



Cloud Mobility Manager, Release
22.5, Operating Documentation, v.
1

MME Feature Overview

DN09131794

Issue 14-0

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia. This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2022 Nokia.

Table of Contents

Summary of changes	38
1 Introduction	43
2 Standards updates	44
2.1 Release 12 and Release 13 standards update for MME (Feature f10001-01)	44
2.2 Release 13 and Release 14 standards update for MME (Feature f10002-01)	47
2.3 Release 14 and Release 15 standards update for MME (Features f10002-03, f10002-04, f10002-05)	52
2.4 Release 14 and Release 15 baseline update for UE monitoring (Feature f11015-02)	58
2.5 MME support for 3GPP standards update (Feature f10002-06)	60
2.6 MME support for 3GPP standards update (Feature f10002-07)	61
2.7 MME support for 3GPP standards update release 16 for September 2019 and December 2019 - phase 1 (Feature f10002-08)	63
2.8 MME support for 3GPP standard update release 16 for March/June/Sept/Dec 2020 and March 2021 - phase 2 (Feature f10002-09)	65
3 Mobility management	68
3.1 Attach	68
3.1.1 Attach (Feature m10001-01)	68
3.1.2 Initial Attach Indication setting in ULR (Feature m11327-01)	69
3.1.3 8K UE radio capability information (Feature m10907-02)	69
3.1.4 Treating non-emergency PDN connection as a new PDN connection at attach (Feature f10164-01)	71
3.1.5 Restricting the number of attached UEs per TA (Feature f10168-01)	71
3.1.6 Always send EPS Network Support Feature Support IE in Attach and TAU Accept messages (Feature f10173-01)	72
3.1.7 MME support for optional IE for T3402 (Feature f10926-01)	72
3.1.8 Multi SIMs with same MSISDN (Feature f10411-01)	72
3.1.9 Scaling the maximum IMSI range services to 10K (Feature f14619-01)	73
3.2 Authentication and security	73
3.2.1 Authentication (Feature m10001-01)	74
3.2.2 Air interface security support	74
3.2.3 NAS signaling protection (Feature m10607-01)	74
3.2.4 AES ciphering and integrity protection (Feature m10607-02)	75
3.2.5 Null ciphering and integrity protection (Feature m10607-02)	75
3.2.6 SNOW 3G ciphering and integrity protection (Feature m10607-02)	76
3.2.7 ZUC ciphering and integrity protection (Feature m10612-01)	77
3.2.8 Disabling Immediate Response Preferred AVP on S6a (Feature m11317-01)	77
3.2.9 Configuration of authentication frequency for IRAT TAU procedure (Feature m30106-01)	78

3.2.10 Configurable repetition rates for authentication (Feature f10404-01)	79
3.2.11 MME support for authentication frequency per IMSI range (Feature f10423-01)	80
3.2.12 MME support for GUTI reallocation upon expiration of refresh timer (Feature f10414-01)	80
3.3 HSS interaction	80
3.3.1 HSS interworking (Feature m10001-01)	81
3.3.1.1 HSS user profile management	81
3.3.2 Active-APN AVP as mandatory (Feature m11329-01)	83
3.3.3 NOR modification (Feature m11334-01)	84
3.3.4 IMEISV update to HSS through NOR (Feature m10001-01)	84
3.3.5 Configurable Destination Realm for IMSI series (Feature m11311-01)	84
3.3.6 Reset ID across S6a interface upon HSS restart after failure (Feature f11305-01)	86
3.3.7 Release 14 Inclusion of modified/deleted subscription data with the RSR (Feature f11311-01)	87
3.3.8 MME support for HSS reset enhancement (Feature f11345-01)	88
3.4 IMEI check/validation	89
3.4.1 IMEI checking (S13) (Feature m10205-02)	89
3.4.2 IMEI validation (Feature m11020-01)	93
3.4.3 Exclude the vendor specific application ID (Feature f11335-01)	94
3.4.4 MME EIR enhancements for TAU procedure EIR queries and MSISDN inclusion in ECR (Feature f11309-01)	94
3.4.5 EIR check result of Equipment Unknown to attach successfully (Feature f11309-03)	95
3.4.6 IMEI check for roammers (Feature f10416-01)	95
3.4.7 MME support for locally provisioned IMEI-TACs rejection list (Feature f10422-01)	96
3.4.8 MME support for selective IMEI-based operator policies (Feature f10422-02)	97
3.4.9 MME support for IMEI and TAC/SV ranges (Feature f14620-01)	98
3.4.10 CMM support for EIR enhancements (Feature f11309-02)	99
3.5 Detach	100
3.5.1 Detach (Feature m10000-04)	100
3.5.2 Enhanced handling of network-initiated detach (Feature m10143-01) ...	101
3.5.3 Immediate detach after receiving barring of packet oriented services (Feature m10124-01)	102
3.5.4 2G/3G UE not detached upon moving to a co-located MME (Feature f52038-01)	102
3.5.5 TA group based handling enhancement (Feature f10123-02)	103
3.5.6 Mass detach of all UEs on a TA group (Feature f52060-01)	104
3.5.7 CMM support for CLI command to explicitly detach all UEs for an input roaming PLMN (Feature f10428-01)	105

3.6 Reachability and paging	106
3.6.1 Impact of paging policy provisioning	117
3.6.2 Monitoring of paging message traffic	119
3.7 Paging	120
3.7.1 MME support for 23.272 CR 706 (Feature m30101-06)	120
3.7.2 Paging policy selection based on QoS Class Identifier (QCI) (Feature m10202-01)	121
3.7.3 Paging discrimination by Paging Priority Indication (Feature m11004-04)	122
3.7.4 MME support for 6 byte UE Radio Capability for Paging IE (Feature f10925-01)	122
3.7.5 SGs paging enhancements (Feature m30114-01)	123
3.7.6 MME support to add S1-AP paging priority to paging profiles (Feature f10203-01)	123
3.7.7 Paging 1200 eNBs (Feature f10204-01)	124
3.7.8 Extending PPI paging to include QCI 65, 66, 69, and 70 (Feature f10201-02)	125
3.7.9 MME support for QCI 67 to support push-to-talk video (MCVideo) (Feature f10220-02)	125
3.7.10 MME support for Assistance Data for Recommended Cells (Feature f10221-01)	126
3.7.11 Paging gap control based on paging type (Feature f10202-01)	126
3.7.12 MME support for enhanced condition to trigger page gap timer (Feature f10227-01)	127
3.7.13 Pre-emption of paging by overlapping DDN (Feature f10224-01)	128
3.7.14 MME support for paging when cause code received in UE Context Release Request with cause code = Inter-RAT Redirection (Feature f10226-01)	129
3.7.15 MME support for paging upon T-ADS received in IDR message (Feature f10228-01)	130
3.8 Tracking area management	130
3.8.1 Intra-MME tracking area update (Feature m10001-01)	130
3.8.2 Static tracking area lists (Feature m10001-02)	131
3.8.3 Removing static provisioning of TAC on MME for eNB access (Feature m10916-01)	132
3.8.4 Basic and enhanced automatic neighbor list generation (Feature m10210-02, m10210-03)	134
3.8.5 Automatic neighbor list generation for up to three TAs (Feature m10210-05)	137
3.8.6 Idle mode TAU handling enhancements (Feature m10144-02)	138
3.8.7 Operator controlled TAU suppression (Feature m10215-01)	139
3.8.8 Rejecting node relocating TAU with update type periodic (Feature m10155-01)	143
3.8.9 UE activity notification (Feature m10105-01)	144
3.8.10 Configuration of MME relative capacity per tracking area (Feature	

m10725-01)	145
3.8.11 TAI/LAI mapping so that MME can select LAI from PLMN not matching UE PLMN (Feature f11811-01)	147
3.8.12 Adding default TAC mapping to TA discovery provisioned parameters (Feature f11813-01)	147
3.8.13 MME support for enhanced TA discovery auto-provisioning (Feature f11813-02)	148
3.8.14 MME support for increased number of region TAC and LAC groups (Feature f80015-01)	149
3.8.15 MME support for increased number of TAI of 20K (Feature f10567-01)	149
3.8.16 MME support for sending configuration update on data changes (Feature f10934-01)	149
3.8.17 MME support for preserving VLR for sending NOR to HSS for SGSN to MME tracking area update procedure (Feature f10425-02)	150
3.8.18 CMM support for multiple TAC operation trigger enhancements (Feature f14622-01)	150
3.8.19 MME support for combined attach without CS (Feature f10426-01)	151
3.8.20 MME support for ignoring malformed PDN connection in mobility scenario(s) (Feature f13501-08)	151
3.9 Handovers	152
3.9.1 Mobility and intra-MME handover with X2 interface (Feature m10001-01)	152
3.9.2 MME-assisted S1-based eNB handoff (Feature m10900-01)	153
3.9.3 MME continuation of S1 handover procedure due to CIDF/failure/no response (Feature m10915-01)	154
3.9.4 Include Handover Restriction List always (Feature f10505-01)	155
3.9.5 CMM support for sending HRL in all messages where CMM supports HRL IE (Feature f10910-03)	155
3.9.6 Change retransmission timer for E-RAB setup request (f10931-01)	155
3.9.7 Error handling in Create Session Response for PDN Connectivity Request type of handover (Feature f10565-01)	156
3.9.8 MME support for QCI1 HO attempt rejection (Feature f10502-04)	156
3.9.9 MME support for fail HHO with SRNS if indirect forwarding tunnel cannot be established (Feature f11816-01)	157
3.9.10 MME support for adding s1hoResourceReleaseWithNoMmeSgwRel timer (Feature f10568-01)	157
3.10 Time zone management	158
3.10.1 EMM information procedure (Feature m10102-01)	158
3.10.2 Additional time zone distribution functionality (Feature m10102-04)	159
3.10.3 TAI/RAI-based time zone distribution (Feature m10102-05)	160
3.10.4 Delivering network name or network short name based on IMEI and TA (Feature f10418-01)	160

3.10.5 MME support for sending network name to the UE after attach/TAU on an imsiRangeServices level (Feature f10418-02)	161
3.10.6 MME provisioning option to send or ignore MM info from MSC/VLR (Feature f10401-01)	162
3.10.7 MME support for spreading time zone updates due to DST change (Feature f10102-03)	162
3.10.8 Periodical TAU triggered EMM Information with NITZ (Feature f10402-01)	163
3.11 Cause code management	164
3.11.1 Enhanced NAS cause code functionality (Feature m10108-01)	164
3.11.2 Provisionable EMM and ESM cause code values (Feature f10403-01)	164
3.11.3 EMM and ESM cause code mapping enhancements (Feature f10119-02)	167
3.11.4 Default cause code for roamer UE's PLMNs (Feature m10109-04)	168
3.11.5 MME support for change CC for UE attempting combined attach in TAI (Feature f10413-01)	168
3.11.6 MME support for provisionable cause code for Update Bearer Response during inter-RAT redirection (f11346-02)	169
3.12 RFSP management	169
3.12.1 Connected mode mobility enhanced for reserved cells (Feature m10908-01)	169
3.12.2 Provisioning the RFSP in CMM based on IMEI/TAC (Feature f51024-02)	172
3.12.3 CMM support for RFSP override based on IMSI and TAC (Feature f51024-03)	173
3.12.4 MME support for RFSP enhancement (Feature f51024-04)	174
3.12.5 MME support for single IMSI group HSS unavailability/down declaration (Feature f11346-01)	174
3.12.6 MME support for sending RAT-Frequency-Selection-Priority-ID update to eNB received in IDR from HSS (Feature f10939-01)	177
3.13 Roaming	178
3.13.1 MME roaming support (Feature m10100-02)	178
3.13.2 Roamer UE's HSS selection based on IMSI range (Feature m11314-01)	182
3.13.3 P-GW selection for IRAT mobility of roamers (Feature m30113-01)	182
3.13.4 Roaming enhancement (scale, imsi-ta restriction, auth policy) (Feature m10109-02)	183
3.13.5 LBO roamers to select S5-only S-GW (Feature m30113-03)	184
3.13.6 MME provisioning of default QoS profile for visiting roaming subscribers (Feature m10520-02)	185
3.13.7 Roaming QoS enhancements (Feature m10520-03)	185
3.13.8 MME support for additional roaming QoS enhancements (Feature m10520-04)	188
3.13.9 Enhanced roaming restriction for IPv4v6 bearers (Feature m50051-02)	

.....	189
3.13.10 Inter-PLMN TAU and attach restrictions (Feature m10151-01)	193
3.13.11 Forbidden PLMN using regional subscription zone codes (Feature m10135-01)	195
3.13.12 Treating an IMSI series as home subscribers (Feature m10132-01)	199
3.13.13 Local breakout enhancements (Feature m10128-02)	203
3.13.14 IMS/LBO related modification to HSS/P-GW override (Feature f10101-01)	207
3.13.15 IMS APN roaming control (Feature f10113-01)	208
3.13.16 QoS value modifications for roamers (Feature f10112-01)	211
3.13.17 Inbound roamer QoS enhancements (Feature f10130-01)	213
3.13.18 Autonomous local breakout for roamers (Feature f10165-01)	213
3.13.19 Overriding of roamer QoS (Features f10112-05 and f10112-06)	214
3.13.20 Overriding of roamer QoS enhancements (Feature f10112-07)	214
3.13.21 MME support for roamers QoS enhancements (Feature f10112-04)	215
3.13.22 MME support for enhancements to QoS values modifications for roamers (Feature f10112-09)	215
3.13.23 MME support for multiple-home PLMN - phase 1 (Feature f10193-01)	216
3.13.24 CMM support for roaming - phase 2 (Feature f20028-02)	216
3.14 Network sharing	217
3.14.1 Network sharing (Feature m10902-01)	217
3.14.2 15 equivalent PLMNs (Feature m10104-01)	219
3.14.3 MME support for dedicated core network (Feature f11601-01)	220
3.14.4 MME support for dedicated core networks – mode 2 P-GW selection (Feature f11601-02)	222
3.14.5 MME support for dedicated core networks - mode 1 (Feature f11601-03)	222
3.14.6 MME support for assigning UE usage type (Decor) on IMSI range basis (Feature f11601-06)	223
3.14.7 MME support for local provisioning of UE usage type based on 5G subscription (Feature f11601-07)	223
3.14.8 MME support for dedicated core network enhancement (Feature f11601-08)	224
3.14.9 IMSI and TAI specific EPLMN lists (Feature f10910-01)	224
3.14.10 MME support for customization of HRL equivalent PLMN list (Feature f10910-02)	225
3.14.11 Enhanced triple access scenarios - delivery (Feature f14605-03)	225
3.14.11.1 Pooling	226
3.14.11.2 Target Identification IE in GTPv1 Forward Relocation Request message	230
3.15 Inter radio access technology (IRAT)	232
3.15.1 Support for Gn HSAPA handoffs - RAU (Feature m30100-01)	232

3.15.2 RIM procedure between E-UTRAN and UTRAN (Feature m30030-01)	235
3.15.3 A/Gb and Iu mode capable UEs (Feature m30100-06)	237
3.15.4 Interworking between E-UTRAN and UTRAN/GERAN over S3 interface (Feature m30200-01)	238
3.15.5 E-UTRAN to GERAN/UTRAN cell reselection and redirection (Feature m10906-01)	240
3.15.6 LAC values greater than 32 767 (Feature m30105-01)	240
3.15.7 Inter-RAT handover procedure from E-UTRAN to GERAN (Feature m30104-01)	242
3.15.8 Gn/S3 enhancements (Feature m30111-01)	243
3.15.9 IRAT mobility QoS parameter updates (Feature m30106-02)	243
3.15.10 Indirect data forwarding during pre-Rel 8 PS handover (Feature m30103-02)	244
3.15.11 Enhanced eHRPD to LTE idle mode handover (Feature m20100-03)	244
3.15.12 Cell redirection from LTE to 1xRT (Feature m20103-06)	244
3.15.13 Cell S3 Forward Relocation Response from different IP (Feature m30112-01)	245
3.15.14 WiFi handoff with mode 2 (Feature m10130-01)	246
3.15.15 MME support for forming APN FQDN on non-3GPP handover scenarios (Feature f10560-01)	246
3.15.16 Unconditionally set up radio bearers for inter-RAT TAU (Feature f10128-01)	246
3.15.17 Emergency calls WLAN handover (Feature f10509-01)	247
3.15.18 CMM support for ARD provisioned in HSS and pass it with service-based HO to radio accordingly (Feature f11343-01)	247
3.15.19 MME support for inter-system RAU enhancements (Feature f11821-01)	249
3.16 CSFB	250
3.16.1 SGs based CS fallback and SMS interworking with GSM/UMTS (Feature m30101-03)	250
3.16.2 SMS-only over SGs interface (Feature m11004-02)	252
3.16.3 Additional SMS enhancements (Feature m30101-09)	253
3.16.4 CSFB enhancements (Feature m30102-03)	255
3.16.5 S102-based CS fallback to 3G1X voice (Feature m20103-01)	256
3.16.6 Provisioning control whether ESR for MO call is accepted (Feature f10111-02)	258
3.16.7 3G1x voice on dual transceiver handset (Features m20103-04, m20103-05)	258
3.16.8 Modify Bearer Request during CSFB (Feature f10111-01)	259
3.16.9 Suppress registered LAI in Context Setup Requests to eNB (Feature f10412-01)	260
3.16.10 Maintain UE SGs-Association state to MSC after SGs link failure (Feature f11812-01)	260

4 Session management	261
4.1 Idle-active change (Feature m10001-01)	261
4.2 Piggyback functionality for default bearer activation (Feature m11006-01)	261
4.3 Scenario-based actions on move VLR (Feature m10714-03)	263
4.4 P-GW pause of charging (Feature m10219-01)	264
4.5 Selection of action on no response to Modify Bearer (Feature m10804-02)	264
4.6 Piggyback option for dedicated bearer setup (Feature m11006-03)	265
4.7 Modify Access Bearer Request (Feature m20105-01)	265
4.8 Private Extension IE enhancements (Feature m10154-01)	267
4.9 Controlling the Delay Downlink Packet Notification IE is S11 (Feature f10127-01)	268
4.10 Setting up radio bearers during TAU request with GBR bearer present regardless of Active Flag value (Feature f10702-05)	269
4.11 MME relocation for multiple bearers with the same APN and PDN type (Feature f10107-03)	269
4.12 Duplicate PDN connections during 2G/3G to 4G IRAT TAU (Feature f10137-06)	269
4.13 NAS non-delivery indication for session management procedures (Feature f10117-06)	270
4.14 MME support for differentiating LTE-M traffic (Feature f11734-01)	271
4.15 User Location Information (ULI) handling	271
4.15.1 Extended procedures where ULI message is sent over S11 (Feature m10120-01)	272
4.15.2 ULI enhancements (Feature m10120-05)	272
4.15.3 ULI enhancement for dedicated bearer activation procedure (Feature m10120-04)	274
4.15.4 MME/ULI to include ECGI and TAI in Update/Delete Bearer Response messages (Feature m10120-09)	274
4.15.5 Provisionable control of ULI for SGW IE in Create Session Request and Modify Bearer Request (Feature f10105-02)	275
4.15.6 MME support for PSCell IE to determine UE location (Feature f10935-01)	275
4.16 PDN type selection	275
4.16.1 Separate UE PDN connection per PDN type (Feature m10121-01)	275
4.16.2 IPv4/IPv6 selection enhancements (Feature m10129-01)	276
4.16.3 Provisioning for emergency PDN type (Feature f11006-01)	276
4.16.4 MME support for configurable PDN type IPv4v6 (Feature f10174-01) ...	
277	
4.17 QoS	277
4.17.1 MME custom QoS parameter mapping from EPS to Release 99 (Feature m30107-02)	277
4.17.2 Additional extended QoS fields (Feature m30109-01)	278
4.17.3 Flexible QoS mapping (Feature m30107-03)	278

4.17.4 UE AMBR update at the completion of TAU or handover (Feature m11333-01)	281
4.17.5 Extension of maximum bit rates in QoS IE (Feature f11903-01)	281
4.17.6 Operator defined QCI provisioning control (Feature f10167-02)	283
4.17.7 HSS/P-GW QoS parameter override for home subscribers (Feature f10112-03)	283
4.18 MME support for behavior change for Resource Not Available in Modify Bearer and Modify Access Bearer Response (Feature f10184-01)	284
4.19 MME support for CS Service Notification Repeat after UE re-establishment (Feature f10936-01)	284
 5 Node selection	286
5.1 DNS	296
5.1.1 Enhancements to MME DNS support to discover MME/P-GW/S-GW/SGSN (Feature m10103-06)	296
5.1.2 MME support for increased S-GW FQDNs limit in DNS response (Feature f12201-01)	297
5.1.3 SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN (Feature m10103-07)	297
5.1.4 NAPTR records with empty flag (Feature m10103-16)	301
5.1.5 Fallback to default APN-OI on DNS failures (Feature m10121-04)	301
5.1.6 Removing setting of MSB of MME Group ID provisioning restriction (Feature m10533-02)	302
5.1.7 S-GW NAPTR records with empty flag (Feature f10175-01)	303
5.1.8 Increased number of SRV queries (Feature m10103-13)	303
5.1.9 DNS enhancement (Feature f12205-01)	304
5.1.10 MME support for steering option 3x subs to combo nodes for capacity offload (Feature f10004-01)	304
5.1.11 MME support for steering option 3x subs to combo nodes for capacity offload - phase 2 (Feature f10004-02)	308
5.1.12 Steering option 3x subs to combo nodes for capacity offload enhancement (Feature f13034-01)	309
5.1.13 MME support for steering option 3x subs to combo nodes for capacity offload - phase 3 (Feature f10004-03)	311
5.1.14 DNS query to obtain MME IP addresses enhancements (Feature f12207-01)	312
5.1.15 MME support for improved table management for P-GW isolation/gwNodeAdmin (Feature f10166-03)	312
5.1.16 CMM support for configurable DNS timeout alarm (Feature f12115-02)	312
5.2 APN management	313
5.2.1 MME support for APN wildcard (Feature m10100-03)	313
5.2.2 Multiple APNs matching the wildcard APN (Feature m10100-07)	313
5.2.3 Maximum 16 APNs per UE with engineering for 6 APNs per UE (Feature	

m10010-05)	314
5.2.4 Wrong APN correction and default APN NI selection strategy (Feature m10137-01)	314
5.2.5 Enhanced APN correction (Feature m10137-02)	315
5.2.6 MME support to send the UE-requested APN or the corrected APN (Feature m10107-04)	316
5.2.7 APN correction (Feature f10107-01)	316
5.2.8 APN correction configuration enhancements for IMSI ranges (Feature f10107-07)	318
5.2.9 Enhancement to APN correction to accommodate maximum of 255 APNs (Feature f10107-08)	319
5.2.10 CMM support for SGSN national APN database table (Feature f10160-01)	319
5.2.11 APN conversion and correction (Feature f10137-04)	319
5.2.12 APN conversion and correction per IMSI series enhancements (Feature f10137-08)	320
5.2.13 APN correction and conversion per IMSI/IMEI range (Feature f10116-02, f10116-04)	320
5.2.14 APN override with GW selection mode 1 enhancements (Feature f10116-06)	321
5.2.15 APN override with GW selection mode 1 extensions (Feature f10116-09)	321
5.2.16 APN correction and conversion per IMSI/IMEI range enhancements (Feature f10116-07)	322
5.2.17 MME support for APN rate control status (Feature f11701-22)	322
5.3 Gateway selection	323
5.3.1 S-GW and P-GW selection enhancements (Feature m10110-01)	323
5.3.2 Preference for an S-GW supporting S5 and S8 (Feature m10128-01)	326
5.3.3 Enhanced S-GW and P-GW isolation (Feature m10113-04)	327
5.3.4 Provisionable depth of retry for S-GW/P-GW reselection (Feature m10113-06)	329
5.3.5 Additional S-GW and P-GW selection enhancements (Feature m10110-01)	330
5.3.6 Topological label matching for S8 P-GW selection (Feature m10136-01)	331
5.3.7 P-GW reselection on no response from S-GW (Feature m10112-06)	332
5.3.8 Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures (Feature m10113-01, m10113-02)	332
5.3.9 Partial label matching on TAC query (Feature m10113-03)	333
5.3.10 Extending Gn S-GW selection for additional scenarios (Feature m30113-04)	333
5.3.11 Selection of an S-GW with x-s8-gtp only service (Feature m30113-02)	334
5.3.12 Intelligent P-GW selection based on requested PDN type (Feature	

f10102-01)	334
5.3.13 S-GW/P-GW selection based on IMSI/MSISDN range (Feature f10110-01)	336
5.3.14 P-GW selection based on charging characteristics (Feature f10106-01)	339
5.3.15 Mode 2 enhanced S-GW selection for IRAT TAU (Feature f10125-01) ...	341
5.3.16 Alternate GW reselection (Feature f10125-02)	342
5.3.17 S-GW relocation on modify bearer request failures (Feature f10148-02)	344
5.3.18 Restricting S-GW relocation (Feature f10166-01)	345
5.3.19 Optional P-GW ID determination for statically allocated P-GW (Feature f10132-01)	345
5.3.20 Intelligent roamer P-GW selection based on requested PDN type (Feature f10102-04)	346
5.3.21 Sending P-GW IP in NOR (Feature f10169-01)	346
5.3.22 MME support to obtain P-GW FQDN for SGSN to MME relocation (Feature f10125-03)	347
5.3.23 MME support for enhanced alternate S-GW/P-GW reselection and isolation (Feature f10125-04)	347
5.3.24 Restricting S-GW relocation enhancements (Feature f10166-02)	349
5.3.25 MSISDN number based home GGSN/P-GW selection enhancement (Feature f10176-01)	349
5.3.26 MME support for enhanced NR S-GW/P-GW selection after 3G to 4G IRAT idle mode TAU (Feature f10185-01)	349
5.3.27 MME support for using topological label matching for GW selection (Feature f10125-05)	351
5.3.28 MME support for GW selection considering more than two IP addresses per FQDN (Feature f10191-01)	351
5.3.29 MME support for enhanced S-GW selection for roammers for GW selection mode 1 (Feature f10190-01)	352
5.3.30 MME support for roamer co-located GW selection (Feature f10110-08)	352
5.3.31 MME support for locally configured S-GW/P-GW selection based on IMSI/MSISDN range for inbound roammers (Feature f12208-02)	352
5.3.32 MME support for statically configured S-GW/P-GW selection with Topon option for roammers based on IMSI/MSISDN range plus APN (Feature f12208-01)	353
5.3.33 MME support for handling nc-smf tagged service type for non-N1-mode UEs (Feature f20003-15)	355
5.3.34 MME support for sending P-GW FQDN in EPS to 5GS mobility (Feature f10125-09)	355
5.3.35 CMM support for configuration control for restriction of P-GW selection to colocated GGSN/P-GW during IRAT mobility (Feature f10172-01)	356
5.4 Node selection for emergency services	356

