SGSN-MME uses it instead of the common MSISDN. In this case, A-MSISDN is used as the Correlation MSISDN (C-MSISDN) in SRVCC and PS Handover procedures over the following interfaces:

— Sv, for SRVCC PS to CS Requests

— S3, for Forward Relocation Requests

— S10, for Forward Relocation Requests

During an SRVCC procedure, using A-MSISDN as the C-MSISDN enables the MSC to transfer the correct call anchored in the IMS.

The SGSN-MME also supports the A-MSISDN Withdrawal bit 16, in AVP Delete-Subscriber-Data-Request Flags to the HSS, which triggers theSGSN-MME to delete an A-MSISDN from the UE context.

25 Resilience and Overload Protection

Resilience and overload protection protect the SGSN-MMEE from failures and keep the SGSN-MME functional. The recovery mechanisms primarily provide a non-stop mode of operation of the SGSN-MME, making it possible to recover from both software and hardware failures with minimal inconvenience for the attached subscribers. Redundancy makes it possible for the SGSN-MME to handle various types of failures and maintain its system operation. The SGSN-MME overload protection mechanisms protect internal and external resources, and perform traffic prioritization. For more information, see Resilience and Overload Protection.

26 Diameter S6a Error Code to NAS Cause Code Mapping

If the MME receives an Authentication Information Answer message or an Update Location Answer message with a Diameter S6a error code from the HSS, the MME can map the S6a error code to a configurable NAS cause code and send the NAS cause code to the UE in an Attach, TAU or Service Reject message. For an overview of Diameter S6a error code to NAS cause code mapping, see Table 12.

Table 12 Diameter S6a Error Code to NAS Cause Code Mapping

Diameter S6a Error Code	Default NAS Cause Code	Alternative NAS Cause Codes	Parameter	CLI Command
DIAMETER_ERROR_RAT_NOT_ALLOWED	#15 (No suitable cells in tracking area)	#13 (Roaming not allowed in this tracking area) #12 (Tracking area not allowed)	CcS6aRatNotAllowed	modify_nas_cc_mapping
DIAMETER_AUTHORIZATION_REJECTED	#15 (No suitable cells in tracking area)	#17 (Network failure) #42 (Severe network failure)	CcS6aAuthorizationRejected	modify_nas_cc_mapping
DIAMETER_UNABLE_TO_DELIVER			CcS6aUnableToDeliver	
DIAMETER_REALM_NOT_SERVED			CcS6aRealmNotServed	
DIAMETER_ERROR_ROAMING_NOT_ALLOWED	Without error diagnostics: #11 (PLMN not allowed)	#15 (No Suitable Cells in Tracking Area)	diameter_nas_roaming_not_allowed_cc_remap	modify_node_function
	With error diagnostic: #14 (EPS services not allowed in this PLMN)			
DIAMETER_ERROR_USER_UNKNOWN	#8 (EPS services and non-EPS services not allowed)	#15 (No Suitable Cells in Tracking Area)	diameter_nas_user_unknown_cc_remap	modify_node_function
DIAMETER_UNABLE_TO_COMPLY	#17 (Network Failure)	#42 (Severe Network Failure)	diameter_nas_severe_nw_failu	modify_node_function

Diameter S6a Error Code	Default NAS Cause Code	Alternative NAS Cause Codes	Parameter	CLI Command
DIAMETER_INVALID_AVP_VALUE DIAMETER_AVP_UNSUPPORTED DIAMETER_MISSING_AVP DIAMETER_RESOURCES_EXCEEDED DIAMETER_AVP_OCCURS_TOO_MANY_TIMES DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE			re_cc_remap_home	
DIAMETER_UNABLE_TO_COMPLY DIAMETER_INVALID_AVP_VALUE DIAMETER_AVP_UNSUPPORTED DIAMETER_MISSING_AVP DIAMETER_RESOURCES_EXCEEDED DIAMETER_AVP_OCCURS_TOO_MANY_TIMES DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	#17 (Network Failure)	#42 (Severe Network Failure)	diameter_nas_severe_nw_failure_cc_remap_roamers	modify_node_function

27 UE Registration Quarantine Timer (T3402)

The UE registration quarantine timer value controls when to retry network access on a temporary network failure. The UE registration quarantine timer value can be configured based on IMSINS. For more information about configuring the timer, see Configuring Session and Mobility Management.

If the NasUeRegistrationQuarantine parameter is set to `enabled` and the IMSINS is configured in the UE registration quarantine profile table, the MME sends the UE registration quarantine timer value in the `Attach Accept`, `TAU Accept` and `Attach Reject` messages to the UE.

If the NasUeRegistrationQuarantine parameter is set to `disabled`, the MME does not send a UE registration quarantine timer to the UE, so the UE waits 12 minutes (720 seconds) for network access retries.

28 Operation and Maintenance

28.1 Parameters

To display the configuration classes and parameters related to LTE Mobility Management, use the get_config_area –can CLI command for the following configuration areas:

- AdaptivePaging
- ClosedSubscriberGroup
- EmergencyCall
- EquivalentPlmn
- HandoverRestrictionList
- ImsiNumberSeries
- InterfaceS1MME
- InterfaceS11
- Mps
- Plmn
- RegionalSubscription
- RoamingRestrictions
- SgsnMme
- TimeZones

28.2 Counters

The following counters and PmGroups are valid for LTE Mobility Management:

- SGSN-MME_Mobility_hho_E
- SGSN-MME_Mobility_HO_E
- SGSN-MME_Mobility_MM_E
- SGSN-MME_Mobility_MM_Hss

— SGSN-MME_Mobility_UnstableSubscribers

28.3 Alarms and Events

The following alarms and events are valid for LTE Mobility Management:

— nwcMmeEnodebUpdateIncomplete

28.4 Logs

The Mobility Event Log is valid for LTE Mobility Management. For descriptions of the log file, refer to Operation and Maintenance Description and Mobility Event Log.

28.5 EBM

For descriptions of sub-cause codes and EBM events, see EBM Cause Codes and EBM Events and Parameters.

29 Compliance

For compliance information on 3GPP interfaces, see the following references:

- SoC with 3GPP TS 23.401
- SoC with 3GPP TS 24.301
- SoC with 3GPP TS 29.272
- SoC with 3GPP TS 36.413