5.4.1 Enhanced P-GW selection for emergency PDN (Feature m10123-01)	357
5.4.2 Mode 1 P-GW node selection using E911 APN NI (Feature m10123-02)	358
5.4.3 Selecting P-GW for emergency sessions based on requested PDN type (Feature f11010-01)	359
5.5 SGSN selection	359
5.5.1 DNS SGSN discovery query method based on provisioning SGSN (Feature m10103-08)	359
5.5.2 DNS fallback for SGSN call scenarios (Feature m10125-01)	360
5.5.3 Fallback to GTPv1 support (Feature m10119-02)	361
5.5.4 DNS fallback enhancements from Rel 8 DNS query to pre-Rel 8 DNS query (Feature m10133-01)	361
5.5.5 MME support for 4-digit legacy MNC-MCC DNS query to find Gn-SGSN (Feature f12202-01)	362
5.6 MSC selection	372
5.6.1 MSC selection for SRVCC based on DNS procedures (Feature f11803-01)	372
5.6.2 Provisioning of MSC selection for multiple 3G networks (Feature f11809-01)	373
5.6.3 CMM support for use HPLMN for SGs interface towards MSC (Feature f11815-01)	373
5.6.4 CMM support for 3GPP IMSI hash for assigning a UE to an MSC over SGs (Feature f11823-01)	374
5.6.5 MME support for enhanced MSC/VLR selection (Feature f11807-01)	374
6 Voice over LTE (VoLTE)	375
6.1 IMS voice over PS (VoLTE) critical CRs (Feature m10099-11)	375
6.2 Capability of several ways to configure IMS APN (Feature f14616-01)	375
6.3 Rejection of IMS PDN connection when only wildcard is provided in subscription data (Feature f10100-01)	376
6.4 Back-off timer inclusion when IMS APN not subscribed (Feature f10170-02)	376
6.5 SRVCC	377
6.5.1 MME support for UE radio capability match request (Feature m10099-06)	377
6.5.2 S102-based 3G1X circuit voice hand down (Feature m20102-01)	379
6.5.3 Sv-based UMTS hand down (Feature m30102-01)	380
6.5.4 1xRT SRVCC emergency call handling (Feature m11019-01)	382
6.5.5 Sv MSC Server selection enhancement for SRVCC HO (Feature m30102-07)	382
6.5.6 VoLTE support determination enhancements (Feature f10503-01)	383
6.5.7 SRVCC possible indication for emergency calls (Feature f11008-01)	383
6.5.8 Customized setting of voice parameters towards HSS (Feature f11319-01)	384
6.5.9 Multi-SIM with VoLTE and SRVCC (Feature f10129-02)	387

6.6 VoLTE access control	388
6.6.1 Selective VoLTE enablement (Feature f10407-01)	388
6.6.2 Selective VoLTE enablement enhancements (Feature f10407-02)	393
6.6.3 Extending range of entryId in vdpRangeServices provisioning command (Feature f10407-03)	394
6.6.4 MME support for VDP profile-based forbidden TAI inclusion separately per UE ranges (Feature f10407-04)	394
6.6.5 CSFB and VoLTE enhanced restrictions (Feature f10510-01)	395
6.6.6 CSFB sunsetting enhancement (f10510-02)	398
6.7 IMS VoPS support	399
6.7.1 Homogeneous support of IMS VoPS indication to HSS (Feature m11315-01)	399
6.7.2 Homogeneous support of IMS VoPS indication to HSS for shared network (Feature m11315-02)	400
6.7.3 Enhanced homogeneous support of IMS VoPS indication to HSS (Feature m11315-03)	400
6.8 S1AP cause codes	404
6.8.1 MME provisioning for S1AP cause code to Normal release for double S1 and path switch (Feature f10907-01)	404
6.8.2 MME support for flexibility in configuring the S1AP cause codes (Feature f10902-02)	404
6.9 VoLTE QoS	405
6.9.1 Operator defined QCI (Feature m10202-02)	405
6.9.2 3GPP specified new QCI values for mission critical and non-critical push to talk voice (Feature f10220-01)	406
6.9.3 Enhanced operator defined QCI (Feature f10167-01)	407
6.10 IMS emergency services	408
6.10.1 IMS emergency services (Feature m10106-01)	408
6.10.2 IMS emergency services enhancements (Feature m10106-02)	411
6.10.3 Emergency dedicated bearer setup without piggybacking (Feature m11006-02)	411
6.10.4 Configuration of E911 per TAI (Feature m10122-01)	412
6.10.5 Allow transfer of emergency bearers to SGSN (Feature m10106-03)	412
6.10.6 E911 enhancements (Feature m10112-03)	412
6.10.7 Non-standard treatment of serving node AVP in LRR (Feature f11308-01)	414
6.10.8 SIMless UEs to emergency attach independent of TAI (Feature m10141-01)	414
6.10.9 Removing need for static IP and FQDN in emergency profile (Feature m10112-07)	415
6.10.10 IMS emergency services configuration enhancements (Feature m11003-01)	415
6.10.11 IMS emergency services configuration at the IMSI-NS level (Feature m10112-09)	415

6.10.12 Enhancements for VoLTE emergency call deployment (Feature f11009-01)	417
6.10.13 Emergency service enhancements (Feature f11017-01)	417
6.10.14 MME support for emergency call enhancements on LTE (Feature f11020-01)	418
6.11 Location services	418
6.11.1 Homogeneous LCS enhancements: continuation of LCS session after S1 connection release (Feature m11000-02)	419
6.11.2 Location report for UEs not supporting LTE positioning protocol (LPP) (Feature m11000-03)	419
6.11.3 (Emergency) location based services (Feature m11000-01)	419
6.11.3.1 Mobile terminating location request (MT-LR) procedure	426
6.11.3.2 Network-induced location request (NI-LR) for emergency calls ...	427
6.11.4 Customer specified emergency LCS handling (Feature f11007-01)	428
6.11.5 Configurable control emergency MT-LR eCGI timestamp (Feature f11007-02)	430
6.11.6 MME support for configurable control with or without E-SMLC for any client type MT-LR (Feature f11016-01)	430
6.11.7 MME support for 4 ESMLCs per TA for emergency sessions (Feature f11011-01)	431
6.11.8 MME support for NI-LR during MT-LR collision handling (Feature f11022-01)	431
7 Home eNodeB (HeNB)	432
7.1 MME support for Home eNB (Feature m14000-01)	432
7.2 20 bit Home eNB identifier (Feature m14003-01)	439
7.3 X2 HO between macro eNB/HeNB connected to a HeNB gateway (Feature m14002-01)	440
7.4 Local IP access (LIPA) (Feature m14000-01)	441
7.5 LIPA enhancements (Feature f10927-02)	443
7.6 256 TAs per eNB (Feature f10901-01)	443
7.7 Raising an alarm when a TA is shared by two HeNB GWs (Feature f10903-01)	444
7.8 Non-standard HeNB GW selection (Feature f10905-01)	445
7.9 CMM support for release of active LIPA PDN connections (Feature f10927-01)	446
7.10 MME support for restrict LIPA service for DCNR capable UE(s) (Feature f10927-03)	447
7.11 MME support for CSG ID enhancements (Feature f10906-03)	447
8 Multimedia broadcast multicast services	448
8.1 Multimedia broadcast/multicast service (MBMS or eMBMS) (Feature m11007-01)	448
8.2 MBMS restoration (Feature m11007-04)	459

9 MME/SGSN support for lawful interception	469
9.1 Lawful interception (LIPv2 based)	472
9.2 LCS client type lawful interception (Feature f10308-01)	473
10 Public safety services	474
10.1 Enhanced multimedia priority services (MPS) (Feature m11009-01)	474
10.2 Advance priority for eMPS (Feature f11303-01)	477
10.3 MME support for eMPS priority on RRC establishment cause only (Feature f12126-01)	478
10.4 Overlapping position requests for a single UE (Feature m10112-10)	478
10.5 Heightened accuracy location support for SLs/SLg interface (Feature f11001-01)	480
11 CMAS/ETWS	482
11.1 Warning message delivery (Feature m11005-01)	482
11.2 Restoration of warning message delivery upon eNB restart (Feature m11005-09)	485
11.3 Provisioning restriction for warning area list sent to eNB (Feature f11101-01)	486
11.4 TAI alarm if TAI is not recognized in CMAS messages from SBc (Feature f11102-01)	488
11.5 MME support for new Warning Area Coordinates IE (Feature f11105-01)	488
11.6 CMAS enhancements for Write Replace Warning message (Feature f11106-01)	489
12 Commercial location services	490
12.1 Coarse positioning (Feature m10112-02)	490
12.2 Expanded LPP container maximum size (Feature m11018-01)	490
12.3 HSS-initiated location request	491
12.4 Location services enhancements - phase 1 (Feature m11016-03)	493
12.5 Location services enhancements - phase 2 (Feature m11016-01)	494
12.6 Including age of location in Provide Subscriber Location Response for failure cases (Feature f10405-01)	495
12.7 MSISDN in SLg Provide Subscriber Location Request Message (Feature f11004-01)	496
13 M2M, Internet of things support (IoT)	497
13.1 Periodic TAU timer override at attach (Feature m10214-01)	498
13.2 UE power saving mode (PSM) (Feature m10923-01)	499
13.3 Coverage enhancement paging (Feature m11604-01)	501
13.4 Back-off timer for overload control (Feature m10709-02)	501
13.5 MME support for MBMS	502
13.6 Multi operator core network (MOCN) (Feature m10902-01)	503
13.7 IMSI - ISDN range MME assisted move - UE load balancing (Feature m10713-01)	503

13.8 Extended Idle Mode DRX (eDRX) (Feature f11603-01)	504
13.9 MME support for HLCOM (Feature f11603-02)	512
13.10 Aging out UE contexts from CPPS cache (Feature f14103-01)	512
13.11 Configurable cause code sending in SGs for eDRX/PSM (Feature f11725-01)	513
13.12 Handling MT SMS for UE in power savings (Feature f11721-02)	513
13.13 Minimum T3412 timer for UE power saving mode (PSM) (Feature f10409-01)	516
13.14 MME support for 320 hours unit in the T3412 extended timer (Feature f10409-02)	517
13.15 Active timer in the UE subscription (Feature f11732-01)	518
13.16 Configuration of eDRX and PSM parameters per APN and IMSI series (Features f11721-01 and f11603-05)	518
13.16.1 Functionality of eDRX and PSM provisioned per APN and IMSI series	519
13.16.2 MME support for 10K APNs in a list (Feature f11708-07)	522
13.17 MME support for subscription-based aerial UE identification (Feature f11337-01)	523
13.18 MME support for IoT purge timer provisioning range to 30 days (Feature f12005-01)	523
14 CloT optimization	525
14.1 LAP (low access priority) devices (Feature m10115-01)	526
14.2 MME support for NB-IoT and EMM-REGISTERED UE without PDN connection (Feature f11701-01)	529
14.3 Extended Protocol Configuration Option (ePCO) (Feature f11711-01)	531
14.4 Preferred network behavior provisioning (Feature f11307-01)	532
14.5 Group service provisioning (Feature f11701-07)	532
14.6 MME support of NB-IoT/CIoT trials with R12 HSS (Feature f11713-01)	533
14.7 CMM support for tunneling of S1AP messages associated with CloT Attach/TAU Requests (Feature f11728-01)	534
14.8 MME support for enhancement of CloT interoperability (Feature f11726-01)	535
14.9 CloT traffic control (Feature f11701-06)	536
14.10 User plane CloT EPS optimizations - bearer activation without SR (Feature f11701-04)	537
14.10.1 Procedure descriptions	538
14.11 Switching data transport between control plane and user plane (Feature f11708-01)	542
14.12 Current location event report enhancement (Feature f11015-01)	543
14.13 MME support for sending immediate S6a:IDA for MONTE current location request (Feature f11733-08)	544
14.14 Inter-UE QoS for NB-IoT UEs using control plane CloT EPS optimization (Feature f11720-01)	544

14.15 eDRX cycle 5.12 seconds for EUTRAN (Feature f11603-06)	545
14.16 Service gap control (Feature f11730-01)	546
14.17 NIDD and IP via S11/SGi	548
14.17.1 Extended NAS timer values (Feature f11707-01, f11707-02)	548
14.17.2 Control plane CloT EPS optimizations for both non-IP data and IP through SGi (Feature f11701-03)	550
14.17.3 Robust Header Compression (ROHC) (Feature f11701-09, f11701-10)	551
14.17.4 MME support for S11-U downlink user data buffering (Feature f11701-11)	552
14.17.5 MME support for non-IP with S1-U transferred (Feature f11723-01)	552
14.17.6 IPv6 address selection when presented with IPv4/IPv6 in transport layer address (Feature f11723-02)	554
14.18 NIDD via SCEF	554
14.18.1 Control plane CloT optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF) (Feature f11701-02)	554
14.18.2 MME support for CloT monitoring procedures (Feature f11702-01) ...	559
14.18.3 CMM support for Rel 16 MONTE and CloT CRs (Feature f11733-11) ...	561
14.18.4 PDN connectivity status event reporting (MONTE) (Feature f11733-04)	562
14.18.5 MME support for MONTE communications failure event (Feature f11733-05)	565
14.18.6 MME support for MONTE number of UEs per location (Feature f11733-07)	566
14.18.7 UE monitoring enhancements (Feature f11733-01)	567
14.18.8 MME support for generating idle status report if configured when UE is idle (Feature f11733-10)	567
14.18.9 Using the S6a/S13/SLg SCTP association for T6a (Feature f11701-15)	569
14.18.10 Simultaneous support of SCEF with S11-U (Feature f11701-12)	570
14.18.11 Simultaneous support of SCEF with S11U - part 2 (Feature f11701-16)	571
14.18.12 MME support for changing the range of controlPlaneUserInactivity timer (Feature f14612-01)	571
14.18.13 Validating the AVPs times are not out of date (Feature f11736-01)	572
14.18.14 MME support for early data transmission for control plane and user plane CloT EPS optimization (Feature f11701-18)	572
14.18.15 MME support for accepting connection release from SCEF for temporarily unreachable UE (Feature f11701-20)	575
14.19 Sending AADDNF notification during eDRX and send LoC when entering PSM (Feature f11702-04)	576
14.20 MME support for generating loss of connectivity (LoC) event reports during eDRX	576

cycle (Feature f11735-02)	577
14.21 MME support for eNB CP relocation indication for NB-IoT UE (Feature f11727-01)	578
14.22 MME support for CloT for inbound roamer phase - 1 (f11738-02)	578
14.23 MME support for CloT feature control via IMSI ranges (Feature f11737-01)	579
14.24 MME support for CloT for inbound roamers (Feature f11738-01)	581
14.25 MME support for wake-up signal for CloT (Feature f11701-21)	585
15 SMS in MME (Feature f11004-03)	587
15.1 SMS in MME procedures	588
15.2 SMS registration parameters	600
16 Presence reporting area (PRA)	605
16.1 Presence reporting area (Feature f11003-01)	605
16.2 PRA reporting for transitions from eNB to gNB (Feature f10904-07)	607
16.2.1 PRA reporting procedures	608
16.3 PRA reporting optimizations for transitions from eNB to gNB (Feature f10904-10)	613
16.4 MME support for PRA 3GPP release 14 and 15 standard additions - part 1, part 2 (Features f10904-11 and f10904-16)	614
16.5 Dormant PRA state (Feature f10904-12)	617
16.6 PRA message pacing (Feature f10904-14)	619
16.7 PRA area ranges (Feature f10904-15)	620
16.8 MME support for scaling PRA limits (Feature f10904-17)	620
16.9 PRA optimizations and additional timers (Features f10904-20 and f10904-30)	621
16.10 PRA dual connectivity reporting for IPv4 gNBs (Feature f10904-22)	622
16.11 MME support for optimizing standard PRA reporting (Feature f10904-28) ...	622
16.12 MME support for new PRA action on 5GS to EPS mobility for DC PRA (Feature f10904-35)	623
16.13 MME support for receiving new PRA action during additional procedures (Feature f10904-34)	623
17 5G support	626
17.1 MME support for dual connectivity (Feature f10904-01)	626
17.2 MME support for NSA option 3A/3X EDCE5 enhancements (Feature f10904-08)	627
17.3 Secondary RAT usage reporting for 5G NSA option 3X (Feature f10904-03) ... 629	
17.3.1 Secondary RAT usage reporting procedures	632
17.4 MME support for 3GPP 5G dual connectivity EDCE5 enhancements (Feature f10904-02)	637
17.5 Treating UE as supporting DC-NR based solely on HSS ARD “NR as Secondary RAT in E-UTRAN Not Allowed” bit (Feature f10904-24)	638

17.6 Indication of DC-NR support in Attach/TAU Accept message even when UE is not allowed 5G3x service (Feature f10904-31)	638
17.7 MME support for N26 LTE Interworking - 5G (Features f13501-03 and f13501-05)	638
17.7.1 N26 interworking procedures	640
17.7.1.1 EPS to 5GS idle mode mobility procedure	640
17.7.1.2 5GS to EPS idle mode mobility procedure	641
17.7.1.3 EPS to 5GS handover procedure	643
17.7.1.4 5GS to EPS handover procedure	646
17.7.2 Support of UE usage type for selecting the target AMF	647
17.7.3 Return Preferred indication	648
17.7.4 N26 interworking with DCN and DCNR features	648
17.7.5 Inter-system cause value mapping	649
17.7.6 Emergency bearer over the N26 interface	653
17.7.7 Security context establishment	653
17.7.8 MME support for release 16 direct data forwarding (Feature f13501-07)	654
17.8 CMM support for Ethernet PDU for mobility across N26 interface (Feature f20102-01)	655
18 Availability/reliability	656
18.1 Overload control	656
18.1.1 Overload notification to eNBs (Feature m10702-01)	659
18.1.2 MME enhancements to overload control (Feature m10711-01)	660
18.1.3 Sending RAB to S-GW as part of safety net upon DDN for connected UE (Feature m10138-01)	660
18.1.4 Enhanced overload control to rebalance CPPS load (Feature m10709-01)	661
18.1.5 Provisionable NAS cause code for throttling (Feature m10108-04)	662
18.1.6 Offloading overloaded CPPSs and support for T3346 timer (Feature m10709-02)	662
18.1.7 Offloading 3GPP Rel 12 diameter overload control - phase 1 (Feature m11316-03)	664
18.1.8 GTP load and overload control (Feature m10727-01)	665
18.1.9 SCTP chunk throttling (Feature f12108-01)	669
18.1.10 Age out of S10 links based on actual usage (Feature f12118-02)	671
18.1.11 Paging overload control enhancements (Feature f10225-01)	671
18.1.12 MME support for APN level overload control (Feature f10701-01)	673
18.2 Session restoration	673
18.2.1 Evolved ARP and PDP context for dual stack (Feature m30108-01)	673
18.2.2 UE notification on specific PDN disconnection while the UE is in the idle state (Feature m10139-01)	674
18.2.3 Enhanced S-GW restoration procedure (Feature m10538-08)	675
18.2.4 P-GW restart - S11 (Feature m10538-02)	679

18.2.5 P-CSCF recovery	681
18.2.5.1 P-CSCF recovery – Option 1 (Feature m11331-01)	683
18.2.5.2 P-CSCF recovery – Option 2 (Feature m11002-01)	683
18.2.5.3 P-CSCF recovery – Option 3 (Feature m11331-03)	685
18.2.6 PDN connection re-establishment after S-GW change (Feature f10103-01)	685
18.2.7 PDN connection re-establishment after S-GW change with roammers and voice (Feature f10103-02)	686
18.2.8 PDN connection re-establishment after S-GW change with roammers and voice enhancements (Feature f10103-03)	687
18.2.9 Session restoration FNS compatibility (f10713-01)	687
18.3 Session restoration server	688
18.3.1 Session restoration server (SRS) (Feature m10538-01)	688
18.3.2 MME support for SRS geo-redundancy (Feature m10538-10)	689
18.3.3 Throttling ULR during UE restoration (Feature m10538-18)	691
18.3.4 Service restoration enhancements (Feature m10538-22)	692
18.3.5 CMM support for resynch of SRS data (Feature f17008-14)	694
18.3.6 MME support for enhanced backup of 4G UE context to the SRS for ISSU (Feature f17008-07)	695
18.4 Pool level redundancy (Feature f14109-06)	696
18.4.1 Support for spread NR-10 links on multiple IPDS (Feature f72001-19)	696
18.4.2 MME support for pool redundancy record delete enhancements (Feature f14109-08)	697
18.4.3 CMM support for inter-release pool redundancy versions (Feature f14109-09)	697
18.4.4 CMM support for NR10 optimization enhancements - phase 1 (Feature f14109-13)	699
18.4.5 CMM support for NR10 optimization enhancements (Feature f14109-14)	700
18.5 Collision control	701
18.5.1 MME support for managed objects and enhanced collision handling (Feature m10508-01)	702
18.5.2 Queuing network-initiated session request during mobility management procedures (Feature m10117-01)	709
18.5.3 Extend queuing for all CSFB scenarios (Feature m10117-02)	709
18.5.4 E911 collision scenarios (Feature m10112-04)	710
18.5.5 Enhanced queuing network-initiated session requests for X2/S1 HO (Feature m10117-04)	710
18.5.6 MME collision handling of HO/TAU and ESM procedures (Feature m10117-05)	712
18.5.7 PDN KPI improvement (Feature m10152-01)	715
18.5.8 Collision of incoming delete bearer request procedure and ongoing update bearer request procedure (Feature f10159-01)	715

18.5.9 MME support for SRVCC HO and X2 HO collision (Feature f10502-01)	716
18.5.10 Improved handling of QoS modification collisions (Feature f13304-01)	717
18.5.11 Send Delete Bearer Response with cause 110 during SRVCC collision (Feature f10502-03)	718
18.5.12 CMM support for Origination Time Stamp IE and Maximum Wait Time IE to help P-GW to detect collisions (Feature f11504-01)	718
18.6 Signaling optimization	718
18.6.1 Basic DPR/DPA (Feature m11301-02)	719
18.6.2 MME support for basic DRA (Feature m11307-01)	719
18.6.3 Basic DRA for SLg interface (Feature m11309-01)	720
18.6.4 Enhanced DRA support (Feature m11303-01)	721
18.6.5 Automatic neighbor relations (ANR) (Feature m10904-01)	721
18.6.6 S6a retry for NOR S6a messages (Feature m11323-01)	723
18.6.7 S6a retry for PUR S6a messages (Feature m11323-02)	723
18.6.8 Error handling enhancements for PDN connectivity rejections (Feature m10140-01)	724
18.6.9 Barring access above UE procedure frequency count (Feature f10726-01)	725
18.6.10 S6a fault handling enhancement (Feature m11318-01)	727
18.6.10.1 S6a fault handling scenarios and parameters	729
18.6.11 HSS signaling load reduction (Feature m11308-01)	729
18.6.12 MME support for KPI improvement (Feature m10911-02)	730
18.6.13 NAS CC to S-GW reject code mapping (Feature m10108-02)	731
18.6.14 Exclude destination host (Feature f11335-01)	731
18.6.15 Controlling sending of S1AP Connection Establishment Indication message (Feature f10410-01)	731
18.6.16 Diameter routing message priority (Feature f11322-01)	732
18.6.17 Further enhancements on HSS unavailability (Feature f11318-01)	732
18.6.18 MME support for HSS unavailability recovery (Feature f11318-02)	734
18.6.19 CMM support for treat MIP6-Agent-Info in IDR as one entity (Feature f11336-01)	735
18.7 Load balancing	735
18.7.1 MME S1 flex - basic pooling (Feature m10800-01)	735
18.7.2 MME offloading (S1 flex – SON) (Feature m10800-01)	737
18.7.3 Directed inter-MME subscriber move (Feature m10713-01)	739
18.7.4 S-GW draining (Feature m10131-01)	741
18.7.5 Extending provisioned timer range for UELB (Feature m10702-04)	742
18.7.6 S-GW geo-redundancy via ICR (Feature m10804-01)	744
18.7.7 MME support for DDN Ack for abnormal S-GW geo-redundancy switchover (Feature f10188-01)	745
18.7.8 IMSI range-based routing to the HSS (Feature m11008-01)	745
18.7.9 Diameter connections with load balancing (Feature m11320-01,	

f11304-01)	746
18.7.10 HSS retry	748
18.7.11 Multiple IWSs for same MSC ID (Feature m20103-02)	750
18.7.12 CLI-triggered MSS SGs offloading (Feature f11802-01)	751
18.7.12.1 MSS SGs offloading collision handling	753
18.7.13 MME support for passive offloading (Feature f10710-01)	755
18.7.14 Directed UE moved by TA (Feature f10711-01)	756
18.7.15 Relative capacity calculation enhancements (Feature f71001-12)	757
18.7.16 UE load balancing compatibility (Feature f10712-01)	758
18.7.17 UELB enhancements for soft offload of UE (Feature f10710-02)	759
18.8 System/process reliability	760
18.8.1 CMM support for using REMc (Feature f70012-03)	760
18.8.2 Full/partial IP isolation detection (Feature f70012-05)	761
19 Interface/Link management	762
19.1 IP address management	762
19.1.1 Same IP address for S6a and SLg (Feature m11310-01)	762
19.1.2 Multiple S1-MME local IP addresses (Feature m10910-01)	762
19.1.3 Multiple eNBs with the same IP address (Feature m10919-01)	764
19.1.4 Sv and SGs interface using the same remote endpoint IP and different port number (Feature m30102-06)	764
19.1.5 S1-MME and M3 sharing the same IP with different ports (Feature m10432-01)	764
19.1.6 IP address flipping for SGs and S6a interfaces (Feature m10432-02)	765
19.1.7 MME support for detection of S11 load balancer by IP address (Feature f10195-01)	765
19.2 IP version support	765
19.2.1 Bidirectional Forward Detection for dual stack (IPv4 and IPv6) (Feature m80140-06)	765
19.2.2 IPv4/IPv6 dual stack (Feature m10403-01)	766
19.2.3 IPv4, IPv6 implementation for ping/traceroute source based routing enhancement (Feature m10425-02)	767
19.2.4 MME support for IPv4/IPv6 dual stack transport for Gn (Feature f12101-09)	767
19.2.5 CMM support for Gn dual stack (Feature f11810-01)	767
19.2.6 CMM support for IPv6 internal communication (Feature f12119-01)	769
19.3 SCTP	769
19.3.1 SCTP multi-homing (Feature m10402-07)	769
19.3.2 SCTP multi-homing: S1-MME, S6a, SGs, SBc interface enhancements (Feature m10402-06)	770
19.3.3 Provisioning of separate SCTP interfaces for SGs interface (Feature m10404-01)	772
19.3.4 Multiple S6a streams (Feature m80300-02)	772
19.3.5 SCTP path availability alarm for multi-homed connections (Feature	

m10402-12)	774
19.3.6 MME support for same SCTP association to DRA and higher peer count (Feature f11304-01)	775
19.3.6.1 DRA requiring different realms per application ID	776
19.3.6.2 Emergency service DRA selection for SLg	777
19.3.7 Enhancement of SCTP state when locking SGs links (Feature f11806-01)	777
19.3.8 UE Retention Information IE in S1 Setup Request/Response message to handle SCTP association restart (Feature f10909-01)	778
19.3.9 Reassembly of fragmented IP datagrams (Feature f12113-01)	778
19.3.10 MME support for MTU discovery for S1/M3 links over IPv6 (Feature f12107-02)	779
19.3.11 MME support for 32 SCTP associations per MSC for SGs and 32 endpoints for Sv (Feature f12123-01)	780
19.3.12 MME support for SGd on combined SCTP association (Feature f11004-05)	780
19.3.13 MME support for override diamConnection profile default value parameters per UE PLMN service (Feature f11347-01)	780
19.4 GTP	781
19.4.1 Extended GTP Echo Timer (Feature m11501-02)	782
19.4.2 Configuration options for GTP echo (Feature m11501-01)	782
19.4.3 N3 and T3 timers per GTP message type (Feature m11502-01)	783
19.4.4 Improved S11 path management (Feature m10144-01)	785
19.4.5 Configurable CRSI flag for GTPv2 messages (Feature f11502-01)	785
19.4.6 MME support for provisioning control for GTPv2 cause code 110 (Feature f11505-01)	786
19.4.7 Create session request enhancements (Feature f10186-01)	786
19.4.8 GTP sequence number management enhancements (Feature f11506-01)	787
19.4.9 MME support for GTP restart counters dump (Feature f11507-01)	787
19.5 Link management	787
19.5.1 Restricting S10 to neighboring MME (Feature m10533-01)	787
19.5.2 Eliminating alarms for links that were never active (Feature m30111-02)	788
19.5.3 Multiple DSCP values on all network interfaces (Feature m11014-01)	789
19.5.4 Link and interface specific alarms with severity control (Feature f14208-01)	789
19.5.5 S1 CLI enhancements (Feature f14603-05)	789
19.5.6 Enhancements to eNB configuration update and S1 setup procedures (Feature f10933-01)	790
19.5.7 Extending TAI/eNB query to include TAC range and state of S1-MME links (Feature f14611-01)	790
19.5.8 MME support for increasing the S11 links (Feature f12118-03)	791

19.5.9 MME support for increasing the number of S10 and N26 links from current limit to combined 512 (Feature f12118-01)	791
19.5.10 Dynamic link exhaustion alarm at reaching static thresholds (Feature f13306-01)	792
20 Layer 3 network steering (L3NS)	793
20.1 Achieved capacity at various spread configurations	793
20.2 Multiple IPDS (Feature f80005-01)	794
20.3 L3NS/VSR for multiple IPDS (Feature f12112-03)	794
20.4 MME support for 1.6M messages per second on OpenStack (Feature f80012-01)	795
20.5 SGSN support for TA configuration with MME scaled to 1.2M on OpenStack (Feature f80005-09)	796
20.6 CMM support for fourth IPDS pair in a TA configuration (Feature f80005-18)	796
20.7 Support for L3NS Release 20.5 (Feature f12112-11)	796
20.8 CMM support for 100K asymmetric MH SCTP eNodeB in deployments with L3NS (Feature f12112-08)	796
20.9 L3NS-based multiple IPDS deployment with dedicated spread S11 IPDS (Feature f12112-10)	797
21 Operability	798
21.1 Real time monitoring	798
21.1.1 Per call measurement data (PCMD)	798
21.2 MME/SGSN PM data transfer towards ONAP-DCAE and MME/AMF PCMD data transfer towards CA4MN (Feature f14615-05)	800
21.3 Backup scheduling (Feature f14509-01)	801
21.4 Remote copy of backup files (Feature f12003-01)	801
21.5 Cloud backup and restore improvements via NSP (Feature f14008-01)	802
21.6 CMM support for secure backup and restore of CMM instance (Feature f14008-02)	802
21.7 CMM support for performance measurements (Feature f60110-11)	802
21.8 PM evolution for static counters (Feature f13012-02)	803
21.9 PM evolution for component counters (Feature f13012-03)	805
21.10 MME support for additional component counters - part 1 (Feature f13033-01)	808
21.11 MME support for additional component counters - part 2 (Feature f13033-02)	808
21.12 MME support for additional component counters - part 3 (Feature f13033-03)	808
21.13 MME support for additional static and component counters (Feature f13029-02)	809
21.14 CMM support for additional PM counter for CMM system up time (Feature f13036-01)	809

21.15 CMM support for enabling Prometheus direct scraping of metrics (Feature f14705-01)	809
21.16 CMM support for “measInfold” field in performance management reports (Feature f13032-01)	810
21.17 CMM support for call trace (Feature f60110-12)	810
21.18 CMM support for source and destination IP and port preservation in call trace - Phase 1 (f13402-01)	813
21.19 MME support for UE counts per eNB (Feature f14117-01)	813
21.20 Management activation for area-based minimization of drive test (Feature f10918-01)	814
21.21 Service mirroring (Feature f13401-01)	814
21.22 Service mirroring enhancements (Feature f13401-02)	815
21.23 OAM enhancements (Feature f13204-01)	815
21.24 Syslog collection and streaming to remote server (Feature f13207-02)	816
21.25 Event logging of PDN connectivity failures (Feature f10170-01)	816
21.26 CMM support for sending log and alarm information to stdout in addition to current destinations (Feature f14402-01)	816
21.27 CMM support for streaming PM XML file to Fluentd (Feature f14402-03)	817
21.28 CMM support for inactive session timeout configurable in CMM CLI (Feature f13213-02)	821
21.29 CMM support for authentication of NTP server (Feature f13213-05)	822
21.30 CMM support for OAM alignment (Feature f14516-01)	822
21.31 Trap notification enhancements (Feature f14618-01)	823
21.32 CMM support for network trace/trace all for MME/SGSN CNF (Feature f23401-02)	823
21.33 CMM support for show command to display 20 representative IMSIs for an input PLMN (Feature f13406-01)	824
21.34 CMM support for CMPv2 protocol (Feature f13216-01)	824
22 MME/SGSN support for lawful interception	826
23 Multi-IPDS deployments on CNFs	829
23.1 CMM support for MME and AMF using flow distribution - delivery (Feature f72002-43)	829
23.2 CMM support for flow distributor with multi-home and dynamic flow control (Feature f72002-48)	831
24 Software architecture	832
24.1 MME support for simplex DBS (Feature f14111-06)	832
24.2 CMM support for flexible size CPPS/DBS for MME/TA/AMF on OpenStack - Delivery (Feature f80005-10)	833
24.2.1 MME support for flexible size CPPS (Feature f80005-03)	834
24.2.2 CMM support for flexible size DBS (Feature f80005-15)	834
24.3 Support for quad access (Feature f20060-05)	835
24.4 CMM support for Quad Access on VMware (Feature f70006-13)	837

24.5 Support for CPPS VM auto-balancing AMMS and EMMS for quad access (Feature f20060-07)	838
24.6 CMM support for providing container and multi-service VM infrastructure (Feature f72011-03)	839
24.7 AMF support for event exposure pod (Feature f72006-06)	840
24.8 CMM support for call trace/alarm pod (Feature f72006-04)	841
24.9 MME support for 24K UE radio capability information using RCIS for VNF (Feature f10937-01)	842

List of Figures

Figure 1	EPS authentication procedure	74
Figure 2	Signaling traffic protection command	75
Figure 3	Security - ciphering and integrity protection - SNOW 3G	76
Figure 4	Security - ciphering and integrity protection - ZUC	77
Figure 5	IMEI checking	89
Figure 6	ME identity check	90
Figure 7	IMEI	93
Figure 8	NTSR paging procedure	107
Figure 9	TA list from the UE's point of view	108
Figure 10	Tracking area update	131
Figure 11	EPS network feature support IEI	138
Figure 12	UE reachability notification request procedure	144
Figure 13	UE activity notification procedure	145
Figure 14	Subscriber moves between eNBs	152
Figure 15	Subscriber moves between eNBs through S1	153
Figure 16	NITZ delivery to UE	158
Figure 17	EMM information procedure	162
Figure 18	Roaming architecture for 3GPP accesses - home routed traffic	178
Figure 19	Roaming architecture for local breakout, with home operator's application functions only	179
Figure 20	Inter-RAT handover preparation phase (TS 23.401)	191
Figure 21	Inter-RAT handover execution phase (TS 23.401)	192
Figure 22	IRAT reject (TS 23.401)	193
Figure 23	GWCN configuration	218
Figure 24	MOCN configuration	219
Figure 25	GWCN configuration variant	219
Figure 26	NAS message redirection	221
Figure 27	Mapping of 2G/3G identifiers to LTE GUMMEI	227
Figure 28	MME selection in idle mode IRAT change to LTE	228
Figure 29	MME functionality via example of 7-bit-NRI	229
Figure 30	Gn interface protocol stack (MME – SGSN)	233
Figure 31	Gn interface protocol stack (SGSN – P-GW)	233
Figure 32	3GPP Access for pre-Release 8 SGSN	234
Figure 33	Interworking with pre-Release 8 WDCMA core	234
Figure 34	RIM	236
Figure 35	Support for A/Gb and Iu mode capable UEs	238
Figure 36	Interworking between E-UTRAN and UTRAN/GERAN over S3	239
Figure 37	CSFB architecture	250
Figure 38	Architecture with IWF	254
Figure 39	GTP-C path initial and triggered messages	262

Figure 40 EPS quality of service information element	282
Figure 41 NAPTR procedures	286
Figure 42 Isolation of S-GW and P-GW for create session failures because of P-GW	328
Figure 43 S-GW selection based on IMSI/MSISDN range	338
Figure 44 P-GW selection based on IMSI/MSISDN range	338
Figure 45 CC bits in P-GW selection	340
Figure 46 3G to 4G IRAT handover SP-GW reselection for NSA capable UE	350
Figure 47 Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query	363
Figure 48 Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (NRI provisioned in the MME)	363
Figure 49 Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	364
Figure 50 Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query	364
Figure 51 Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (NRI provisioned in MME)	365
Figure 52 Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	365
Figure 53 Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN)	366
Figure 54 Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN)	367
Figure 55 Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	368
Figure 56 Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	369
Figure 57 Inter-system RIM with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN)	370
Figure 58 Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query	370
Figure 59 Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	371
Figure 60 Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)	371
Figure 61 MSC selection based on IMSI range/prefix to TAI-LAI mapping	373
Figure 62 Attach reject due to unsubsribed APN	377
Figure 63 PDN connectivity reject due to unsubsribed APN	377

Figure 64	Sv-based UMTS hand down	381
Figure 65	SRVCC-capability AVP value towards the HSS	385
Figure 66	Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions IE based on system capability	386
Figure 67	Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions IE based on IMSI prefix, UE capability, and MS network capability	387
Figure 68	Attach example	392
Figure 69	Intra-LTE TAU example	392
Figure 70	X2-based handover example	393
Figure 71	S1-based handover example	393
Figure 72	TAU restricted to EPS only with configurable NAS code	396
Figure 73	Attach restricted to EPS only with configurable NAS cause	397
Figure 74	IMS supervision	397
Figure 75	Operator-defined QCI	405
Figure 76	EPS LCS reference architecture	422
Figure 77	Protocol layering for E-SMLC to UE signaling	423
Figure 78	Protocol layering for E-SMLC and eNB	424
Figure 79	Protocol layering between MME and GMLC	424
Figure 80	Protocol layering between E-SMLC and MME	425
Figure 81	3GPP EPC MT-LR procedure	428
Figure 82	MT-LR without contacting E-SMLC	429
Figure 83	HeNB architecture	433
Figure 84	Gaps in supporting X2 handover	440
Figure 85	LIPA architecture	441
Figure 86	MBMS network architecture	449
Figure 87	M3AP protocol stack	450
Figure 88	Sm protocol stack lower layers	451
Figure 89	MCE failure/restart	460
Figure 90	M3AP path failure/recovery	461
Figure 91	MME restart	462
Figure 92	Transient Sm path failure	463
Figure 93	Non-transient Sm path failure	464
Figure 94	Sm path recovery	464
Figure 95	MBMS GW restart	465
Figure 96	Non-transient SGmb path failure	466
Figure 97	BM-SC failure/restart	467
Figure 98	MME/SGSN lawful interception architecture	469
Figure 99	LI interfaces in MME/SGSN	472
Figure 100	Use of ARP during initial attach (call flow)	476
Figure 101	Interim location to PSAP, control plane call flow	479
Figure 102	Restoration of warning message delivery upon eNB restart	485
Figure 103	Provisioning restriction for warning area list in SBc Write Replace Warning	

Request message	487
Figure 104 Provisioning restriction for warning area list in SBc Stop Warning Request message	487
Figure 105 Provisioning restriction for warning area list when a race condition occurs	488
Figure 106 Periodic TAU timer override at attach	498
Figure 107 UE power savings mode	499
Figure 108 T3324, T3412, mobile reachable timer and UE implicit detach timer	500
Figure 109 Back-off timer for overload control	502
Figure 110 EMBS	502
Figure 111 MOCN	503
Figure 112 Subscriber relocation to IoT core network	504
Figure 113 Relationship between SFN and H-SFN	505
Figure 114 MME time offsets and eDRX PTW	506
Figure 115 Option 2 for handling MT SMS for UE in the power saving mode	514
Figure 116 eDRX selection at Attach/TAU Request	521
Figure 117 PSM T3324 (active timer) selection at Attach/TAU Request	522
Figure 118 CloT architecture	525
Figure 119 Overload Start/Stop for LPA UEs (enhanced access barring)	527
Figure 120 Support for EMM-REGISTERED UE without a PDN connection	531
Figure 121 Tunneling of S1AP messages associated with CloT Attach/TAU Requests	534
Figure 122 Connection suspend procedure	540
Figure 123 Connection resume procedure	541
Figure 124 Connection resume procedure from a different eNB	542
Figure 125 Establishment of S1-U bearer during data transport in control plane CloT EPS optimization	543
Figure 126 Inter-UE QoS for NB-IoT UEs using control plane CloT EPS optimization	545
Figure 127 Control plane CloT optimizations through SGI	550
Figure 128 ROHC	551
Figure 129 Non-IP with S1-U	553
Figure 130 S1-U transport layer address (TLA) of IPv4v6 address type	554
Figure 131 NIDD over T6a/SCEF architecture	555
Figure 132 Architecture	560
Figure 133 CMM with the same SCTP association shared between different interfaces	570
Figure 134 Generation of LoC reports when the UE exits a PTW within an eDRX cycle	577
Figure 135 IWF-SCEF connections via DRAs	582
Figure 136 SMS in MME architecture with IWF	587

Figure 137	SMS registration	589
Figure 138	HSS-triggered SMS deregistration	590
Figure 139	MME-triggered SMS deregistration	591
Figure 140	Successful MT SMS delivery	592
Figure 141	Successful MO SMS delivery	597
Figure 142	Option 3a (SCG bearer)	629
Figure 143	Option 3x (SCG split bearer)	630
Figure 144	Secondary RAT usage report is provided by S1AP E-RAB-RELEASE-RESPONSE	633
Figure 145	Secondary RAT usage report is provided by S1AP E-RAB-RELEASE-INDICATION	633
Figure 146	Secondary RAT usage report is provided by S1AP E-RAB-MODIFICATION-INDICATION	633
Figure 147	Secondary RAT usage report is provided by S1AP UE-CONTEXT-RELEASE-REQUEST	634
Figure 148	Secondary RAT usage report is provided by S1AP UE-CONTEXT-RELEASE-COMPLETE	634
Figure 149	Secondary RAT usage report is provided by S1AP UE-CONTEXT-SUSPEND-REQUEST	634
Figure 150	Handover flag not present	635
Figure 151	Handover flag is true	636
Figure 152	Ongoing handover procedure	636
Figure 153	MME relocation	637
Figure 154	EPS to 5GS registration procedure	640
Figure 155	5GS to EPC TAU procedure using the N26 interface	642
Figure 156	EPS to 5GS handover using N26 interface, preparation	644
Figure 157	EPS to 5GS handover using N26 interface, execution	645
Figure 158	5GS to EPS handover procedure using N26 interface	646
Figure 159	Overload control	656
Figure 160	MME's actions for UEs associated with a failed S11 path	678
Figure 161	SRS phase 1 geo-redundancy architecture	689
Figure 162	Pool redundancy upgrade and downgrade use cases	699
Figure 163	SRVCC HO - X2 HO collision handling	717
Figure 164	ANR	722
Figure 165	UE denylisting logic	726
Figure 166	Example of S1 flex implementation	737
Figure 167	Subscriber move based on IMSI/MSISDN range	741
Figure 168	S-GW geo-redundancy through ICR	744
Figure 169	Signaling flow of MSC/VLR offloading when UE is in ECM-CONNECTED state	752
Figure 170	Signaling flow of MSC/VLR offloading when UE is in ECM-IDLE state	753
Figure 171	Use of multiple S1-MME IP addresses to segregate traffic to eNBs of different	753

PLMN	763
Figure 172 Clusters of operator's using eNBs using different S1-MME IP addresses	763
Figure 173 Dual stack support	766
Figure 174 Relationship of an SCTP association to streams	773
Figure 175 L3NS and multiple IPDS	795
Figure 176 PCMD flow	799
Figure 177 4G + 5G flow	800
Figure 178 HSS-initiated call trace	812
Figure 179 Service mirroring	815
Figure 180 Stdout and Fluentd on a CNF CMM	817
Figure 181 Fluentd on a CNF CMM with stderr	818
Figure 182 MME/SGSN lawful interception architecture	826
Figure 183 Example of a CNF MME multi-IPDS configuration	829
Figure 184 CMM with two simplex DBS instances	832
Figure 185 EEMS in VNF CMM	841
Figure 186 EEMS in CNF CMM	841

List of Tables

Table 1	Release 12 and Release 13 standards update impacts	44
Table 2	Release 13 and Release 14 standards update impacts	47
Table 3	Release 14 and Release 15 standards update impacts	52
Table 4	Release 14 and Release 15 standards update impacts for UE monitoring	59
Table 5	Supported 3GPP release 15 March 2019 and June 2019 CRs	60
Table 6	Supported 3GPP release 15 Sept 2019 and December 2019 CRs	61
Table 7	Supported 3GPP release 16 for September 2019 and December 2019 CRs	63
Table 8	Supported 3GPP release 16 March/June/Sept/Dec 2020 and March 2021 CRs	65
Table 9	HSS user profile management procedures	82
Table 10	IMSI	91
Table 11	Paging DRX value	114
Table 12	IEs sent to MME in S1 setup procedure	133
Table 13	Information elements (IEs) sent to TA parameters	134
Table 14	Information elements related to NITZ	159
Table 15	Provisionable EMM/ESM cause code values for existing scenarios before this feature	165
Table 16	Provisionable EMM/ESM cause code values for scenarios introduced by the feature	166
Table 17	RFSP Index	171
Table 18	MME behavior based on related-settings	175
Table 19	Per PLMN provisionable roaming parameters (svcAgreementProfile)	179
Table 20	MME actions depending on UE APN OI and APN NI	204
Table 21	DNS realm selection for APN FQDN for NAPTR query, home subscriber	205
Table 22	DNS realm selection for APN FQDN for NAPTR query, treat as home subscriber	206
Table 23	DNS realm selection for APN FQDN for NAPTR query, inbound roamer	206
Table 24	DNS realm selection for APN FQDN for NAPTR query, inbound roamer with home routed APN	207
Table 25	IMS PDN connection setup during attach and standalone PDN connection	209
Table 26	Roamer IMS PDN connection during inter-PLMN TAU	210
Table 27	IMS APN roaming control provisioning	211
Table 28	Received and provisioned PCI and PVI	212
Table 29	Feature interaction: features f10112-01 and f10101-01	212
Table 30	3GPP versions and corresponding gtpTargetIdEncoding parameters	230

Table 31	MNC+MCC encoding/decoding for 3GPP versions between CR0668 and CR0808	231
Table 32	MNC+MCC encoding/decoding for 3GPP versions are newer than CR0808	231
Table 33	Gn target ID format based on GTP target ID encoding value	231
Table 34	Optional IE in SGsAP messages	255
Table 35	QCI to 2G/3G QoS parameters (TS 23.401)	279
Table 36	2G/3G QoS parameters to QCI	280
Table 37	S-NAPTR record fields	287
Table 38	Definitions of NAPTR record fields	288
Table 39	Attach procedure: Cause values and MME actions	291
Table 40	Standalone PDN connectivity request procedure: Cause value and MME actions	293
Table 41	S-GW relocation: cause values and MME actions	295
Table 42	RData field of the RR record	298
Table 43	Search order for service capabilities	306
Table 44	Service selection for multiple service parameters	308
Table 45	Search order for service capabilities	309
Table 46	S-GW and P-GW reselection in attach procedure	343
Table 47	P-GW reselection in standalone PDN connectivity request	343
Table 48	P-GW reselection in standalone PDN connectivity request with Request Type Handover	343
Table 49	S-GW selection during intra-LTE handover, inter-RAT handover and intra-LTE and inter-RAT idle mobility	344
Table 50	IMS voice over PS support	378
Table 51	Combinations of VDP and UE's usage setting (VDP profiles)	390
Table 52	VDP and UE's usage setting combinations and forbidden TAI list sending	391
Table 53	UE IMSI is not in any provisioned IMSI series	402
Table 54	UE IMSI is in a provisioned IMSI series	403
Table 55	Global eNB ID IE	434
Table 56	Class 1 elementary procedures (M3AP)	451
Table 57	Class 2 elementary procedures	451
Table 58	Class 1 elementary procedures (Sm)	452
Table 59	Sm to M3 information element mapping for session start procedure	454
Table 60	Sm IE to M3 IE mapping	456
Table 61	LI functions and VM/link usage	469
Table 62	Devices	497
Table 63	Key terms of eDRX paging opportunity calculation	506
Table 64	MME PTW time offsets	507
Table 65	Minimum T3412 timer	517
Table 66	Timers	549

Table 67	CMM support for Rel 16 MONTE and CIoT CRs	561
Table 68	No RIR sent scenarios	565
Table 69	SMS registration (UE input: combined attach or inter-MME/inter-system TAU with combined TA/LA updating, no update type, no NB-IoT)	601
Table 70	SMS registration (UE input: EPS attach or inter-MME/inter-system TAU with TA updating, with 'SMS only' update type, NB-IoT true	602
Table 71	Cause value mapping from S1AP cause to NGAP cause	650
Table 72	Cause value mapping from NGAP cause to S1AP cause in case of failure	651
Table 73	Cause value mapping from NGAP cause to S1AP cause	652
Table 74	Cause value mapping from S1AP cause to NGAP cause in case of failure	653
Table 75	Mapping of SCTP chunk types to threshold	670
Table 76	P-CSCF recovery modes	682
Table 77	Behavior content	726
Table 78	Parameters controlling S6a fault handling	729
Table 79	CPPS N+K sparing	757
Table 80	Diameter application profile logical view	781
Table 81	GTP profile T3/N3	785
Table 82	Progression of capacity as configuration is grown for MME-only deployments	793
Table 83	Progression of capacity as configuration is grown for MME/SGSN deployments	794
Table 84	Additional component type fields included in JSON	819
Table 85	LI functions and VM/link usage	826
Table 86	CPPS and DBS VM size options	833
Table 87	CPPS VM size options	834
Table 88	DBS VM size options	835

Summary of changes

A list of changes between document issues. Click the links to view the updated sections.

Changes between issues 13-0 (CMM22.2) and 14-0 (CMM22.5)

New and updated features in CMM22.5

- [CMM support for CLI command to explicitly detach all UEs for an input roaming PLMN \(Feature f10428-01\)](#)
- [Treating an IMSI series as home subscribers \(Feature m10132-01\): updated the note about roamer that are treated as home subscribers](#)
- [MME support for customization of HRL equivalent PLMN list \(Feature f10910-02\)](#)
- [MME support for forming APN FQDN on non-3GPP handover scenarios \(Feature f10560-01\)](#)
- [MME support for CS Service Notification Repeat after UE re-establishment \(Feature f10936-01\)](#)
- [Enhancement to APN correction to accommodate maximum of 255 APNs \(Feature f10107-08\)](#)
- [MME support for APN rate control status \(Feature f11701-22\)](#)
- [CMM support for configuration control for restriction of P-GW selection to colocated GGSN/P-GW during IRAT mobility \(Feature f10172-01\)](#)
- [MME support for sending P-GW FQDN in EPS to 5GS mobility \(Feature f10125-09\)](#)
- [MME support for flexibility in configuring the S1AP cause codes \(Feature f10902-02\)](#)
- [MME support for CSG ID enhancements \(Feature f10906-03\)](#)
- [CMM support for Rel 16 MONTE and CloT CRs \(Feature f11733-11\): updated description for 3GPP TS 29.272 v16.1.0 CR 0810 Standard/CR](#)
- [MME support for wake-up signal for CloT \(Feature f11701-21\)](#)
- [CMM support for Ethernet PDU for mobility across N26 interface \(Feature f20102-01\)](#)
- [Directed inter-MME subscriber move \(Feature m10713-01\): updated the related descriptions](#)
- [CMM support for using REMc \(Feature f70012-03\): updated the whole description](#)
- [MME support for DDN Ack for abnormal S-GW geo-redundancy switchover \(Feature f10188-01\)](#)
- [CMM support for sending log and alarm information to std::out in addition to current destinations \(Feature f14402-01\): updated the information provided about the CMM logs and the information related to the host side](#)
- [CMM support for streaming PM XML file to Fluentd \(Feature f14402-03\): updated the](#)

information provided about the docker log driver and the information related to the host side

- CMM support for network trace/trace all for MME/SGSN CNF (Feature f23401-02)
- CMM support for show command to display 20 representative IMSIs for an input PLMN (Feature f13406-01)
- CMM support for CMPv2 protocol (Feature f13216-01)
- CMM support for MME and AMF using flow distribution - delivery (Feature f72002-43): removed the reference to the capacity limits
- CMM support for flow distributor with multi-home and dynamic flow control (Feature f72002-48)
- MME support for 24K UE radio capability information using RCIS for VNF (Feature f10937-01)
- Support for CPPS VM auto-balancing AMMS and EMMS for quad access (Feature f20060-07): added a note about reverting personality changes

Removed features in CMM22.5

- *MME support for provisionable S1AP Cause Codes (Feature f10902-01): removed. This feature is enhanced by MME support for flexibility in configuring the S1AP cause codes (Feature f10902-02)*

Changes between issues 12-0 (CMM22) and 13-0 (CMM22.2)

New and updated features in CMM22.2

- MME support for 3GPP standard update release 16 for March/June/Sept/Dec 2020 and March 2021 - phase 2 (Feature f10002-09)
- MME support for GUTI reallocation upon expiration of refresh timer (Feature f10414-01)
- MME support for paging upon T-ADS received in IDR message (Feature f10228-01)
- MME support for combined attach without CS (Feature f10426-01)
- MME support for ignoring malformed PDN connection in mobility scenario(s) (Feature f13501-08)
- MME support for adding s1hoResourceReleaseWithNoMmeSgwRel timer (Feature f10568-01)
- MME support for RFSP enhancement (Feature f51024-04)
- MME support for single IMSI group HSS unavailability/down declaration (Feature f11346-01)
- MME support for sending RAT-Frequency-Selection-Priority-ID update to eNB received in

IDR from HSS (Feature f10939-01)

- MME support for local provisioning of UE usage type based on 5G subscription (Feature f11601-07)
- MME support for dedicated core network enhancement (Feature f11601-08)
- MME support for PSCell IE to determine UE location (Feature f10935-01)
- MME support for improved table management for P-GW isolation/gwNodeAdmin (Feature f10166-03)
- CMM support for configurable DNS timeout alarm (Feature f12115-02)
- MME support for handling nc-smf tagged service type for non-N1-mode UEs (Feature f20003-15)
- MME support for receiving new PRA action during additional procedures (Feature f10904-34)
- CMM support for inter-release pool redundancy versions (Feature f14109-09): added a reference to the *Release Compatibility Report*
- MME support for HSS unavailability recovery (Feature f11318-02)
- MME support for override diamConnection profile default value parameters per UE PLMN service (Feature f11347-01)
- MME support for additional static and component counters (Feature f13029-02)
- CMM support for additional PM counter for CMM system up time (Feature f13036-01)
- MME support for UE counts per eNB (Feature f14117-01)
- CMM support for streaming PM XML file to Fluentd (Feature f14402-03)
- CMM support for MME and AMF using flow distribution - delivery (Feature f72002-43)
- Support for quad access (Feature f20060-05): updated commands for controlling the capability
- Support for CPPS VM auto-balancing AMMS and EMMS for quad access (Feature f20060-07): added note about reverting personality changes

General changes

- Moved chapter *Multi-IPDS deployments on CNFs* from *MME User Guide* to *MME Feature Overview*

Changes between issues 11-0 (CMM21.8) and 12-0 (CMM22)

New and updated features in CMM22

- CMM support for EIR enhancements (Feature f11309-02): updated description.
- MME support for enhanced condition to trigger page gap timer (Feature f10227-01)

- MME support for paging when cause code received in UE Context Release Request with cause code = Inter-RAT Redirection (Feature f10226-01)
- MME support for preserving VLR for sending NOR to HSS for SGSN to MME tracking area update procedure (Feature f10425-02)
- CMM support for multiple TAC operation trigger enhancements (Feature f14622-01): added
- CMM support for sending HRL in all messages where CMM supports HRL IE (Feature f10910-03)
- Connected mode mobility enhanced for reserved cells (Feature m10908-01): added the `rfspIndexVoiceCapableUe` parameter of the `svcAgreementProfile` command for voice capable UE and the description about when to select the provisioned generic RFSP index
- MME support for steering option 3x subs to combo nodes for capacity offload - phase 3 (Feature f10004-03)
- MME support for emergency call enhancements on LTE (Feature f11020-01)
- MME support for IoT purge timer provisioning range to 30 days (Feature f12005-01)
- MME support for accepting connection release from SCEF for temporarily unreachable UE (Feature f11701-20)
- MME support for new PRA action on 5GS to EPS mobility for DC PRA (Feature f10904-35)
- CMM support for NR10 optimization enhancements (Feature f14109-14)
- IPv4/IPv6 dual stack (Feature m10403-01): removed Traffica from the MME interfaces due to CMM support for Kafka Removal (Feature f14203-02).
- MME support for SGd on combined SCTP association (Feature f11004-05)
- Operability: removed Traffica reference due to CMM support for Kafka Removal (Feature f14203-02).
- Real time monitoring: removed Traffica reference
- PM evolution for static counters (Feature f13012-02): removed Kafka-related information
- PM evolution for component counters (Feature f13012-03): removed Kafka-related information
- CMM support for enabling Prometheus direct scraping of metrics (Feature f14705-01)

Removed features in CMM22

- MME support for sending NOR to HSS for Gn/Gp SGSN to MME tracking area update procedure (Feature f10425-01): removed. The feature replaced and enhanced by MME support for preserving VLR for sending NOR to HSS for Gn/Gp SGSN to MME tracking area update procedure (Feature f10425-02).
- Section Traffica removed due to CMM support for Kafka Removal (Feature f14203-02).

- Some lawful interception related features are removed because they are documented in the *Lawful Interception* document:
 - CMM support for SHA-256 onwards hash in IPsec (Feature f13206-01)
 - CMM support for LI enhancement (Feature f10314-03)
 - Consistency check with LIPv2 (Feature f10307-01)
 - Lawful interception for SMS (Feature f11004-04)
 - ASN.1 encoding userLocationInfo without the octets containing length (Feature f10321-01)
 - Lawful interception unique encryption key/element (Feature f10306-01)

1. Introduction

This document provides a general description of the features available for Nokia Cloud Mobility Manager MME.

The Cloud Mobility Manager (CMM) performs the 3GPP mobility and session management control functions in the 5GC, EPC and GERAN/UTRAN network.

Cloud Mobility Manager (CMM) application introduces the mobility management entity (MME) control plane functionality as a part of the Nokia long-term evolution (LTE) offering. The MME is a pure control element in a flat network architecture optimized for LTE use.

For more information about general introduction about the CMM, see *Product Description*.

2. Standards updates

Features supporting and incorporating 3GPP release CRs.

2.1 Release 12 and Release 13 standards update for MME (Feature f10001-01)

This feature supports and incorporates final phase of Release 12 CRs that are introduced for Dec 2014. In addition, this feature introduces Critical CRs from 3GPP Release 13 2016. Critical CRs for Release 13 2016 include CRs from March, June, September, and December of 2016.

Table 1: Release 12 and Release 13 standards update impacts

Standard/CR	Description
TS 23.216 CR 0332	When the MME determines that SRVCC operation possible to eNB needs to be updated, for example, when the UE updates its SRVCC capability indication when in connected mode, the MME immediately provides the updated SRVCC operation possible value in use to eNB by modifying an existing UE context. The MME sends SRVCC operation possible change to an eNB either in a subsequent DOWNLINK NAS TRANSPORT message or in HANOVER REQUEST.
TS 23.246 v13.1.0 CR 0396	MME includes the capability to include a list of cell IDs IE if available in the MBMS session start and update procedures.
TS 23.272 CR 0941 TS 29.118 CR 0343	If the SGs Paging Request does not contain the LAI, and if the MME can retrieve the S-TMSI associated to the IMSI, the MME temporarily stores this MSC/VLR number and forces the UE to re-attach to the non-EPS services based on: <ul style="list-style-type: none"> If the UE is in connected mode, the MME does not send a SGs Service Request to the MSC/VLR as it normally would, but instead sends a Detach Request (IMSI Detach) to the UE as described in clause 5.3.2 of 23.272 If the UE is in idle mode and if the mobile reachable timer is still running, the MME pages the UE with IMSI and the CS indicator (for CSFB) or with S-TMSI and the PS indicator (for SMS). At the reception of Extended Service Request (for CSFB) or Service Request (for SMS) from the UE, the MME does not send a SGs Service Request to the MSC/VLR as it normally would, but instead sends a Detach Request (IMSI Detach) to the UE as described in clause 5.3.2 of 23.272.

Standard/CR	Description
TS 23.401 CR 2825	MME does not send DDN Reject (that is, DDN Failure Indication) to S-GW when the old MME detects inter MME/SGSN idle mode mobility, that is, when old MME receives Context Request message and is waiting for Context Acknowledge message.
TS 23.401 CR 2865	MME includes CSG information if available in Create Session Request that is sent to the new S-GW during S-GW relocation.
TS 23.401 CR 2928	If the S1 connection had already been released by the eNB due to radio link failure and the MME receives a Delete Bearer Request while it is still deferring the sending of the S1 release (see 23.401 sub clauses 5.3.5), the MME includes in the Delete Bearer Response the RAN/NAS Cause received in the S1 Release due to radio link failure procedure.
TS 23.401 Clause 5.5.3.2.7 item a	MME sends S1AP PAGING message for each paging attempt using S-TMSI from old GUTI and also S-TMSI from the new GUTI. MME is not required to page UE with IMSI if paging with old and new S-TMSI fails. MME supports provisioning of global parameter to allow old GUTI paging per MME: <code>enableOldGutiPaging</code> . The default value is <code>No</code> .
TS 29.168 CR 0058	MME supports a new PWS Failure Indication message from MME to CBC. MME initiates the PWS Failure Indication procedure by sending a PWS FAILURE INDICATION message to the CBC upon receiving a PWS Failure Indication message from an (H)eNB (TS 36.413). The MME copies the Global eNB ID of the (H)eNB and E-CGI List Failed for PWS into the Failed-Cell-List parameters from the PWS Failure Indication received from the (H)eNB into the corresponding parameters in the PWS-FAILURE-INDICATION towards the CBC.
TS 29.272 v12.6.0 CR 0578	When sending the ULR command for a certain user due to HSS restoration procedure (after the MME has received a Reset command from the HSS), the MME may consider the stored address/name of the HSS for the user to be invalid and hence not known.
TS 29.274 v13.3.0 CR 1667	MME sets Operation Indication flag to 1 in a Create Session Request on S11 interface for MME-triggered S-GW relocation.
TS 29.274 v13.3.0 CR 1626	MME supports Cell List IE that is encoded as an ECGI-List Type in MBMS Session Requests that is accepted by MME. MBMS GW provides the MBMS Cell List in the MBMS Session Start Request and Session Update Request over the Sm interface if received from the BM-SC. The MBMS Cell List can contain from 1 up to 4096 cells.

Standard/CR	Description
TS 29.274 v13.3.0 CR 1663	<p>MME includes RAN/NAS Cause in Delete Bearer Response on the S11 interface to indicate the RAN release cause and/or NAS release cause to release the bearer. If both a RAN release cause and a NAS release cause are generated, several IEs with the same type and instance value are included to represent a list of causes. The S-GW includes this IE on the S5/S8 interface if it receives it from the MME.</p>
TS 29.274 v13.5.0 CR 1710	<p>During a Network Triggered Service Request procedure, which is triggered by a dedicated bearer creation procedure towards a UE in Idle mode, the MME includes only the existing Bearer Contexts (not the new Bearer Contexts just created) in the corresponding Modify (Access) Bearer Request message. The same principle applies the Modify Bearer Request is piggybacked in the Create Bearer Response message.</p>
	<p> Note:</p> <p>During a Network Triggered Service Request procedure, which is triggered by a dedicated bearer creation procedure towards a UE in Idle mode, bearer mismatches can be avoided by the MME sending the Create Bearer Response only after it receives the Modify Bearer Response message. However, in some rare cases, the signaling can be delayed for the UE, for example, if the Modify Bearer Response is lost.</p>
TS 36.413 CR 1305	<p>The CR adds clarification on how bits are mapped.</p>
TS 36.413 CR 1373	<p>The CR introduces a new PWS Failure Indication message. The purpose of PWS Failure Indication procedure is to inform the MME that ongoing PWS operation for one or more cells of the eNB has failed. The procedure uses non UE-associated signaling.</p>
TS 36.444 v13.0.0 CR0072	<p>MME includes MBMS Cell list IE in MBMS Session Start and MBMS Session Update Request message that is sent to MCE. If the MCE receives MBMS SESSION START REQUEST message including the MBMS Cell List IE and the list includes no cell controlled by eNB with which the MCE has connection, the MME is informed by the MBMS SESSION START FAILURE message including a suitable cause value, for example, Un-involved MCE.</p>
	<p> Note:</p> <p>3GPP calls for supporting 4096 cell ids, however, MME supports 1024 cell ids.</p>

2.2 Release 13 and Release 14 standards update for MME (Feature f10002-01)

This feature supports and incorporates the final phase of Release 13 CRs that were introduced for March 2017. This feature also incorporates remaining CRs from WM11.0 and introduces critical CRs from 3GPP Release 14 June, Sept, Dec 2016, and March 2017.

Table 2: Release 13 and Release 14 standards update impacts

Standard/CR	Description
3GPP TS 29.118 Mobility Management Entity (MME) - Visitor Location Register (VLR) SGs interface specification:	
CR 0370r1	If the MME has a stored TMSI for a UE, the MME can include this TMSI in the TMSI based NRI container IE in the SGsAP-LOCATION-UPDATE-REQUEST message. Otherwise the MME indicates "no valid TMSI available" in the TMSI status IE in the SGsAP-LOCATION-UPDATE-REQUEST message. If the VLR included the location area identifier or the mobile identity information element in the SGsAP-LOCATION-UPDATE-ACCEPT message, the MME stores the received location area identifier or the mobile identity information element for the subsequent location update for non-EPS services procedures for the UE. If the mobile identity information element contains a new TMSI, the MME sends to the VLR the SGsAP-TMSI-REALLOCATION-COMPLETE message when the MME indicates to the UE the acceptance of SMS services. If the mobile identity information element contains an IMSI, the MME deletes any stored TMSI for the UE.
3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS):	
CR 2207	The MME supports TS 24.301 CR 2207 by handling the collision scenarios mentioned in White Paper C1-152857.
CR 2568r2	The MME supports the provisioning of the following parameter for Attach Reject and TAU Reject when Attach Request or TAU Request is rejected due to CloT features unsupported by the MME: Send Extended EMM cause IE with bit 2 of octet 1 set to indicate that "requested EPS optimization is not supported" when EMM cause value #15 is used in attach reject due to unsupported CloT features. The default is Set the EPS optimization info bit.

Standard/CR	Description
CR 2677	<p>This requirement specifies various changes introduced in 3GPP in MME and UE handling of attach request with and without the support of EMM-REGISTERED without PDN connection.</p> <ul style="list-style-type: none"> • If EMM-REGISTERED without PDN connection is not supported by the UE or the MME, and the Activate Default Bearer Context Request message combined with the Attach Accept is not accepted by the UE due to failure in the UE ESM sublayer, the UE initiates the detach procedure by sending a Detach Request message to the network. Further UE behavior is implementation specific. • If EMM-REGISTERED without PDN connection is supported by the UE and the MME, and the Activate Default Bearer Context Request message combined with the Attach Accept is not accepted by the UE due to failure in the UE ESM sublayer, the UE either sends an Attach Complete message together with an Activate Default EPS Bearer Context Reject contained in the ESM message container information element to the network or initiates the detach procedure by sending a Detach Request message. Further UE behavior is implementation specific. In this case, the MME keeps the UE EMM-REGISTERED without PDN connection if the MME receives Attach Complete with an Activate Default EPS Bearer Context Reject. • If EMM-REGISTERED without PDN connection is supported by the UE and the MME, and the MME receives an Attach Request message with an ESM message included in the ESM message container information element, and the ESM sublayer in the MME detects a message error per clause 7 (Handling of unknown, unforeseen, and erroneous protocol data), the MME can decide to proceed with the attach procedure or to reject it. When sending the Attach Accept or Attach Reject message to the UE, the MME includes the ESM message provided by the ESM layer in the ESM message container information element.
CR 2771r3	<p>The MME supports a provisioning parameter per MME to include SMS Services Status IE in Attach Accept and TAU Accept message, if the MME fails to set up SMS for NB-IoT UEs and MME only accepts EPS attach only. The MME sets the SMS Services Status for the following MME or MSC/VLR Cause codes as follows:</p> <ul style="list-style-type: none"> • SMS is not enabled for home subscriber - SMS service is not available • SMS is not enabled for a roamer - SMS service is not available in this PLMN • Congestion from MSC/VLR - Congestion • All other MME or MSC/VLR failure causes - Network failure

Standard/CR	Description
CR 2765r4	<p>CAT-M1 CE Mode B UE EMM Timer Increment and CAT-M1 CE Mode B UE ESM Timer Increment parameter provisioning have been replaced as follows:</p> <ul style="list-style-type: none"> • CAT-M1 CE Mode B UE EMM timer values: <ul style="list-style-type: none"> - T3422 timer: default: 24 seconds, Range: 1 to 60 seconds - T3450 timer: default: 18 seconds, Range: 1 to 60 seconds - T3460 timer: default: 24 seconds, Range: 1 to 60 seconds - T3470 timer: default: 24 seconds, Range: 1 to 60 seconds • CAT-M1 CE Mode ESM timer values: <ul style="list-style-type: none"> - T3485 timer: default: 16 seconds, Range: 1 to 60 seconds - T3486 timer: default: 16 seconds, Range: 1 to 60 seconds - T3489 timer: default: 12 seconds, Range: 1 to 60 seconds - T3495 timer: default: 16 seconds, Range: 1 to 60 seconds

3GPP TS 23.007 Restoration procedures

CR 0318	When establishing MBMS bearer services in an MCE, to ensure the distribution of content from ongoing MBMS sessions to an MCE that modifies the lists of the MBMS service areas it serves via the MCE configuration update procedure, the MME encodes the MBMS Session Start Request upon receipt of a Reset or M3 Setup Request message from the MCE.
CR 0320	Upon receipt of an HSS reset, the MME marks each relevant MM context as invalid and sets the non-EPS Alert Flag (NEAF), if an MME - MSC/VLR association exists. After detection of any activity (either signaling or data) from a marked UE or any other implementation-dependent trigger for a marked UE in ECM-CONNECTED state, the MME performs an update location to the HSS as in the attach or inter-MME TA update procedures and, if NEAF is set, the procedure of NON-EPS Alert is followed.

3GPP TS 29.272 Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on the Diameter protocol:

CR 0619	When receiving an Update Location Response from the HSS in the TAU procedure, for each of the received APN-Configurations in the APN-Configuration-Profile, if both the MIP6-Agent-Info and the PDN-GW-Allocation-Type AVPs are absent in the APN-Configuration AVP and the MME has associated P-GW information and the UE-level access restriction "HO-To-Non-3GPP-Access Not Allowed" is not set, the MME sends a Notify Request if HO to the WLAN is supported in the network, including the APN and PDN GW identity to the HSS in order to restore this information in the HSS, for example, after a reset procedure
---------	--

Standard/CR	Description
CR 0641	If the MME receives a Delete Subscriber Data Request with DSR-Flags (bit 23) set (MSISDN Withdrawal), it indicates to the MME that the MSISDN is deleted from the subscriber data. However, if the MSISDN is deleted from the subscription data, the MME maintains the existing MSISDN throughout the lifetime of the existing PDN connections that were established prior to the deletion of the MSISDN (that is, other network nodes, such as PDN-GW, are not informed of such deletion for the existing PDN connections).
CR 0655	If the MSISDN is deleted from the subscription data, the MME maintains the existing MSISDN throughout the lifetime of the existing PDN connections that were established prior to the deletion of the MSISDN (that is, other network nodes, such as PDN-GW, are not informed of such deletion for the existing PDN connections).
CR 0671	If the MME determines that it needs to update Homogeneous Support of IMS Voice Over PS Sessions in the HSS, the MME sends a Notify Request with the "Homogeneous Support of IMS Voice Over PS Sessions" bit set (bit 7) in the NOR-Flags AVP; if there is homogeneous or non-support of IMS Voice Over PS Sessions, the MME reports it by including the updated Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP; if the support is not homogeneous, the MME reports it by leaving such AVP absent in the Notify Request to the HSS.
CR 0697	If an MME receives a Delete Subscriber Data Request with the "Complete APN Configuration Profile Withdrawal" bit set in the DSR-Flags AVP, it returns an error with a Result-Code set to DIAMETER_UNABLE_TO_COMPLY.
3GPP TS 29.274 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)	CR 1653 The MME supports the cause code “UE Not Authorized Cause Code Support Indicator” within the Create Session Request to indicate to the P-GW that the MME supports the new cause code. The new cause “UE not authorized by OCS or external AAA Server” is added to the Create Session Response message. The mapping of the new GTP cause code to the ESM NAS cause code #29 is added to the hardcoded mapping table.

Standard/CR	Description
CR 1806	<p>The MME does not check the PLMN ID in the TMGI received in the MBMS Session Start Request message against the PLMN IDs either reported by the MCEs or configured as supported PLMNs, when supporting the shared MBMS network over E-UTRAN.</p> <p> Note:</p> <p>When deploying a shared MBMS network over E-UTRAN, the TMGI for a service can contain a different PLMN ID than the one was reported by the MCE at M3 Setup, or the ones as configured in the MME. Therefore, the MME does not check the PLMN ID in the TMGI received in the MBMS Session Start Request message against the PLMN IDs either reported by the MCEs or configured as supported PLMNs.</p>
CR 1766	<p>This CR supports the inclusion of the sender's F-TEID in the Bearer Resource Command, Delete Bearer Command, and Modify Bearer Command messages, and specifies that the receiver compares the sender's F-TEID with the stored F-TEID, and handle the message only if they are same.</p>
CR 1768	<p>This CR supports feature indication for eNB change reporting. Indication Flags IE in Create Session Request has introduced eNB Change Reporting Support Indication flag, this flag is set to 1 on S11 and S5/S8 interfaces if the MME supports location Info Change Reporting and if the MME's operator policy permits reporting of location change to the operator of the P-GW with which the session is being established.</p> <p>This CR is applicable also for the Modify Bearer Request message.</p>
CR 1778	<p>This CR supports the inclusion of IMSI in Modify Bearer Request message so that the P-GW can use the IMSI/IMEI to verify if the received message is for the right UE context, and similar issues may happen for Suspend/Resume Notification message, thus inclusion of Sender's F-TEID in the Suspend Notification and Resume Notification messages.</p>

Related descriptions

- [Extended NAS timer values \(Feature f11707-01, f11707-02\)](#)
- [Enhanced homogeneous support of IMS VoPS indication to HSS \(Feature m11315-03\)](#)

2.3 Release 14 and Release 15 standards update for MME (Features f10002-03, f10002-04, f10002-05)

This feature supports and incorporates another phase of Release 14 CRs that are introduced for June and September 2017, March 2018 and June 2018. This feature also introduces critical CRs from 3GPP Release 15 June/ September/December 2017 and March/June/September/December 2018.

Table 3: Release 14 and Release 15 standards update impacts

Standard/CR	Description
	3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS):
CR 2871r2	<p>The MME enables checks for handling MO detach without integrity protection by using a global parameter <code>authntDtchIntgChkFail</code>. By default, the capability is disabled.</p> <p>The Detach Request message can be sent by the UE without integrity protection, for example:</p> <ul style="list-style-type: none"> • if the UE is attached for emergency bearer services and there is no shared EPS security context available. • due to user interaction, an attach procedure is canceled before the secure exchange of NAS messages has been established. <p>For these cases, the MME completes any ongoing procedures such as TAU request and paging before processing the detach request procedure.</p> <p>If a Detach Request message fails the integrity check, the MME proceeds as follows:</p> <ul style="list-style-type: none"> • If it is not a detach request due to switch-off, and the MME initiates an authentication procedure, the MME authenticates the subscriber before processing the detach request procedure any further. • If it is a detach request due to switch-off, or the MME does not initiate an authentication procedure for any other reason, the MME may ignore the detach request procedure and remain in state EMM-REGISTERED. <p>Note:</p> <p>The network can attempt to use additional criteria, (such as, whether the UE is subsequently still performing periodic tracking area update or still responding to paging) before marking the UE as EMM-DEREGISTERED.</p>

Standard/CR	Description
CR 2826r2	<p>For the MME, the extended protocol configuration option is supported by the network and the UE end-to-end for a PDN connection:</p> <ul style="list-style-type: none"> • if the UE is in NB-S1 mode. • if the PDN type requested for the PDN connection is non-IP. • if the UE has indicated support of the extended protocol configuration options IE in the last Attach Request or Tracking Area Update Request message, and the MME has received the extended protocol configuration options IE in at least one message sent by the PDN GW towards the UE for this PDN connection.
CR 2875	<p>The MME supports two new cause codes:</p> <ul style="list-style-type: none"> • #57 "PDN type IPv4v6 only allowed": This ESM cause is used by the network to indicate that only PDN types IPv4, IPv6, or IPv4v6 are allowed for the requested PDN connectivity. • #58 "PDN type non-IP only allowed": This ESM cause is used by the network to indicate that only PDN type non-IP is allowed for the requested PDN connectivity.
CR 2830r1	<p>If the attach request included the PDN Connectivity Request message in the ESM message container information element to request PDN connectivity, the MME when accepting the attach request will:</p> <ul style="list-style-type: none"> • send the Attach Accept message together with an ESM Dummy message contained in the ESM message container information element and discard the ESM message container information element included in the attach request if <ul style="list-style-type: none"> - the UE indicates support for EMM-REGISTERED without PDN connection in the UE network capability IE of the Attach Request message. - the MME supports EMM-REGISTERED without PDN connection and PDN connection is restricted according to the user's subscription data. - the attach type is not set to "EPS emergency attach". - the request type of the UE requested PDN connection is not set to "emergency"; • otherwise, send the Attach Accept message together with an Activate Default EPS Bearer Context Request message contained in the ESM message container information element to activate the default bearer (see subclause 6.4.1). The network can also initiate the activation of dedicated bearers towards the UE by invoking the dedicated EPS bearer context activation procedure (see subclause 6.4.2).

Standard/CR	Description
CR 2853r2	<p>If the Attach or TAU Request fails the integrity check at the MME, or integrity protection of the message cannot be checked by the MME because the message is sent without integrity protection, then the MME calculates a hash of the message it received and sends the hash to the UE in the Security Mode Command message.</p> <p>The UE calculates a hash of the Attach or TAU Request message it had sent to the network and compares it to the hash value received in the Security Mode Command message.</p> <p>If the hash calculated by the UE is different from the hash value received in the Security Mode Command message, the UE includes the Attach Request/TAU Request message into the Security Mode Complete message, and the MME uses the message in the Security Mode Complete message to complete the rest of the procedure.</p> <p>If the hash calculated by the UE is the same as the hash value received in the Security Mode Command message, the UE does not include the Attach Request/TAU Request message into the Security Mode Complete message, and the rest of the procedure completes as currently specified.</p> <p>The MME provide a global parameter <code>secureHandlingOfAttachTau</code> to enable the capability provided by the CR.</p>
CR 2761r3	<p>The MME supports provisioning per home, shared and roaming PLMN a configurable parameter “Use Non-3GPP NW provided Policies for emergency calls (<code>useNon3gppEmergencyPolicy</code>). By default, the capability is disabled. If the capability is enabled, the MME includes the Non-3GPP NW provided policies IE in the Attach Accept and TAU Accept messages. If the capability is disabled, MME does not include the IE.</p>

Standard/CR	Description
CR 2843r6	<p>For the most part, the MME supports specifications in clause 5.6.1.4.2 and 5.6.1.5. The MME supports the following additional specifications.</p> <p>The MME considers the procedure as completed successfully when any of the following occurs:</p> <ul style="list-style-type: none"> • successful completion of a NAS security mode control procedure. • receipt of an indication from the lower layer that the user plane is set up. • receipt of the Control Plane Service Request message and completion of the EMM common procedures, if any, if the MME has downlink user data or signaling not related to an EMM common procedure pending. • transmission of a SERVICE ACCEPT message. <p>After receipt of a security protected ESM message or a security-protected EMM message not related to an EMM common procedure, the UE considers the receipt of a Service Accept message as a protocol error. This means that MME must not send Service Accept message after sending EMM or ESM message. However, the MME can send the Service Accept message after the SMC to synchronize bearers.</p> <p>The MME must send the Service Reject message before the SMC because the UR considers the SMC as the acceptance of the CPSR.</p> <p>If the UE or the network receives an ESM Data Transport message including an unknown EPS bearer identity, the receiver responds with an ESM Status message with ESM cause #43 "invalid EPS bearer identity".</p>
CR 2891	<p>This CR introduces extending maximum bit rate in EPS QoS IE. An extended quality of service information element is defined to support bit rates of 20 Gbps. Additionally, an extended APN-AMBR is also defined. It is also proposed to extend the maximum bit rate encoding to support high bit rates. This IE is specified in the following message types:</p> <ul style="list-style-type: none"> • Activate Dedicate EPS Bearer Context Request • Activate Default EPS Bearer Context Request • Bearer Resource Allocation Request • Bearer Resource Modification Request • Modify EPS Bearer Context Request
CR 2919	<p>This CR specifies that the sending entity only includes the extended QoS IE or the extended APN-AMBR IE in the messages if the bit rate to be signalled goes beyond the maximum value defined in the QoS IE or the APN-AMBR IE. The minimum unit of 100 kbps in the extended QOS IE is increased to 200 kbps.</p>
CR 3135	<p>If the Network receives a Tracking Area Update Request message in response to a CS Service Notification message, the network progresses with the tracking area update procedure.</p>

Standard/CR	Description
	<p>3GPP TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access:</p> <hr/> <p>3GPP TS 29.274 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C):</p> <hr/>
CR 1824	<p>The MME always includes the newly introduced User Location Information for SGW IE in Create Session Request and Modify Bearer Request messages on the S11 interface, based on operator's policy for the user location information to be sent to the S-GW. This IE is sent even if the user location information is already reported in the User Location Information IE in this message. When present, this IE includes the ECGI, TAI, eNB ID, RAI and/or RNC-ID. In addition, the CR also introduces the following new IEs in the Create Session Request message:</p> <ul style="list-style-type: none"> • Mapped UE Usage Type • S-GW-U node name <p>The MME includes Mapped UE Usage Type on S11 interface if available. When present, this IE contains the mapped UE usage type applicable to the PDN connection.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> i Note: <p>This information is used for the S-GW-U or P-GW-U selection. Although the CR calls for sending this IE only if User Location Information IE has not been sent to the S-GW. The requirement above is modified to state that user location information for S-GW IE shall be sent.</p> </div> <hr/>
CR 1827	<p>The MME sends the S11-U MME F-TEID IE in the Modify Bearer Request message on the S11 interface if S11-U is being used for TAU with S-GW change procedure and data forwarding of downlink data buffered in the old S-GW for a control plane only PDN connection.</p>

Standard/CR	Description
CR 1831	<p>The MME supports a new condition for the Modify Access Bearer Request message. The MME sends the Modify Access Bearer Request message to S-GW if the support of extended protocol configuration option (ePCO) has not changed during inter-MME mobility.</p> <p>Note:</p> <p>During inter-MME mobility procedure, the support of ePCO may be changed. If so, the target MME uses the Modify Bearer Request message which contains the Extended PCO Support Indication bit in the Indication Flags IE, to indicate to the P-GW if the ePCO is supported or not for the PDN connection.</p>
-	<p>The MME includes ePCO IE in Delete Bearer Response if it receives from the UE. (supporting f11711-01 Extended Protocol Configuration Option (ePCO))</p>
3GPP TS 29.272 MME and SGSN related interfaced based in Diameter Protocol:	
CR 0709	<p>If the MME and the UE support attach without PDN connection (such as EMM-REGISTERED without PDN connection) and the PDN-Connection-Restricted flag is set in the received Subscription-Data-Flags AVP (IDR and ULA), the MME does not establish any non-emergency PDN connection and tears down any existing non-emergency PDN connection for this user.</p> <p>Note: PDN-Connection-Restricted bit 3 (Subscription-Data-Flags), if set, indicates to the MME that it does not establish any non-emergency PDN connection for this user if the MME and the UE support attach without PDN connection.</p>
CR 0718	<p>The MME does not use the notification procedure to inform the HSS about the identity of the dynamically selected PDN-GW, if the access restrictions indicate that the user is not allowed to get service via non-3GPP access, or the PDN type of the APN is of type "non-IP".</p> <p>This CR clarifies the list of reasons to send Notify command, that this interaction towards HSS is not needed when the APN is of type Non-IP.</p>
CR 0768	<p>The MME upon receiving a Monitoring-Event-Configuration in the ULA starts the detection of the monitoring events indicated in that AVP, if not already started, and stops the detection and deletes the previous monitoring events (if any) which are not indicated in that AVP. If Monitoring-Event-Configuration is not received, the MME stops the detection and deletes all monitoring events (if any).</p>

Standard/CR	Description
CR 0786	<p>When receiving a Monitoring-Event-Configuration in the ULA, the MME starts the detection of the monitoring events indicated in that AVP. If there is a failure when starting the detection (for example, maximum resources exceeded), the MME sends a notification of those events whose configuration have failed, as described in clause 5.2.5.1.2 (NOR/NOA messages).</p> <p>If the MME has received the monitoring event configurations in an ULA command and one, several or all event detections fail to be started (such as, due to maximum resources exceeded), the MME sends the Notify Request message with the Monitoring-Event-Config-Status AVP for the failed monitoring event configurations.</p>
CR 0785	<p>If the MME determines that a monitoring event configuration for a UE is to be deleted in the HSS (for example, the SCEF responds to a monitoring event report with DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN), the MME sends a Notify Request message with the Monitoring-Event-Config-Status AVP. The Monitoring-Event-Config-Status AVP includes the error as received from SCEF.</p>
CR 0784	<p>If the MME receives a failure response, such as DIAMETER_UNABLE_TO_COMPLY, corresponding to a Notify Request message to notify the HSS about the selected PDN-GW, the MME does not trigger a detach for the subscriber based only on this failure.</p> <p>Note: A failure to indicate the selected PDN-GW to the HSS does not impact connectivity provided via 3GPP access.</p>
CR 0770	<p>The MME supports Active-Time-Withdrawal (bit 29) in DSR flags, this bit when set, indicates that the active time used for PSM will be deleted from the subscriber data.</p>
3GPP TS 36.413 S1 Application Protocol (S1AP):	
CR 1534	<p>This CR introduces a new cause value “Release due to pre-emption”. This cause value may be used in UE Context Release Request messages, when the UE Context release in the eNB is due to RAN pre-emption action.</p> <p>For this CR, the MME supports PM counts UE Context Release Request messages with cause “Release due to pre-emption”.</p>

2.4 Release 14 and Release 15 baseline update for UE monitoring (Feature f11015-02)

This feature supports the standards updates for CMM 3GPP release 15.

Table 4: Release 14 and Release 15 standards update impacts for UE monitoring

Standard/CR	Description
TS 29.128 CR0068	This CR introduces Reporting-Time-Stamp AVP to the Monitoring-Event-Report AVP which is present when an event is reported. Inclusion of this AVP is controlled by parameter <code>includeReportingTimeStamp</code> in command <code>ueMonitoringProfile</code> .
TS 29.128 CR0070	This CR introduces Maximum-UE-Availability-Time AVP to the Monitoring-Event-Report AVP which is present when the UE reachability event is reported.
TS 23.682 CR0322	This CR introduces a minimum time interval for continuous location reporting. This CR is controlled by parameter <code>supportPeriodicLocRpt</code> in command <code>ueMonitoringProfile</code> .
TS 29.272 CR0792	This CR introduces Maximum-UE-Availability-Time AVP to the Monitoring-Event-Report AVP which is used when reporting the event type UE Reachability. When the MME reports the events, the Monitoring-Event-Report AVP is included in either the Insert Subscriber Data Answer (IDA) message or the Reporting Information Request (RIR) message based on the provisioning.
TS 29.274 CR1941	With this CR, the source MME transfers the Remaining Minimum Periodic Location Reporting Time IE to the target MME if the source MME received the Minimum Reporting Interval IE from the HSS, as defined in CR0322 TS 23.682. The remaining time is transferred in a new Monitoring Event Extension Information IE in Forward Relocation Request, Context Response, and Identification Response messages. The target MME/SGSN starts the timer with the transferred value, for example, with the time remaining from the Minimum Reporting Interval IE. This CR is controlled by parameter <code>minPerLocRptTimeOverS10</code> in command <code>ueMonitoringProfile</code> .
TS 29.274 CR1942	This CR introduces two new flags. One is to indicate whether the target MME notifies the SCEF/AS when the UE is reachable, and the other is to indicate whether the target MME notifies the SCEF/AS when the UE is idle (idle status indication). This CR is controlled by parameter <code>nsurNsuiOverS10</code> in command <code>ueMonitoringProfile</code> .

 **Note:**

If inter-MME movement occurs for a UE with a running periodic time, the source MME includes the remaining periodic time in the UE context transfer. The target MME interprets the periodic time (if included) as the remaining time until the target MME sends the first report. The target MME does not increment the PM count when the report is suppressed in such situation.

If the value of monitoring duration is less than the periodic time in the monitoring configuration, the MME does not send the report when the periodic time expires. This is because the configuration is removed when the monitoring duration is over.

2.5 MME support for 3GPP standards update (Feature f10002-06)

This feature introduces CRs from 3GPP release 15 March 2019 and June 2019.

Table 5: Supported 3GPP release 15 March 2019 and June 2019 CRs

Standard/CR	Description
TS 29.274 CR1937	<p>CR1937 introduces new indication flag '5GS interworking without N26 indication' in the Indications Flags IE in the Create Session Request message. The flag is set to 1 on S11 and S5/S8 interfaces if the 5GS Interworking Indication (5GSIWKI) is set to 1 and the N26 interface is not supported.</p> <p>Bit 7 - 5GSNN26 (5GS interworking without N26 indication): If this bit is set to 1 and the 5GSIWKI indication is set to 1, it indicates to the PGW-C+SMF that 5GS interworking is supported without the N26 interface. If this bit is set to 0 and 5GSIWKI is set to 1, it indicates to the PGW-C+SMF that 5GS interworking is supported with the N26 interface.</p> <p>The MME is provisioned with global parameter <code>support5gsIwkFlag</code> to control support for new indication flag IE in the Create Session Request message. By default, the parameter is disabled.</p>

Standard/CR	Description
TS 29.274 CR1948	<p>The MME sets Handover Indication bit flag in Create Session Request to 1 on the S11 interface during a 5GS to EPS handover without the N26 interface.</p> <p>The Handover Indication needs to be set in the Create Session Request during a 5GS to EPS handover without the N26 interface to enable the P-GW to differentiate whether the request is for a new PDN connection or a handover of an existing PDU session.</p>
TS 36.413 CR1644	CR1644 introduces extending the GUMMEI Type with an additional value 'mappedFrom5G'. This CR only has an impact on the Initial UE message procedure.
TS 29.272	The MME is provisioned with global parameter <code>supportEdrxRelatedRat</code> . When the parameter is set to <code>No</code> , existing behavior continues (that is, if eDRX-Cycle-Length-Withdrawal is provided, the eDRX cycle length is removed for both NB-IoT and E-UTRAN). If the parameter is enabled (<code>Yes</code>), the only eDRX cycle length deleted will be what the AVP specified. By default, the parameter is disabled.

2.6 MME support for 3GPP standards update (Feature f10002-07)

This feature introduces CRs from 3GPP release 15 Sept 2019 and December 2019.

Table 6: Supported 3GPP release 15 Sept 2019 and December 2019 CRs

Standard/CR	Description
TS 29.274 CR1955	This CR introduces the support of avoiding IP address switching during the PDN connection establishment and avoiding the ambiguity on which IP address the GTP-C peer uses for subsequent communication, a Create Session Request message only includes in the Sender F-TEID the same IP address type as the destination address used in the IP header. An IPv4/IPv6 capable S-GW and P-GW may advertise an IPv4 address and/or an IPv6 address in its F-TEID.

Standard/CR	Description
TS 29.274 CR1940	<p>This CR introduces enhancements to configuration transfer tunnel over the S10 interface. Enhancements to the configuration transfer tunnel procedure are required to support TNL address discovery via the S1 interface or via inter-system signalling for EN-DC. The purpose of the eNB configuration transfer is to transfer information from an eNB to a target eNB or an en-gNB connected to a target eNB in unacknowledged mode. MME shall support mandatory Target eNB ID/en-gNB ID IE which contains the ID of the target eNB or en-gNB. Additionally, Connected Target eNB ID conditional optional IE is present during an TNL address discovery request of a candidate en-gNB via the S1 interface, if the source eNB provided the ID of a target eNB connected to the target en-gNB ID.</p>
TS 29.274 CR1965	<p>This CR introduces two new indications specified below that are defined in the Create Session Request message to indicate to the PGW-C+SMF whether access to the 5GC is restricted or not for the PDN connection.</p>
TS 23.216 CR0356	<p>If a UE is handed over by an AMF, the MME obtains the equipment identifier of the UE.</p>
TS 29.171 CR0051	<p>The MME supports addition of high accuracy location estimates in SLs interface. Two new shapes, High Accuracy Ellipsoid point with uncertainty Ellipse and High Accuracy Ellipsoid point with altitude and uncertainty Ellipsoid are added to the geographic area parameter.</p>
TS 29.172 CR0042	<p>The MME supports addition of high accuracy location estimates in SLg interface. Two new shapes, High Accuracy Ellipsoid point with uncertainty Ellipse and High Accuracy Ellipsoid point with altitude and uncertainty Ellipsoid are added to the supported-GAD-Shapes AVP.</p>
TS 23.032 CR0015	<p>The MME supports mapping the new shapes from the E-SMLC to the format to send to the GMLC.</p>
TS 36.413 CR1688	<p>This CR introduces addressing race condition between X2 and S1. Interactions with E-RAB setup procedure or E-RAB modify procedure: If the E-RAB Modification Indication message is received by the MME during an ongoing E-RAB setup procedure or an ongoing E-RAB modify procedure, the MME proceeds with the E-RAB modification indication procedure.</p>

2.7 MME support for 3GPP standards update release 16 for September 2019 and December 2019 - phase 1 (Feature f10002-08)

This feature supports the standards updates for 3GPP release 16 September 2019 and December 2019.

Table 7: Supported 3GPP release 16 for September 2019 and December 2019 CRs

Standard/CR	Description
TS 29.272 CR0792	The MME supports the Maximum-UE-Availability-Time AVP across the S6a interface. This AVP applies only to the Notify Request (NOR). This IE is included when notifying the HSS that the UE is reachable for the SMS. When present, it indicates the timestamp (in UTC) until a UE using power saving mechanism is expected to be reachable for SM delivery. This information is used by the SMS center to prioritize the retransmission of short message to UEs using a power saving mechanism.
TS 29.272 CR0802	This CR introduces the Ethernet PDN type. A new AVP in the APN-Configuration AVP is introduced to indicate whether the APN has an Ethernet PDN type. If the MME does not indicate the support of this feature in the ULR command, the HSS does not send APN configurations with an Ethernet PDN type in the subscription data sent in the ULA or IDR and does not send IDR commands with the only purpose to update the subscription data. If the MME indicates in the IDA command that it does not support this feature, and the HSS has already sent Ethernet PDN Type APNs within the IDR, the HSS stores this indication, and does not send any further updates related to the Ethernet PDN Type APNs to the MME.
TS 29.272 CR0808	This CR introduces clarification to the applicability of the Core-Network-Restrictions AVP. If the MME receives from the HSS an Update Location Response message containing in the subscription data the Core-Network-Restrictions AVP with the bit "5GC not allowed" set, the MME restricts the mobility towards the 5GC. If the MME receives from the HSS the Insert Subscriber Data Request message containing in the subscription data the Core-Network-Restrictions AVP with the bit "5GC not allowed" set, the MME restricts the mobility towards the 5GC.

Standard/CR	Description
TS 29.272 CR0809	<p>This CR introduces the subscribed ARPI parameter which the HSS sends to the MME in the Subscription-Data AVP. The MME receives the subscribed RFSP index and the subscribed ARPI from the HSS, for example, during the attach procedure, in the Subscription-Data AVP.</p>
TS 29.274 CR1946	<p>This CR specifies the PDN type Ethernet. The PDN type IE is included in the Create Session Request/Response message, Forward Relocation Request message, and Context Response message. Additionally, the PDN Address Allocation (PAA) IE in the Create Session Request/Response message has corresponding Ethernet PDN type. The MME supports the Ethernet PDN type bit in Node Features IE and SGNI Ethernet PDN Support bit in the CloT Optimizations Support Indication IE.</p> <p>If the target MME does not support the Ethernet PDN connections, or the target is an SGSN, the source MME does not include any Ethernet PDN connection in the Forward Relocation Request message or Context Response message.</p> <div style="background-color: #f0f8ff; padding: 10px;"> <p> Note:</p> <p>The MME sends the LI event reports with different UE IP address populated in it. The LI event reports need to support the new Ethernet PDN type.</p> </div>
TS 29.274 CR1962	<p>This CR introduces a new parameter called additional RRM policy index (ARPI) to support the radio resource management in the E-UTRAN. The MME stores the subscribed ARPI values received from the HSS and the ARPI values in use.</p> <p>During the inter-MME mobility procedures, the source MME forwards the ARPI values to the target MME.</p> <p>Additionally, this CR also adds the Subscribed ARPI and ARPI in use IE in the Forward Relocation Request and Context Response messages. Subscribed ARPI is included in Forward Relocation Request and Context Response messages by the MME over the S10 interface if received from the HSS.</p>

Standard/CR	Description
TS 36.413 CR1669	<p>This CR introduces Additional RRM Policy Index IE in the initial context setup procedure, UE Context Modification Request, Handover Request, Path Switch Request Acknowledge, and Downlink NAS Transport messages which is sent by the MME to the eNB.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> i Note: Additional RRM Policy Index IE is used to provide additional information independently from the subscriber profile ID for RAT/frequency priority as specified in TS 36.300. </div>
TS 36.413 CR1670	<p>This CR introduces inclusion of S-TMSI in Error Indication message that is sent by both the MME and the eNB, and is used to indicate that some error has been detected in the node.</p>
TS 36.413 CR1691	<p>The PDN type Ethernet is supported in the Initial Context Setup Request, E-RAB Setup Request and Handover Request messages which are supported by the MME in order to enable the eNB to perform appropriate header compression.</p>
TS 24.301 CR3173	<p>This CR allows the UE to get PDN connectivity for the Ethernet, the UE sets the PDN type IE in the PDN Connectivity Request message to the Ethernet. Additionally, this CR also supports extended protocol configuration options IE for the Ethernet PDN type UEs.</p>
TS 24.301 CR3254	<p>This CR introduces cause code #61 PDN type Ethernet only allowed. This ESM cause is used by the network to indicate that only the PDN type Ethernet is allowed for the requested PDN connectivity.</p>

2.8 MME support for 3GPP standard update release 16 for March/June/Sept/Dec 2020 and March 2021 - phase 2 (Feature f10002-09)

This feature introduces critical CRs from 3GPP release 16 March (v16.2.0) June (v16.3.0), September (v16.4.0), December (v16.5.0) 2020 and March (v16.6.0) 2021.

Table 8: Supported 3GPP release 16 March/June/Sept/Dec 2020 and March 2021 CRs

Standard/CR	Description
TS 36.413 v16.1.0	
CR1774	<p>When the target MME receives the Forward Relocation Request message from the source AMF, the target MME derives the EPS NAS keys, for example, the KNASenc and KNASint, from the received KASME key with the received EPS NAS security algorithm identifiers as input, to be used in the EPC as described in TS 33.401. The target MME needs to include the {NH, NCC=2} pair and the UE security capabilities in the S1 Handover Request message to the target LTE eNB.</p>
TS 29.272 v16.3.0	
CR0822	<p>Upon receiving one or more Monitoring-Event-Configuration AVP(s) in the ULA, the MME starts the detection of the monitoring events indicated in the AVP(s). If there is a failure when starting the detection, for example, maximum resources exceeded, the MME does not store the failed configuration and sends a notification of those events whose configuration have failed. If the Subscription-Data AVP is received in the ULA but it does not contain any Monitoring-Event-Configuration AVP(s), the MME stops the detection and deletes all stored monitoring event configurations.</p> <p>This feature is activated with global parameter <code>monitoringEventsDeletionByUla</code>.</p>
TS 29.274 v16.5.0	
CR1999	<p>This CR introduces correction to note 4 in the Context Response message. If an MME needs to store the last used 5GS or EPS PLMN ID, the MME derives the last 5GS PLMN ID, from the old GUTI received in the TAU Request message.</p>
TS 23.401 v16.5.0	
CR3581	<p>This CR clarifies how the MME handles the situation when receiving the secondary RAT data reporting later than Path Switch Request.</p> <p>In case of X2-based handover, the MME is expected to handle a secondary RAT data reporting from the source eNB after Path Switch Request by forwarding it to the S-GW in a Change Notification Request (secondary RAT usage data) message. The MME stores the secondary RAT usage data, for example, by maintaining the source eNB context for a certain time, and forwards it to the S-GW in the next signalling message or by using the GW secondary RAT usage data reporting procedure. This applies to the previous release as well.</p>
TS 29.272 v15.4.0	

Standard/CR	Description
CR0768	<p>When receiving a Monitoring-Event-Configuration in the ULA, the MME starts the detection of the monitoring events indicated in that AVP. If the event is not started, the MME stops the detection and deletes the previous monitoring events which are not indicated in that AVP. If Monitoring-Event-Configuration is not received, the MME stops the detection and deletes all monitoring events.</p> <p>This feature is activated with global parameter <code>monitoringEventsDeletionByUla</code>.</p>
TS 24.301 v16.5.0	<p>CR3357</p> <p>This CR changes the MME handling of operator-determined barring from the NB-IoT UEs. After the HSS indicates in the subscriber profile that the ODB is active for the NB UE, the MME rejects the next UE access (attach, TAU, service request) with cause #22 and includes a provisionable backoff timer.</p> <p>To implement this CR, new parameter <code>nbIotBarAllPacketOdb</code> in <code>restNasMappingProfile</code> command that defines the cause to use for the NB ODB is added. The default is the same as it is for <code>lteBarAllPacketOdb</code> parameter to allow for backward compatibility. DEFT rules ensures that the <code>nbIotBarAllPacketOdb</code> parameter is set to the same value as the <code>lteBarAllPacketOdb</code> parameter.</p> <p>In addition, timers <code>t3346NbIotOdbRejectMaximum</code> and <code>t3346NbIotOdbRejectMinimum</code> that specify the random backoff value range are added. The backoff timer is used if the <code>nbIotBarAllPacketOdb</code> cause in the <code>restNasMappingProfile</code> is set to 22 per congestion.</p> <p>This feature is activated with the global parameter <code>monitoringEventsDeletionByUla</code>.</p> <p>To change the default cause code:</p> <pre>cmm restNasMappingProfile modify --name default --nbIotBarAllPacketOdb 12</pre> <p>To change the backoff timers values:</p> <pre>cmm timer modify --timerName t3346NbIotOdbRejectMaximum --timerValue 900 cmm timer modify --timerName t3346NbIotOdbRejectMinimum --timerValue 600</pre>

3. Mobility management

The EPS mobility management (EMM) procedures keep track of the current location of a user equipment (UE) as it moves around a network, support paging and handovers, and ensure communication is maintained.

3.1 Attach

Features enabling the subscriber to connect to the network.

3.1.1 Attach (Feature m10001-01)

With the attach procedure, a subscriber connects to an LTE network through an eNB and establishes connectivity. The user is connected to the LTE network and is able to use the services.

In the attach procedure the UE identifies itself using international mobile subscriber identity (IMSI) or previously allocated globally unique temporary identity (GUTI). The following events occur during the attach procedure:

- The MME authenticates the user if needed. (Authentication can be skipped if security context exists.)
- The MME selects and delivers security algorithms for an integrity protection and ciphering for both non-access stratum (NAS) signaling security and radio security. Secure exchange of NAS messages between the UE and the MME is established.
- The MME fetches subscriber data from the HSS if needed. (Subscriber data can already exist because of a previous attach in the same MME.)
- The MME selects an S-GW and a P-GW for the UE and establishes connectivity to a default access point name (APN) configuration or a UE-indicated APN for data transport.

After a successful attach to the network, the subscriber can start using different services and can be reached by network-initiated service requests.

3.1.2 Initial Attach Indication setting in ULR (Feature m11327-01)

The ***Initial Attach Indication setting in ULR*** feature enables operators to control when subscription data is retrieved from the HSS during an initial attach with globally unique temporary identity (GUTI).

This feature introduces a global parameter `initialAttachIndicationInUlR` to control the setting of the Initial Attach Indication (IAI) attribute-value pair (AVP) in S6a Update Location Request (ULR) in the case of a GUTI attach. If the global parameter is set to `Yes`, the MME sets the IAI to 1 in the ULR for any GUTI attaches. If the global parameter is set to `No`, the MME sets the IAI flag for various GUTI attach scenarios as follows:

- IAI = 1 for international mobile subscriber identity (IMSI) attach
- IAI = 0 for local GUTI attach with the context existing on the MME
- IAI = 1 for local GUTI attach without the UE context on the MME
- IAI = 0 for GUTI attach (foreign GUTI), if the MME received the UE context from the old MME or SGSN.
- IAI = 1 for GUTI attach (foreign GUTI), if the MME failed to get the UE context from the old MME or SGSN, the MME asks the UE to provide the IMSI.

For all other scenarios involving ULR, IAI is set to 0, no matter what the global parameter setting is. By default, this global parameter is set to `Yes`.

3.1.3 8K UE radio capability information (Feature m10907-02)

The ***8K UE radio capability information*** feature increases the size of the UE capabilities information to 8K. The MME stores the UE capability information received from the eNB either in the visitor location register or memory pool location depending on its size and sends it to the eNB on a subsequent Initial UE Context Setup and Handover Request messages.

The MME can operate with the latest and future UEs requiring storage space for large amounts of reported radio capabilities.

The MME began supporting the UE radio capability size of 510 octets with an earlier MME release:

- There are new UEs that can support operation on many bands, leading to large values of the UE Radio Capability IE.
- When the UE Radio Capability information is large and when the UE History Information IE

is large, the maximum size of the Source to Target Transparent Container supported by the MME can be exceeded.

- If this occurs, the S1 handover event in which the Source to Target Transparent Container is too large fails.
- The UE stays in the connected state but does not move to the new eNB. Such a condition results in repeated S1 handover failures followed by an abnormal eRAB drop.

With this feature, the MME can store the UE Radio Capability information size of 8192 octets. Note that all UEs might not have the same size of UE Radio Capability information. The size distribution is not known at this point.

The MME can send an UE Radio Capability IE in the following S1-AP messages:

- Initial Context Setup Request
- UE Radio Capability Request

The eNB sends the UE Radio Capability information in the UE Capability Info Indication message.

See *3GPP TS 23.401 sections 5.11 and 5.3.14* for the message flows between the MME and eNB to exchange the UE Radio Capability IE.

The UE Radio Capability information is exchanged using a Source to Target Transparent Container in the case of intra radio access technology (intra-RAT) and inter radio access technology (IRAT) handovers.

The S1-AP messages that have the transparent container are

- Handover Required (MME to target eNB)
- Handover Request (source eNB to MME)

In the MME relocation, the Source to Target Transparent Container is included in the S10 Forward Relocation Request message (E-UTRAN Transparent Container information element (IE)).

In the IRAT handover, the Source to Target Transparent Container is included in the S3 Forward Relocation Request message (E-UTRAN Transparent Container IE by the SGSN or UTRAN/BSS Transparent Container by the MME).

For the message flow, see *3GPP TS 29.274 Annex B2*.

All these message flows are already supported. This feature adds capacity to ensure that all these messages handle the UE Radio Capability IE of 8K octets.

3.1.4 Treating non-emergency PDN connection as a new PDN connection at attach (Feature f10164-01)

The MME supports treating non-emergency PDN connection as a new PDN connection at attach.

By default, the feature is disabled.

When the feature is enabled, the MME treats a PDN Connectivity Request message received in the Attach Request message as a request for a new PDC connection, even if the request type IE in the PDN Connectivity Request message is set to handover.

The feature does not change the behavior of PDN Connectivity Request for emergency (Request type IE set to Emergency).

3.1.5 Restricting the number of attached UEs per TA (Feature f10168-01)

This feature restricts the number of roamer UE attach requests and TAU requests per TA in the serving PLMN.

The restriction is applied at two levels:

- Per roaming UE PLMN and serving PLMN if the total number of registered users per UE PLMN and serving PLMN exceed the provisioned allowed number. Once the total number of registered roaming UEs from all the TAs exceeds the provisioned maximum value per UE PLMN, the MME rejects the Attach and TAU Requests irrespective of per TAC provisioning.
- Per TAC in the serving PLMN for the UE PLMN if the number of registered users in the current TAC exceeds a provisioned number of allowed users per TAC and UE PLMN. Once the total number of users exceeds the provisioned registered UE in the TAC, the MME rejects the UE Attach and TAU Requests.

If MME rejects an Attach or TAU Request due to these restrictions, the MME uses cause code #22 and includes currently supported back-off timer T3346.

If the Attach Requests or TAU Requests for roamer UEs are rejected with cause code # 22, check the PM counters on the MME to see whether the rejections are performed due to TA restriction feature.

Additionally, the MME provides command `taCountQuery` to view the number of attached

users for a UE PLMN and one or all TACs in the serving PLMN. This can be compared with the commands `maxUeAllowedperTac` and `maxUeAllowed` on the MME for UE PLMN and for TAC in the serving PLMN.

3.1.6 Always send EPS Network Support Feature Support IE in Attach and TAU Accept messages (Feature f10173-01)

This feature allows operators to control whether the MME always sends EPS Network Feature Support IE to the UE during in the Attach Accept and TAU Accept message.

The EPS Network Feature Support IE is only required to be included in Attach Accept and TAU Accept messages when the MME has bits to set in that IE. This feature provides conditional control to always include the EPS Network Feature Support IE in Attach Accept and TAU Accept messages regardless whether there are bits to be set in that IE or not.

UEs are supposed to act as if all bits are zero if this IE is not included in those messages, but it has been found that some UEs do not behave properly when this IE is not present (with all zeroes).

Global parameter `alwaysSndEpsNwFeatSuppt` is used to enable and disable this feature.

3.1.7 MME support for optional IE for T3402 (Feature f10926-01)

This feature allows the MME to provide the UE that is being rejected with a T3402 value, which reduces the rate of attaches for UE being rejected but does not alter the behavior for UEs that are successfully attached.

This feature adds the optional IE for T3402 (which controls the wait time for another Attach Request message if the UE's attach counter has reached 5) to the Attach Reject message. In addition to adding this IE, a new DB timer is created so that the T3402 timer which is set to be used in the Attach Reject message is different from the one used in the Attach Accept message.

3.1.8 Multi SIMs with same MSISDN (Feature f10411-01)

This feature supports multiple subscriber identification modules (SIMs) with the same MSISDN. This feature enables users to have a maximum of five IMSIs sharing a common

MSISDN.

The MME always supports and allows more than one IMSI to attach to the MME by using the same MSISDN. The IMSIs are different for different SIMs.

This feature supports up to five UEs to share the same MSISDN. These changes affect lawful intercept, call trace, and UE load balance as follows:

- LI targets are selected based on multiple UE entries that are using the same MSISDN. In addition, all the UE entries are treated as LI targets, if the MSISDN is in the LI target list.
- The MME performs call traces on all UEs that the CT job is keyed by the MSISDN and there are multiple UEs/IMSIMs mapped to the MSISDN.
- During UE load balance, if there are multiple UEs with the same MSISDN, all of them are offloaded.

When the feature is enabled by setting the global parameter `multiSimSupport` to `Yes`, the MME drops an mobile-terminated location request (MT-LR) if it only contains an MSISDN for the location query. When the parameter is set to `No` (default), the MME allows an MT-LR that contains only an MSISDN as the identifier.

3.1.9 Scaling the maximum IMSI range services to 10K (Feature f14619-01)

This feature increases the number of IMSI range service records that can be provisioned to 10 240.

If the global parameter `allowExtendedImsiRangeServices` is set to `Yes`, the system allows 10 240 records of `imsiRangeServices` to be provisioned. If the `allowExtendedImsiRangeServices` parameter is set to `No`, the limit remains 4096 records.

3.2 Authentication and security

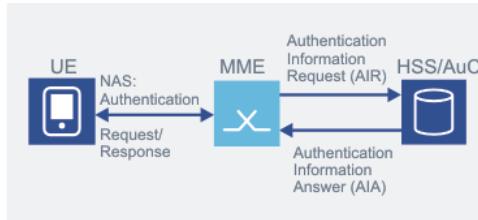
These features provide the operator and user with the necessary and basic functionality for ensuring a secure network environment.

3.2.1 Authentication (Feature m10001-01)

The authentication procedure corroborates the identity of the subscriber. It also corroborates that a user is connected to a serving network that is authorized by the user's home environment to provide services. This includes a guarantee that this authorization is recent.

The UE is authenticated using the evolved packet system (EPS) authentication and key agreement (AKA) procedure, as shown in the figure.

Figure 1: EPS authentication procedure



The MME does the EPS authentication by sending an Authentication Information Request (AIR) message to the HSS. The HSS replies with the Authentication Information Answer (AIA).

The MME sends the Non-Access Stratum (NAS) Authentication Request message to the UE. The UE returns a NAS Authentication Response message to the MME. The MME considers the AKA exchange to be successfully completed if it can verify the return message from the UE.

The UE and MME further derive the keys: eNB key, NAS signaling integrity protection key, and NAS signaling ciphering key. The MME delivers the eNB key (KeNB) to the eNB for user plane and radio resource control (RRC) protection.

3.2.2 Air interface security support

The Air interface security support feature enables the ciphering and integrity protection of signaling and data over the air interface. It provides secured transmission over a radio path.

The MME provides the eNB with an eNB key that is used for user and control plane security over the air interface.

3.2.3 NAS signaling protection (Feature m10607-01)

In the E-UTRAN, NAS signaling traffic between the UE and MME must always be integrity-

protected and optionally ciphered.

The MME supports advanced encryption standard (AES), SNOW 3G, or ZUC ciphering and integrity protection algorithms. The MME also supports Null ciphering and integrity protection. Null integrity protection is only for the LTE trial phase testing.

The MME uses an operator-configured security algorithm for the UEs supporting the specific algorithm. If a (non-standard) UE supports one specific algorithm only, the MME selects the algorithm that the UE supports.

3.2.4 AES ciphering and integrity protection (Feature m10607-02)

Ciphering prevents externals from seeing the content of the messages between the UE and MME. The integrity protection prevents the manipulation of transferred data.

The MME instructs the UE to use advanced encryption standard (AES) ciphering and integrity protection using non-access stratum (NAS) security mode command (SMC), as shown in the figure.

Figure 2: Signaling traffic protection command



With AES ciphering, the exchanging entities (UE or MME) can ensure that others are not able to read the content of the message.

With AES integrity protection, the receiving entity (UE or MME) is able to verify that the signaling data has not been modified, as it was sent by the proper sending entity (UE or MME) and the origin of the received signaling data is indeed the one claimed.

3.2.5 Null ciphering and integrity protection (Feature m10607-02)

If the UE does not support ciphering or its usage is not allowed, it is possible to use the Null ciphering algorithm. The signaling data is not ciphered between the UE and MME.

The LTE system trial initiative (LSTI) defines the use of null integrity handling in the LTE

system trial and possibly in the early phase of the LTE as well. This is because not all terminals can support advanced encryption standard (AES) or SNOW 3G as the recommended method in the LTE trial phase. To be able to do the end-to-end testing between the MME and UE, the MME supports null integrity handling. This means that the MME instructs a UE to use non-integrity protection over the non-access stratum (NAS) link. 3GPP does not allow null integrity handling but it is needed as a temporary solution in the LTE trial phase.

It is possible to run LTE trials without actual ciphering and integrity protection with early phase terminals.

3.2.6 SNOW 3G ciphering and integrity protection (Feature m10607-02)

SNOW 3G is an alternative security algorithm for the LTE security in addition to the advanced encryption standard (AES).

In the E-UTRAN, the non-access stratum (NAS) signaling traffic between the UE and the MME is always integrity-protected and optionally ciphered. The MME instructs the UE to use the selected security algorithm using a NAS security mode command (SMC).

Figure 3: Security - ciphering and integrity protection - SNOW 3G



AES and SNOW 3G provide similar levels of security. Supporting both algorithms in the system provides protection if either algorithm is attacked. The NAS integrity and ciphering keys are generated during evolved packet system (EPS) authentication and key agreement (AKA).

Supporting the second algorithm also ensures network availability if there is a security algorithm attack.

To be able to use the *SNOW 3G ciphering and integrity protection* feature, EPS AKA must be supported.

3.2.7 ZUC ciphering and integrity protection (Feature m10612-01)

Certain markets, for example, China, require a specific ciphering and integrity algorithm.

The MME supports the ZUC algorithm in addition to advanced encryption standard (AES), SNOW 3G, and Null.

Figure 4: Security - ciphering and integrity protection - ZUC



The non-access stratum (NAS) integrity and ciphering keys are generated during evolved packet system (EPS) authentication and key agreement (AKA) procedure (for more information, see [Authentication](#)). The MME instructs the UE to use either ZUC or another security algorithm using NAS security mode command (SMC).

To be able to use the *ZUC ciphering and integrity protection* feature, EPS AKA must be supported.

3.2.8 Disabling Immediate Response Preferred AVP on S6a (Feature m11317-01)

The *Disabling Immediate Response Preferred AVP on S6a* feature provides an option for the HSS to either immediately respond with even lower number of requested authentication vectors to expedite the UE authentication when the feature is not disabled or delay the response until the HSS can provide the requested number of authentication vectors when the feature is disabled.

This feature provides support for disabling the Immediate-Response-Preferred attribute-value pair (AVP) across the S6a interface whereby this optional AVP is not sent by the MME to the HSS.

Immediate-Response-Preferred optional AVP indicates by its presence that immediate response is preferred, and by its absence that immediate response is not preferred.

- When EUTRAN-AVs and UTRAN-AVs or GERAN-AVs are requested, the presence of this AVP within the Requested-EUTRAN-Authentication-Info AVP indicates that EUTRAN-AVs are requested for immediate use in the MME/SGSN.

- Presence of this AVP within the Requested-UTRAN-GERAN-Authentication-Info AVP indicates that UTRAN-AVs or GERAN-AVs are requested for immediate use in the MME/SGSN.
- It can be used by the HSS to determine the number of vectors to be obtained from the authentication center (AuC) and the number of vectors downloaded to the MME or SGSN.

The above applies according to the CMM implementation, for example, GERAN-AVs request does not apply to an MME-only node.

Currently the MME populates Immediate-Response-Preferred AVP with value 1 when AV is needed for current procedure. If the current procedure does not need AV, the MME sends AIR message without this AVP.

The provisioned number of authentication vectors and immediate response preferred are used for both the MME and SGSN. The MME always requests the HSS for the exact number of provisioned authentication vectors. The default (and recommended) number of authentication vectors that the MME requests in the AIR message to the HSS is 1.

The MME can be provisioned with immediate response preferred. Following are possible values of the `immRspPref` parameter (command `localEndPtCfg`):

- Yes – always populates Immediate-Response-Preferred AVP
- No – never populates Immediate-Response-Preferred AVP. This is the default.
- Dynamic – the MME populates Immediate-Response-Preferred AVP when authentication vector is needed for current procedure and synchronization failure.

3.2.9 Configuration of authentication frequency for IRAT TAU procedure (Feature m30106-01)

With the *Configuration of authentication frequency for IRAT TAU procedure* feature, operators can choose to balance between additional UE security and signaling load.

With this feature, the MME supports an ability to provision the percentage of cases in which authentication is invoked for tracking area update (TAU) requests. This feature enhances this provisioning to provide separate provisioning of the percentage separately for LTE TAU request and inter radio access technology (IRAT) TAU procedures.

- The default value for both LTE TAU and IRAT TAU authentication reallocation is set to 10%.
- The term LTE TAU request is used to indicate that the UE's old node was an MME and the term IRAT TAU request is used to indicate that the UE moved from the UTRAN/GERAN to E-UTRAN and the old node of the UE was an SGSN.

- The new MME determines whether the UE is moving from another MME or SGSN by determining whether the UE's globally unique temporary identity (GUTI) is a native GUTI or a mapped GUTI.
 - A native GUTI indicates that the old node was an MME and the UE mobility is an intra-LTE.
 - A mapped GUTI indicates that the old node was an SGSN and the UE might be moving from the UTRAN/GERAN to E-UTRAN. There are two ways the MME can determine whether the UE's GUTI is a native GUTI or a mapped GUTI.
 - Indication using the most significant bit (MSB) in the location area code (LAC) and the MME Group ID of GUTI and by using feature LAC values greater than 32 767.
 - Implicit indication from UE.

This feature does not support a separate provisioning for GUTI reallocation for IRAT TAU as the GUTI reallocation is always required by standards on MME relocations (that is, the MME relocation can be MME to MME or SGSN to MME).

Operators have to change the default setting if they must increase or decrease UE authentication frequency.

Related descriptions

- [Configurable repetition rates for authentication \(Feature f10404-01\)](#)

3.2.10 Configurable repetition rates for authentication (Feature f10404-01)

This feature supports separate provisioning of authentication percentage for inter-MME/intra-MME inter-PLMN tracking area updates.

MME uses the current mechanism to perform authentication based on the provisioning percentage. This feature introduces the value `IPLMNTAU` for the `procedureName` parameter of the `plmnSecurity` command. The range for the percentage is 0 to 100 and default percentage of inter-PLMN TAU is 100.



For intra-PLMN/inter-PLMN IRAT TAUs, the existing provisioning percentage `IRATTAUpdate` should be used.

Related descriptions

- [Configuration of authentication frequency for IRAT TAU procedure \(Feature m30106-01\)](#)

3.2.11 MME support for authentication frequency per IMSI range (Feature f10423-01)

This feature allows a range of IMSIs to use a different PLMN security profile for authentication frequency instead of the security profile configured for the serving PLMN. This is useful for mobile virtual network operators (MVNO) which group IMSIs into a single range.

For MME procedures where a security procedure is optional, if the IMSI of a UE is in the range of the configured IMSI range services, the PLMN security profile linked to the IMSI range services is used for the corresponding MME procedure. For a given MME procedure, the security profile of the linked IMSI range services overrides the serving PLMN security profile for the following authentication frequency parameters: `authInteraction`, `gutiReallocation`, and `irat5gAuth`. The supported MME procedure names and definitions of these parameters are not changed by this feature.

3.2.12 MME support for GUTI reallocation upon expiration of refresh timer (Feature f10414-01)

This feature introduces a new GUTI refresh timer that allows the CMM MME to force a GUTI reallocation based on the timer's expiration.

This feature introduces a new GUTI refresh timer, with which, the CMM MME is able to force a GUTI re-allocation at the next UE involved procedures upon the expiration of the GUTI refresh timer if the timer is configured with a non-zero value. The enhanced procedures are:

- Attach
- TAU
- Service request
- Control plane service request

3.3 HSS interaction

Features enabling subscriber data and authentication parameters management through the HSS.

3.3.1 HSS interworking (Feature m10001-01)

With the *HSS interworking* feature subscriber data and authentication parameters can be managed through the HSS.

The operator can add new data to a user's subscription, modify the subscription information, or delete some of the data in the HSS repository. The HSS updates new subscriber data to the MME using initiating insert subscriber data or delete subscriber data procedures. The HSS can also detach a subscriber through the HSS database with a cancel location procedure as a consequence of subscription data withdrawal or mobility to a new MME. If the UE data is removed from the MME, the MME uses a purge procedure to the HSS to remove the MME registration.

HSS data can also include a static IP address for the UE per access point name (APN) configuration profile. This means that the MME provides this static address to the P-GW through the S-GW and no dynamic address is allocated for the packet data network (PDN) connection.

On an HSS reset, the MME restores the registration of the affected UEs with an additional update location procedure to the reset HSS during the next attach, tracking area update (TAU), or service request procedure.

The HSS selection with the international mobile subscriber identity (IMSI) analysis is enhanced with the longest digit match support. This means that if there are several analyses starting with the same digit sequence, the system compares the analyses to find the best matching analysis for a specified number.

3.3.1.1 HSS user profile management

The MME application accesses the HSS (directly or via DRA) during various procedures to obtain or update subscriber information.

For example, MME accesses the HSS at

- user registration: the HSS is queried by the MME application as the user attempts to register to the network to check the user subscription rights.
- location update: as the UE changes location areas, the HSS is kept updated, and maintains a reference of the last known area.

The table shows the procedures.

Table 9: HSS user profile management procedures

Procedure	Purpose
Authentication	HSS authenticates UE upon request of the MME application.
Update location	The MME application informs HSS about identity of MME serving the user; the MME application provides HSS with user data; HSS may optionally update MME with subscriber data.
UE reachability notification request	If the HSS has received UE reachability status, the HSS sends a UE-REACHABILITY-NOTIFICATION-REQUEST (URRP-MME) to the MME. The MME then reports to the HSS information regarding changes in UE reachability (for example, when the next NAS activity with that UE is detected).
UE activity notification	The MME application informs HSS of a UE-Activity-Notification if URRP-MME for that UE is configured to report once that the UE is reachable.
Notification	The MME application notifies HSS if P-GW for an APN has been removed or changed.
Insert subscriber data	HSS updates the MME application when UE data record has changed.
Purge	The MME application requests to delete a subscriber record from HSS.
Reset	The MME application restores impacted subscriber records to HSS.
Delete subscriber data	HSS notifies the MME application when UE data has been removed.
Cancel location	HSS notifies the MME application when a UE withdraws a subscription.

User profiles are partitioned in memory on the MME application in a UE context data structure, which supports tables for:

- Static data retrieved from the HSS during the Attach procedure (includes authentication, subscription, and APN data).
- Dynamic state information related to the UE and the current UE context (includes UE session and bearer data).

Context information is UE data, such as identity, connection state, location, and routing

information, obtained from various sources (such as the UE and the HSS). For 3GPP-supported context information fields and their descriptions, see *3GPP TS23.401*. The UE context data structure has one tuple per UE, and includes all static data retrieved from the HSS (S6a) interface at attach, as well as all subsequent dynamic state information related to that UE and the current UE context.

The UE context data is a distributed data structure. The UE context data record retrieved from the HSS is populated during the attach procedure. The MME keeps the UE subscriber data, unless purged or the user roams out of the MME.

3.3.2 Active-APN AVP as mandatory (Feature m11329-01)

The Active-APN AVP as a mandatory feature enables operators, during the HSS migration, to inform the new HSS of all UEs' active access point names (APNs) when the UEs' subscription is migrated to the new HSS and the MME has received a S6a Reset Request (RSR).

This feature supports the capability to always include an Active-APN attribute-value pair (AVP) in the S6a Update Location Request (ULR) command that is sent to an HSS in response to an S6a Reset Request (RSR) command from that HSS.

The AVP is optional in 3GPP standards except when the MME previously has sent a Notify Request (NOR) command to update the HSS with the identity of the P-GW selected for the APN.

With this feature enabled, the MME includes an Active-APN AVP for each active APN regardless of whether a PGW-assignment NOR was previously sent or not.

The MME includes Active-APN AVP in Update Location Request message unconditionally after receiving S6a Reset Request (RSR) message from the HSS if the MME previously has sent PGWassignment NOR for the active APN.

3GPP standard has specified Active-APN AVP as optional, however, with this feature enabled, the MME always includes this AVP in the ULR.

This feature is provided to streamline the transition between two vendor's HSS nodes.

- The MME includes only Active-APN AVP in the ULR after RSR/A.
- The MME does not include Active-APN AVP in all ULRs. In other words, the function still has one condition: after Reset Request/Answer. The value Yes can be used during the transition from vendor 1 HSS to vendor 2 HSS. After the transition, the value should be No.

The Active-APN AVP as *mandatory* feature must be enabled by the customer support team.

3.3.3 NOR modification (Feature m11334-01)

The *NOR modification* feature eliminates the need to include the PDN gateway public land mobile network identity attribute-value pair (PGW PLMN ID AVP) in Notify Request (NOR) when P-GW fully qualified domain name (FQDN), which includes the PLMN ID, is present in the NOR.

This feature incorporates support for the exclusion of PGW PLMN ID AVP when the P-GW FDQN is present in the NOR message. PGW PLMN ID IE identifies the PLMN in which the P-GW is located. The global parameter controls whether to exclude the PGW PLMN ID AVP when the P-GW FDQN is present in the NOR message.

By default, this capability is disabled, that is, the PGW PLMN ID is always included.

3.3.4 IMEISV update to HSS through NOR (Feature m10001-01)

With the *IMEISV update to HSS through NOR* feature the automatic device detection is fully supported and the HSS always has an up-to-date international mobile equipment identity and software version number (IMEISV) available for different use cases.

The IMEISV is provided to the HSS using an Update Location Request message. The IMEISV update to HSS through Notify Request (NOR) ensures that the international mobile equipment identity (IMEI) is also updated if the user changes a device and re-registers in the same MME.

The *IMEI sending to HSS* feature must be enabled for the *IMEISV update to HSS through NOR* feature to work.

3.3.5 Configurable Destination Realm for IMSI series (Feature m11311-01)

The *Configurable Destination Realm for IMSI series* feature enables operators to define Destination Realm and Destination Host per international mobile subscriber identity (IMSI) series instead of at a public land mobile network (PLMN) level.

This feature supports configuration of the Destination Realm to be used for IMSI series. This

IMSI series provisioning is supported for the MME home PLMN, shared PLMN and roaming partners.

Before the implementation of this feature, the Destination Realm is provisioned in the remote endpoint table. This feature introduces incorporating the Destination Realm to an IMSI range table. This feature applies to S6a, SLg, and S13 interfaces.

This feature supports an additional Destination Host and Destination Realm specification in the IMSI series for S6a Diameter.

- An IMSI range rule can specify a HSS or DRA group as destination for call processing routing of S6a Diameter messages from the MME.
- In addition, one Destination Host and one Destination Realm is provided per rule.
- For all the supported Diameter interfaces, the remote endpoint specification replaces the existing Destination Realm string with one Destination Host reference and one Destination Realm reference.
- With the implementation of this feature, specifically for S6a logical interface, the MME considers the Destination Realm in the IMSI range table if it exists. The Destination Realm in the IMSI range table has a higher priority than the remote endpoint. In other words, the IMSI to HSS entry always takes precedence over the remote endpoint provisioning.
- The Destination Realm in the IMSI range table is used only when the routing address (DRA) Supported in the remote endpoint table is True.
- If the DRA Supported in the remote endpoint table is False, the Destination Host/Realm is taken from the Origin Host/Realm from the CEA.
 - However, if the DRA Supported in the remote endpoint table is True and if the visitor location register (VLR) exists and has received the Origin Host/Realm from a previous successful AIA/ULA/NOA, the MME populates the Destination Host/Realm with the values stored in the VLR.
 - Otherwise, if the VLR does not exist or the VLR exists but does not have the Destination Host/Realm, the MME does not populate the Destination Host attribute-value pair (AVP), except when the MME receives the Peer-I (DRA selected Diameter Peer) response received via the DRA.
- The MME allows variables such as ueMcc, ueMnc, netMcc, netMnc, in the provisioned Destination Realm, for example, `mcc{ueMcc}.mnc{ueMnc}.com`. Currently the provisioned Destination Realm is a string constant, for example, `custxims.com`.
 - “ue*” means UE home PLMN.
 - “net*” means serving PLMN.
 - At runtime, “`mcc{ueMcc}.mnc{ueMnc}.com`” becomes “`mcc310.mnc012.com`”.
- If the DRA roaming supported global parameter is set to value Yes and Roamer, the MME populates the Destination Realm with hard-coded `epc.mnc##.mcc##.3gppnetwork.org`. However, if the DRA roaming supported

global parameter is set to value No or Homer, and if the IMSI range does not exist or the Destination Realm in the IMSI range table is empty and if the Destination Realm in the remote endpoint table is empty, the Destination Realm is populated with `epc.mnc###.mcc###.3gppnetwork.org`.

- If the Destination Realm in the remote endpoint table is not empty, the Destination Realm is populated with the Destination Realm in the remote endpoint table. However, if the IMSI range exists and the Destination Realm in IMSI range table is not empty, the Destination Realm is set to the Destination Realm in IMSI range table.
- Per S6a routing rule, a new optional DRA Destination Host and DRA Destination Realm are provisioned in the format of a fully qualified domain name (FQDN) string with the UE variables: {ueMnc} {ueMcc} {netMcc} {netMnc}.
- Per S6a interface (also applies to S13 and SLg) remote endpoint, a new DRA Destination Host can be provisioned and the existing DRA Destination Realm (and new DestHost) are extended to support four UE variables. If none are provisioned, the DRA Destination Home is not included and the DRA Destination Realm uses the default according to 3GPP TS 29.272:`epc.mnc{ueMnc}.mcc{ueMcc}.3gppnetwork.org`
- In order of the priority for S6a the following are sent to the DRA in the first time UE S6a request:
 - 1st applicable S6a IMSI series rule
 - 2nd S6a remote endpoint
 - 3rd default values of Host and Realm
- For S13 and SLg, order of priority is:
 - 1st remote endpoint
 - 2nd default values of the Host and Realm are sent to the DRA in first time UE (S13 or SLg) request.
- The MME learns specific routes to Host and Realm from the Peer-I (DRA selected Diameter Peer) response received through DRA.
- Per S6a routing rule provisioned or per remote endpoint (S6a, S13 or SLg), the DRA Destination Host (optional) and DRA Destination Realm are sent to the DRA in first time UE S6a request to the selected DRA-n. The MME learns the specific Peer Host and Realm from the Peer response through the DRA. The MME uses the learned Host/Realm in the subsequent UE procedures.

3.3.6 Reset ID across S6a interface upon HSS restart after failure (Feature f11305-01)

Reset ID across S6a interface upon HSS reset after failure feature introduces reset ID to improve the efficiency of HSS reset after failure.

This feature allows the reset IDs to be included in the Update Location Answer (ULA), Insert Subscriber Data (IDR) and S6a Reset Request (RSR) messages.

When the HSS restarts after a failure occurs, it may detect that the failure is limited to a HSS component or other resources, which only impacts the subset dependent subscribers but not other independent subscribers.

Without this feature, operator can only reset all the subscribers of the HSS, or all the subscribers with a given IMSI range. This may result in long reset messages with thousands of User-ID AVPs.

Reset ID is introduced to identify a failed HSS hardware component or other resources, in order to identify the subscribers that need to be reset and improve the efficiency of HSS restart after failure.

3.3.7 Release 14 Inclusion of modified/deleted subscription data with the RSR (Feature f11311-01)

This feature enhances MME functionality to handle diameter Reset Request (RSR) message containing Subscription-Data or Subscription-Data-Deletion AVP.

Being able to handle this message, a bulk of Insert Subscriber Data Request or Delete Subscriber Data Request messages that would have been sent in place of this Reset Request (RSR) message are avoided and network signaling is minimized. This handling may have a small impact in CPU and memory consumption.

Upon receiving a Reset Request message containing Subscription-Data or Subscription-Data-Deletion AVP, the MME will update all impacted subscriber records accordingly. For example, each impacted subscriber record is updated as if an individual Insert Subscriber Data Request or Delete Subscriber Data Request message for that subscriber was received. The MME will not mark successfully updated subscriber records "Location Information Confirmed in HSS" as "Not Confirmed". If an impacted subscriber record cannot be updated for any reason (such as the updated data is considered not shareable by the MME or the update requires an individual acknowledgement to be sent to the HSS), the MME will mark the record "Location Information Confirmed in HSS" as "Not Confirmed".

In case the MME has the UE record in its local subscriber cache and the update of Shared Subscription Data requires local updates in the MME and/or implies initiating a signalling interaction towards other nodes (for example, towards the P-GW/PCRF for the change of an APN configuration parameter, such as APN-AMBR), the updates should be performed immediately (such as deleting an Operator Determined Barring). Also, the signalling towards other nodes should be initiated immediately. To avoid high processing/signalling load,

resulting from shared subscription data update and external signalling towards other nodes, the MME scans its local subscriber cache to find the impacted UEs in batches. An internal timer is set for this purpose to trigger the MME to scan the functionality periodically. The numbers of scanned and matched subscriber records are set as criteria to stop the MME scan until the next period when it is resumed. When all subscriber records are scanned, the MME scan procedure completes.

 **Note:**

- Scan of local subscriber cache may need minutes to complete depending on the number of reserved subscriber records and the number of matching subscriber records.
- In case the Reset Request message with Subscription-Data or Subscription-Data-Deletion AVP is received when the system is in overload or in case the system enters overload while handling this message, scan of local subscriber cache is slowed down to avoid additional CPU impact.

In case the MME does not have a subscriber record for the UE in the local subscriber cache, the updates will be deferred to the next authenticated radio contact with the UE. In addition, if the update of shared subscription data implies initiating a signalling interaction towards other nodes (such as towards the P-GW/PCRF for the change of an APN configuration parameter, such as APN-AMBR), the MME will not initiate any signalling towards other nodes. Instead, the MME will only update its local data associated with the UE.

 **Note:**

- The MME will not have a subscriber record for a UE in the event of MME signalling service's reset or if the UE has aged out.
- The matching of the affected subscribers is performed by the use of the Reset-Id AVP contained in the Reset Request message.

3.3.8 MME support for HSS reset enhancement (Feature f11345-01)

This feature introduces enhancement to the existing HSS reset functionality by sending the Update Location Request (ULR) message for the service request as part of the DDN (MT Service Request), if it happens after HSS reset.

The MME immediately updates the hssResetFlag in DBS, in case that the Reset Request message comes for only one subscriber (15-digit IMSI).

3.4 IMEI check/validation

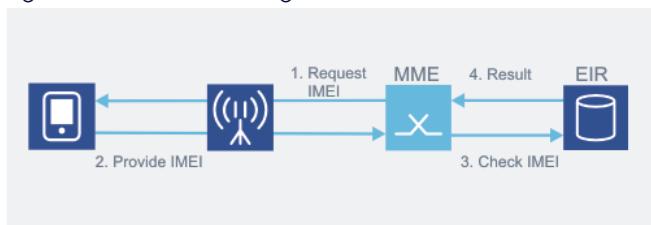
Features enabling CMM to check or validate international mobile equipment identity (IMEI) and interact with the equipment identity register (EIR).

3.4.1 IMEI checking (S13) (Feature m10205-02)

The MME supports checking international mobile equipment identity (IMEI) received from the equipment identity register (EIR).

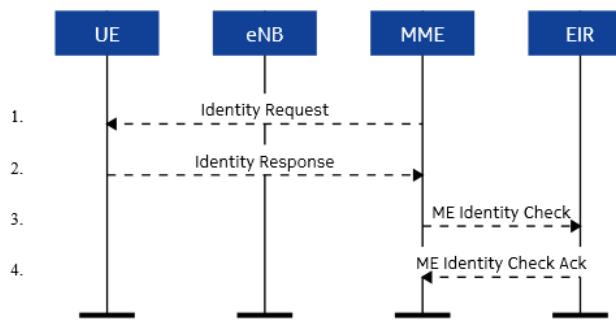
When a UE attaches to the network, the MME requests the UE to provide its IMEI either through non-access stratum (NAS) security mode command (SMC) or through the identity request procedure. The MME then checks the received IMEI against the EIR over the S13 interface.

Figure 5: IMEI checking



The mobile equipment (ME) identity check procedure permits the operator(s) of the MME, HSS, and P-GW to check the mobile equipment's identity (for example, to check that it has not been stolen, or to verify that it does not have faults). The MME checks ME identity by passing it to EIR and then analyzing the response from the EIR to determine its subsequent actions.

Figure 6: ME identity check



The S13 interface is used for the ME identity check procedure between the MME and the EIR as described in the 3GPP TS 23.401. The protocol for the S13 interface is Diameter over SCTP and Stream Control Transmission Protocol (SCTP) multi-homing is supported.

An EIR query does not occur for a roamer, or at least for a roamer that is not from the MME home public land mobile network (PLMN) or from an equivalent PLMN.

The Diameter ECR (ME-Identity-Check-Request) and ECA (ME-Identity-Check-Answer) messages are carried across S13 interface between the MME and EIR.

The MME uses the ECR (ME-Identity-Check-Request) procedure to check the ME identity, if the MME is configured to check the IMEI with the EIR. (The IMSI can be sent together with Terminal Information to the EIR for operator-determined purposes.)

The Terminal Information contains the IMEI, 3GPP2-MEID, and the SW Version for the international mobile subscriber identity (IMSI) attribute-value pairs (AVPs). If IMEI validation is enabled through provisioning, the MME validates the received IMEI to ensure that it complies with 3GPP TS 23.003. The MME rejects UEs with invalid IMEI without waiting to have the HSS trigger the rejection. The IMEI is composed as described in the table.

Table 10: IMSI

IE name	Mapping to Diameter	AVP Category	Description
Terminal Information	Terminal-Information	M	This information element contains the information about the used mobile equipment, that is, IMEI.
IMSI	User-Name	O	This information element contains the user IMSI, formatted according to <i>3GPP TS 23.003 clause 2.2</i>

When receiving an ME Identity Check Request, the EIR checks whether the mobile equipment is known. The EIR identifies the mobile equipment based on the first 14 digits of the IMEI AVP.

If it is not known, a result code of DIAMETER_ERROR_EQUIPMENT_UNKNOWN is returned.

If it is known, the EIR returns DIAMETER_SUCCESS with the equipment status. The Equipment-Status AVP can have the following values:

- ALLOWLISTED (0)
- DENYLISTED (1)
- TRACKLISTED (2)

When receiving the ME Identity Check Answer from the EIR, in the ECA (ME-Identity-Check-Answer), the MME checks the result code and the equipment status. Depending on the result, the MME decides its subsequent actions (for example, it can send an Attach Reject if the EIR indicates that the Mobile Equipment is unknown or denylisted).

S13 protocol stack - MME to EIR

Diameter protocol (as specified in *3GPP TS 29.272*) supports the UE identify check procedure between the MME and EIR. Diameter messages over the S13 interface use SCTP as the transport protocol to transfer signaling messages. S13 over Transmission Control Protocol (TCP) is not supported by the MME.

With SCTP multi-homing, the S13/S13' interface is configured with a primary IP address (IPv4 or IPv6 or both) and an alternate (secondary) IP address of the same type: IPv4 if the primary is IPv4 and IPv6 if the primary is IPv6. S13 can also be provisioned as single homed.

EIR handling of DPR/DPA messages

If the MME detects that the EIR link is being blocked (for example, by command), the MME sends a Disconnect-Peer-Request (DPR) to the EIR, and waits a duration of Diameter profile timer `dprMsgTimer` (default 6 seconds) for the EIR to respond with a DPA.

When the DPA is received or times out, the MME closes the connection and completes the link blocking the operation to this EIR.

S13 link down or no response from EIR

If the S13 link is unavailable, disabled, or out of service or if there is no response to the request initiated by the MME from the EIR, and there is an existing IMEI validation information present in the VLR, the MME processes the attach as if equipment status in the ECA results code indicates equipment is allowlisted (0).

Retries

To mitigate transient or individual EIR UE identity check failures during the ME identity check procedures - ME Identity Check Request (ECR) and ME Identity Check Answer (ECA) - a service provider can do S13 retry on an alternate link. The global parameter `s13retryDifferentEir` enables or disables S13 retry. The function is disabled by default.

When the functionality is enabled:

- Any new mobile equipment identity check procedure executed without the history of EIR would always go to the primary EIR, which is the first one provisioned in S13 diameter connection table.
- Upon ECA timeout or one the following diameter errors, a different EIR would be retried and selected if retry succeeded.
 - DIAMETER_TOO_BUSY
 - DIAMETER_OUT_OF_SPACE
 - DIAMETER_UNABLE_TO_DELIVER
- If the primary EIR becomes available, the MME goes back to the primary EIR.
- Only one retry is attempted. If the retry fails, the procedure will fail, and the primary EIR is selected for the next procedure.

When the functionality is disabled:

- Even if multiple EIRs are defined, only the first EIR available (link enabled) is selected
- If a timeout occurs or the connection goes down, no retry is attempted, resulting in

failure of the overall procedure.

Requirements

S13 enables operators to query EIR for isolated/denylisted UEs and decline these UEs service when they try to register with the network.

To be able to use the *IMEI checking (S13)* feature, EIR, which is an optional mobile network entity, must be deployed.

3.4.2 IMEI validation (Feature m11020-01)

The *IMEI validation* feature gives operators an option to either allow the UE's request to continue or to reject the request if the UE's provided international mobile equipment identity (IMEI) in the request is not compliant with the IMEI format definition in 3GPP TS 23.003.

This feature provides a validation of the IMEI received from the UE to ensure that it complies with 3GPP standards. In particular, the IMEI should be composed of all decimal digits. If this feature is enabled, the MME validates/checks the received IMEI to ensure that it complies with 3GPP TS 23.003 and rejects the UEs with invalid IMEI without waiting to have the HSS trigger the rejection. This feature covers both IMEI and international mobile equipment identity and software version number (IMEISV).

The IMEI is composed as shown in the figure:

Figure 7: IMEI



The IMEI is composed of the following elements (each element consists of decimal digits only):

- Type Allocation Code (TAC), 8 digits
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within the TAC. Its length is 6 digits.
- Check Digit (CD) Spare Digit (SD): Spare Digit it is set to zero, when transmitted by the mobile subscriber (MS). The IMEI (14 digits) is complemented by a Check Digit (CD) that is not part of the digits transmitted when the IMEI is checked. The Check Digit is used to

avoid manual transmission errors, for example, when customers register stolen MEs at the operator's customer care desk. The Check Digit is defined according to the Luhn formula, as defined in *3GPP TS 23.003 annex B*.

With the implementation of this feature, and when provisioned, the MME checks to see if the received IMEI from a UE is composed of all decimal digits, and if the received IMEI contains non-decimal digits or if it follows the 3GPP standard. If this check fails, the UE's attach request is rejected.

Upon receiving the IMEI from an old node (MME/SGSN), if the IMEI validation is enabled, the MME checks the provisioned validation options and if provisioned to validate (either validate continue, validate reject). If an invalid IMEI is received, it is not stored in the VLR, and it is treated as if the IMEI was not received from the old node.

Reject request because of an invalid IMEI(SV) is only done when the IMEI has been received directly from the UE.

If IMEI Digit Validation is provisioned and an invalid value is received from an old node, the IMEI(SV) is not stored in the VLR. The request continues to be processed.

If the MME is provisioned to validate the IMEI and the MME receives an invalid IMEI while a previous IMEI is already in the VLR, the MME does not remove the previous IMEI from the VLR.

3.4.3 Exclude the vendor specific application ID (Feature f11335-01)

By default, the MME includes the vendor specific application (VSA) ID in the S13 ME Identity Check Request message towards EIR entity.

The feature enables operators to exclude the vendor specific application ID from the S13 ME Identity Check Request message towards EIR entity.

Related descriptions

- [Exclude destination host \(Feature f11335-01\)](#)

3.4.4 MME EIR enhancements for TAU procedure EIR queries and MSISDN inclusion in ECR (Feature f11309-01)

The CMM supports mobile equipment (ME) identity check procedure (such as EIR

checking) during the attach procedure for home UEs. With this feature, a new parameter to support sending the UE's MSISDN in the Equipment Check Request message sent over S13 interface is added. In addition, this feature also adds provisionable support for performing EIR checking during tracking area update procedure.

The *IMEI* checking feature is still applicable. If this feature's parameter (`supportMsisdnInEcrMsg`) to support sending MSISDN through the S13 interface towards the EIR is enabled, the MSISDN AVP will be included ECR message, if available.

In a normal registration sequence, the update location procedure towards the HSS occurs after the IMEI checking is performed to send the MSISDN for the MME. If the parameter `supportMsisdnInEcrMsg` is enabled, the MME waits until the update location procedure is finished in order to obtain the MSISDN from the HSS. The MME will then execute the IMEI check procedure.

This feature also introduces provisioning for periodic checking at every TAU.

3.4.5 EIR check result of Equipment Unknown to attach successfully (Feature f11309-03)

This feature supports a provisioning option per PLMN to allow UEs with a EIR check result of "Equipment Unknown" to attach successfully.

The feature is controlled by the `allowUnknEquipEirRsp` parameter of the `cmm plmn` command. When the value of the `allowUnknEquipEirRsp` parameter is set to `true`, the UE is allowed to continue with the attach request towards the MME. If the parameter value is set to `false`, the UE's attach request is rejected.

3.4.6 IMEI check for roamers (Feature f10416-01)

This feature introduces IMEI checking for roamers.

The MME performs IMEI check during initial attach (both GUTI and IMSI attach) procedure for roamers by keeping roamer QoS functionality working in conjunction, and allowing local breakout (used for IMS service) for roamers. Existing `validateImeiEir` parameter of the `cmm plmn` command is used for the activation of this feature when the `plmnType` parameter is `Other Network`.

3.4.7 MME support for locally provisioned IMEI-TACs rejection list (Feature f10422-01)

This feature allows the operator to provision an IMEI-TACs list locally in the MME, which can block UE access to 4G.

This feature allows the MME to define a rejection profile per UE PLMN or serving PLMN. The rejection profile includes the IMEI-TACs list, the EMM cause codes for the Attach/Service/TAU reject message, and, optionally, the Extended EMM cause IE.

When a UE attempts an attach, service request, or intra-MME or inter-MME tracking area update on 4G and its IMEI-TAC is included in the rejection list, the MME rejects the UE attempt with the provisioned EMM cause code.

When the MME is provisioned to reject the UE attempt with EMM cause code #15 No Suitable Cells In tracking area and the CLI parameter

`extendedEmmCauseCurrentRatNotAllowed`, which controls the inclusion of the Extended EMM cause IE, is set to `true`, MME performs the following actions:

- Includes the Extended EMM cause IE on Attach Reject messages and TAU Reject messages.
- Sets the bit, based on the RAT type, to Not Allowed.

When the UE attempts to access a tracking area associated with WB-E-UTRAN or NB-IoT, the MME sets “E-UTRAN not allowed” or “NB-IoT not allowed” respectively.

i Note:

- If the RAT type is not indicated for a tracking area, WB-E-UTRAN RAT type is assumed.
- Extended EMM cause IE is required to disable the E-UTRAN capability. It can only be used together with EMM cause code #15 No Suitable Cells In tracking area. Extended EMM cause IE requires support from the UE, that is, an old UE may not obey it.
- Extended EMM cause IE is defined to be used on Attach Reject messages and TAU Reject messages, not on Service Reject messages.

Emergency calls are not impacted by this feature.

3.4.8 MME support for selective IMEI-based operator policies (Feature f10422-02)

This feature allows the operator to provision the UE access restriction, selectively enable/disable IMEI checking towards the EIR and enable/disable authentication for UEs that match the operator's specified combinations of IMEI-TAC, serving PLMN, UE PLMN and IMSI range.

Different parameter combinations can be provisioned to define the UEs for which the operator's specific policies are applied. The MME supports the following parameter combinations:

- IMEI-TAC only
- IMEI-TAC and serving PLMN ID
- IMEI-TAC and UE PLMN ID
- IMEI-TAC, UE PLMN id and serving PLMN ID
- IMEI-TAC and IMSI
- IMEI-TAC, IMSI and serving PLMN ID

Additionally, the MME supports the following policy options for the UEs matching the provisioned criteria:

- Access is restricted/rejected. The UE's attempt is rejected as soon as the MME has the IMEI of the UE.
- Access is directly granted without any EIR check, that is, the MME overrides or skips any possibly provisioned EIR check for this UE.
- Authentication is disabled.

The policy provisioned criteria are the following:

- IMEISV list or range (either the IMEISV list or the range must be specified)
- Serving PLMN id (optional)
- UE PLMN id (optional)
- IMSI range (optional)

For UEs that match the provisioned criteria, one or more of the above policies are applied.

For UEs that do not match the provisioned criteria, the MME performs EIR check and authentication according to the existing settings and continues the procedure according to the result.

If the UE access is restricted, the MME does not proceed further with the procedure after receiving the IMEI/IMEISV. The MME allows the operator to provision the causes for the

attach/TAU reject procedure when the access is restricted.

In case the reject policy has been provisioned in the UE, the MME rejects the UE to access the MME as soon as the MME receives the IMEI of the UE. This happens in the following cases:

- Attach when the IMEI/IMEISV is retrieved via the NAS Identity Response (IMEI/IMEISV Request).
- Attach when the IMEI/IMEISV is retrieved via the NAS Security Mode Complete message (IMEISV Request).
- TAU when the IMEI/IMEISV is retrieved via the NAS Security Mode Complete message (IMEISV Request).
- Inbound handover when the IMEI/IMEISV is received during TAU procedure.
- S10 and S3 attaches when the IMEI/IMEISV is retrieved with IMSI on GTP Identification Response message.
- Inter-RAT TAU and intra-LTE TAU with MME change when IMEI/IMEISV is received with IMSI on Context Response message.

If the EIR check policy is disabled, the UE accesses the MME without performing any EIR check. This applies to procedures in which the EIR check is performed like the attach and the TAU procedures. The cases in which the IMEI is received, if not already known by the MME, are the same as mentioned above on the access rejection cases.

The MME supports the attach, TAU (intra/inter MME) and service request procedures as part of this feature to check for the UE provisioned policy. The MME allows the operator to provision the service reject cause when the access restriction is provisioned and the UE is already attached. In case that a UE, that is already attached to the MME, is provisioned with the reject policy and performs a service request or TAU procedure, the MME rejects the UE procedure with a provisioned cause code. The service request and intra-MME TAU procedures are included to cover provisioning updates when the impacted UEs are already registered on the MME.

 **Note:**

The IMEI-based operator policies are not applicable for the emergency calls.

3.4.9 MME support for IMEI and TAC/SV ranges (Feature f14620-01)

This feature enhances the current call processing algorithm for reading the IMSI range

services relation to allow the IMEI type approval code (TAC)/software version (SV) matching (where the TAC is the type approval code within the IMEI).

The call processing reads the IMSI range service relation using keys uePlmnServicesName, starting with entryId 1 and going up to entryId N until a match is found or until all records are exhausted.

For each retrieved record uePlmnServicesName, the call processing performs the following steps:

- If the UE IMSI does not fall within the provisioned MSIN range, that is, minMsin and maxMsin, on the record, the UE IMSI discards the record and restarts the algorithm using the next record.

 Note:

The current provisioning mandates MSIN range.

- If the UE's current tracking area does not fall within the provisioned taiLaiAreaListName on the record, it discards the record and restarts the algorithm using the next record.

 Note:

Current provisioning mandates taiLaiAreaList (if the TAI refinement is not necessary, “all TAC” is used.)

- If the IMEI TAC/SV list name is provisioned in the record but the UE IMEI type approval code (TAC)/software version (SV) is not specified in the list, the record is discarded and the algorithm is restarted using the next record.
- If the call processing finds the first record match based on steps 1, 2 and 3, the call processing stops the search and uses this record to obtain the UE's information. Otherwise, if no IMSI range service record match is found, it falls back to the UE PLMN services record to obtain the UE's information. The IMSI range services translation in CMM supports IMEI TAC and SV provisioning.

3.4.10 CMM support for EIR enhancements (Feature f11309-02)

This feature enhances the EIR support by having the MME reject the UE attach when the Equipment-Status AVP in the ME Identity Check Answer (ECA) message from the EIR is denylisted. This applies to both the IMSI and the GUTTI attach.

In all other cases, the MME continues the attach/TAU request. For example:

- Equipment-Status AVP in the ME Identity Check Answer (ECA) message is not denylisted.
- No response is received from the EIR.
- Diameter error cause code is received from the EIR.

This feature is controlled with global parameter `allowProcEirFailure`. By default, this feature is disabled.

When interact with feature *EIR check result of Equipment Unknown to attach successfully* (Feature f11309-03), CMM support for EIR enhancements (Feature f11309-02) takes precedence when both features are enabled.

3.5 Detach

Features controlling the way subscribers detach from the network.

3.5.1 Detach (Feature m10000-04)

With the detach procedure, a subscriber leaves the LTE network in a controlled manner and resources are released. The MME removes the temporary subscriber data from its data repository in a controlled manner and deletes allocated resources (radio and evolved packet system (EPS) bearers).

A detach procedure can be initiated by the UE or the network:

- Detach is initiated by the UE when the subscriber moves out of the LTE network range or shuts down the UE or the UE connectivity. If there is an explicit detach, the UE sends a Detach Request message. If the detach is not a power-off detach, the MME responds with a Detach Accept message. The MME makes an implicit detach if the UE moves out of the network coverage area when the MME timers expire and the UE has not done periodic updates to the network.
- The MME detaches the subscriber by sending a Detach Request message to the UE. The UE responds with a Detach Accept message to the MME. The operator can detach the subscriber manually with a command.
- The HSS detaches a subscriber through the HSS database with a cancel location procedure. The MME initiates a detach procedure to the UE.
- The gateway deletes the last default bearer of the UE. The MME initiates a detach procedure to the UE.

3.5.2 Enhanced handling of network-initiated detach (Feature m10143-01)

The **Enhanced handling of network-initiated detach** feature enables operators to define and choose appropriate detach profiles to control and customize network-initiated detach handling at the UE public land mobile network (PLMN) level.

This feature supports provisioning of detach UE parameters to control the behavior of the UE when the UE is detached by the MME. The provisioning consists of a detach reason and a number of parameters for each detach reason. The provisioning is provided per UE PLMN. The MME provides an ability to create up to 8 detach profiles and assign a profile to a UE PLMN. The detach profile consists of the following parameters:

- Detach reason specifies the reason for detaching a UE. Part 1 of this feature supports three reasons: S6a Cancel Location Request with cancelation type Subscription Withdrawal, SGW failure/SGW restart, and Delete Bearer Request with no Cause information element (IE) included.
- For each detach reason, the MME supports provisioning of the following parameters:
 - Notify ECM-IDLE UE: If this parameter is set to true, the MME pages the UE. Once the UE responds to the page, the MME sends the Detach Request to the UE (explicit detach). If the parameter is set to false, the MME implicitly detaches the UE, that is, no paging and no sending of Detach Request message to the UE.
 - Detach type to be sent to the UE in the non-access stratum (NAS) Detach Request message: re-attach required and re-attach not required.
 - Include the EMM cause in the NAS Detach Request Message: the MME includes the EMM cause with the provisioned cause value if the parameter is set to true. If it is not, the MME does not include the IE.
 - EMM Cause: The cause code is included in the detach request if Include EMM cause in the NAS detach message is set to true. Any cause codes in 3GPP TS 24.301 Annex A can be selected.

An ECM-CONNECTED UE is always explicitly detached with the provisioned parameters. For all other detach reasons the existing implementation applies. For a UE that is attached for E911 whose home network does not have roaming agreements, the MME applies the detach profile of the serving PLMN.

3.5.3 Immediate detach after receiving barring of packet oriented services (Feature m10124-01)

The ***Immediate detach after receiving barring of packet oriented services*** feature provides operators the flexible operator-determined barring (ODB) handling that can allow a UE to continue having service in its public land mobile networks (PLMNs) or in the visited network (VPLMN) based on the ODB setting received from the HSS.

This feature supports the barring of the existing evolved packet system (EPS) bearer contexts based on the ODB for the packet-oriented services that are invoked in the MME. If the MME receives Insert Subscriber Data message because of the barring of packet-oriented services being applied to a subscription (or the existing barring of the packet-oriented services is modified) by an administrative action in the HSS, the MME takes one of the following actions depending on the barring category when one or more EPS bearer contexts exist in the MME.

- For subscribers barred completely from the packet-oriented services, the MME deactivates all the existing EPS bearer contexts.
 - In addition, if ODB-HPLMN-APN barred bit is set to 1 (roamer access HPLMN-APN barred) and ODB-VPLMN-APN barred bit is set to 0, the MME deletes home network (HPLMN) bearers and if there are no bearers left, the MME detaches the UE.
 - If ODB-VPLMN-APN barred bit is set to 1 and ODB-HPLMN-APN barred bit is set to 0, the MME deletes VPLMN bearers and detaches the UE if there are no bearers left.
- When either ODB ROAMER_ACCESS_HPLMN_AP_BARRED or ODB ROAMER_ACCESS_TO_VPLMN_AP_BARRED is 1 in the Update Location Answer, and if the procedure is the MME relocation TAU, the MME deletes the corresponding HPLMN or VPLMN bearers after the procedure is completed. If there are no bearers left, the MME detaches the UE.

3.5.4 2G/3G UE not detached upon moving to a co-located MME (Feature f52038-01)

With this feature, the CMM does not detach UE when the IRAT mobility within a region is between the collocated MME and SGSN.

This feature only applies to IRAT handover.

In the following cases, if the MME cannot determine region change due to lack of knowledge of the old TAI, then the MME detaches the UE with reattach required.

For intra-MME mobility:

- UE mobility within a region: MME does not detach the UE.
- UE mobility between two regions: In case of intra-MME mobility, the MME has the knowledge of the new TAI and old TAI. The MME checks whether the UE moved to a new region or not. If it does, the MME detaches the UE with reattach required.
- UE mobility between a TAI which is not assigned to a region and a TAI which is assigned to a region: The MME detaches the UE with reattach required.
- UE mobility between two TACs which are not assigned to a region: The MME does not detach the UE.

For MME relocation:

- The new MME uses the last-visited-registered TAI to determine the region change and whether the IE is included or not. If the IE is not included, the MME detaches the UE with reattach required.

For IRAT mobility:

- If the IRAT mobility within a region, for example, the UE is moving from a location area to a tracking area, is between the collocated MME and SGSN, such as MME/SGSN, the MME does not detach the UE.
- If the UE is moving from a non-collocated SGSN, the new MME uses the mapped GUTI to derive LAC (MME group ID maps to LAC), to determine the region change and to decide whether the UE should be detached or not.

In case of S1HO or X2HO with TAI change, a TAU request is expected. An internal timer is started to wait for the TAU request. If the timer expires before the reception of the TAU request, the MME detaches the UE when the old TAI and the new TAI are not in the same region.

In all these cases above, the UE is not detached if UE has an emergency QCI=1 bearer.

The feature can be enabled for 2G/3G or LTE. There is a threshold and monitor time parameter which causes the MME to stop detaching UEs for a provisioned suppression interval.

3.5.5 TA group based handling enhancement (Feature f10123-02)

This feature brings APN level enhancements into the existing functionality to detach a UE when it moves across regions.

This feature introduces CMM enhancements to the capabilities introduced by the WMM

support for UE detach upon moving across region (m10143-03) feature.

The legacy feature always performs a detach when the UE crosses a region border.

This feature introduces two new APN lists with new functionalities and enhanced APN level logic. These enhancements allow scenarios in which some UEs may not be detached upon mobility regions:

- The SustainAPN list type allows the operator to provision APN(s) that need to be sustained despite of the UE moving between regions.
- The DelayedAPN list type allows the operator to provision APN(s) that can only be deactivated when no dedicated bearer(s) are established.

If a UE moving between regions has either a PDN towards an APN on the sustained APN list established or has a PDN towards an APN on the delayed deactivation APN list with dedicated bearer(s) established, the UE is allowed to access the new TA. Any PDNs retained for delayed deactivation, will be deactivated upon the deletion of the final dedicated bearer associated with that PDN.

The new functionalities require the legacy functionality to be enabled in addition to the new functionality.

3.5.6 Mass detach of all UEs on a TA group (Feature f52060-01)

This feature allows an operator to activate a mass detach or force an IP address change for all UEs in a specified tracking area (TA) group.

This feature allows operators to force subscribers to change their IP addresses, which are used for PDN connections, to new addresses from a specific pool, as per a security regulations order. Operators can use the `mmeForceIpChange` to perform a mass detach or forced PDN reactivation of all subscribers from a specified region, defined as a TA group. This feature builds on the WMM support for UE detach upon moving across region (m10143-03) feature, which enables the operator to restrict UE mobility across TA groups, forcing a UE to re-attach or re-activate all its active PDNs when it moves from one TA group to another.

To prevent overloading neighboring network elements during a mass detach or PDN deactivation, MME performs the detach or PDN deactivation with a harmless rate limit, evenly initiating the detach or deactivation of all UEs or PDN connections in a controlled time period.

When a mass detach or forced IP address change on TA group affects a UE, the action

depends on ECM state of the UE:

- If the UE is in the ECM-CONNECTED state, then communication with UE or eNB is performed; for example, the MME then sends the Detach Request with EMM cause #10 (implicitly detached) and detach type set to Re-attach required.
- If the UE is not in the ECM-CONNECTED state, the MME applies associated signaling towards network peers without paging the UE.

 **Note:**

Actions are performed even if UE has aged out but remains in the EMM-REGISTERED state.

A mass detach or forced IP address change does not affect any emergency-attached UEs; that is, any UE that has only an emergency PDN. If UE has both an active emergency PDN and one or more non-emergency PDNs when the mass detach or forced IP address change is performed, the MME only deactivates the non-emergency PDNs.

Parallel mass detaches or forced IP address change operations in different TA groups are not supported.

3.5.7 CMM support for CLI command to explicitly detach all UEs for an input roaming PLMN (Feature f10428-01)

This feature introduces a CLI command to explicitly detach all the UEs for a specific roaming PLMN.

The subscriber force detach process on a UE PLMN is performed for a specific UE depending on the UE state. If the UE is in the idle state, it implicitly detaches without paging. If the UE is in the connected state, the UE explicitly detaches. After the UE is detached, the UE context is removed by deleting a subscriber.

The CLI command starts and stops the force detach procedure based on the roaming PLMN entered. Also, the command shows the progress of the mass detach procedure.

The start and stop commands can only be performed by the admin user.

Note:

The detach process must be performed in a controlled way to avoid overload of the CMM. The detach operation takes into account the current unit load status so that the mass detach does not lead the system to overload; that is by dynamically adapting the mass detach rate based on the unit load status.

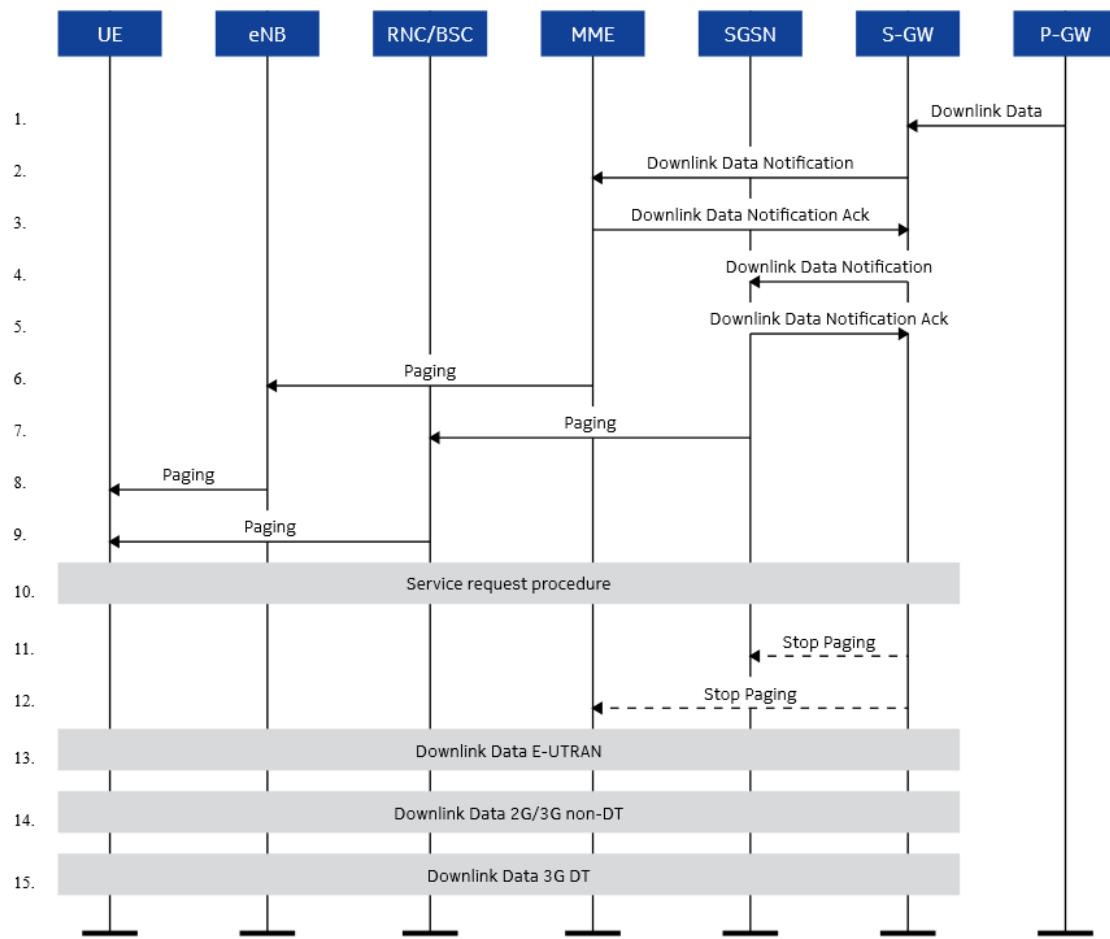
3.6 Reachability and paging

The tracking area update (TAU) functionality enables the MME to be aware of the UE's location. The purpose of the service request procedure (idle - active change) is to transfer the UE's external provisioning system connection management (ECM) state from ECM-IDLE to ECM-CONNECTED and establish the radio and S1 bearers when uplink user data or signaling is to be sent. In the network-initiated service request, the MME uses paging to activate the UE.

Paging procedures for network service requests

In a network triggered service request (NTSR), paging is initiated by the MME to establish a non-access stratum (NAS) signaling connection to the UE when notification is received from the S-GW that a radio bearer must be established to the UE. Paging messages are sent to a set of eNBs based on the current paging method and the last known location of the UE (for example, page all eNBs in the last seen tracking area (TA)). When the UE receives the paging message, a network triggered service request procedure is initiated. Upon reception of a paging indication, the UE responds to the paging with a Service Request message. The call message flow diagram for this type of service request is from 3GPP TS 23.401 Section 5.4.3 and is shown in the figure.

Figure 8: NTSR paging procedure



Paging for EPS services through E-UTRAN using IMSI

Paging procedures for services using international mobile subscriber identity (IMSI) is an abnormal condition used only for the error recovery in the network. The network can initiate paging using IMSI with the core network domain set to packet switching (PS) if the S-temporary mobile subscriber identity (S-TMSI) is not available because of a network failure.

Upon reception of paging services using IMSI, the UE locally deactivates any evolved packet system (EPS) bearer contexts and locally detaches from the EPS, deletes EPS parameters, and changes the state to EMM-DEREGISTERED.

After having done the local detach from the LTE network, the UE does an attach procedure. If the UE is operating in circuit switching/packet switching (CS/PS) mode 1 or CS/PS mode 2 of operation, it does a combined attach procedure.

Paging for CS fallback to A/Gb or Iu mode

The network can initiate the paging procedure for a circuit switched fall back services (CSFB) when the UE is IMSI attached for non-EPS services. This paging procedure can be initiated by the network with or without an existing NAS signaling connection.

Upon receipt of a page, the UE responds with an Extended Service Request. If the page is received in EMM-IDLE mode, the UE responds immediately. If the paging is received as NAS CS Notification message in EMM-CONNECTED mode, the UE can request input to accept or reject CS fallback before responding with an Extended Service Request. The response is indicated in the CSFB response information element in the Extended Service Request message in both EMM-IDLE and EMM-CONNECTED modes.

Tracking area

A TA represents a group of contiguous cells with the E-UTRAN and is used to help locate a device (UE) that has gone into EMM-IDLE state. It is analogous to location area (LA) or routing area (RA) in the GSM/UMTS networks though the size of the TA typically is smaller than either a RA or LA. Tracking areas are used by the MME to locate a UE within a group of cells (eNBs) in which it was last registered (EMM-REGISTERED). The MME pages the UE within the TA to locate the UE and determine which particular eNB it is nearest. A TAU is generated when the UE crosses the boundary from one TA to another TA.

The 3GPP standards define a multiple-TA registration scheme whereby the MME sends a TA list (one or more TAs) to the UE. The UE requests TAU only when it moves to a TA that is not in its current TA list with the exception of a periodic TAU. An example of a TA list with two TAs is shown in the figure. In this example, the UE can move to any cell within TA1 and TA2 without requiring a TAU because it has both TAs in its current TA list.

Figure 9: TA list from the UE's point of view



In addition to the MME managing TA lists and TAUs in LTE networks, it must also consider routing area updates (RAU) and location area updates (LAU) or combined RAU/LAU, when the UE moves out of the LTE coverage and into the 3G or 2G coverage. At TA and RA/LA borders, significant amount of paging can occur because of frequent area updates as the UE moves between networks. The 3GPP standards have defined idle mode signaling reduction (ISR) as a

means of mitigating the paging attempts during area updates between the LTE and 2G/3G networks but care must be taken in designing the area boarders between the 2G, 3G, and LTE networks to minimize signaling because of an area update.

Tracking area identity

A tracking area identity (TAI) is a 32 bit code used to uniquely identify a TA. The MME maintains a list of TAs by TAI. The MME is responsible for the selection of registered tracking areas for each UE during the attach and TAU procedures. During these procedures, the UE is sent a list of TAI where the UE's location is registered within the Attach Accept and TAU Accept messages. The UE can move within any of these registered tracking areas without triggering a location-based TAU.

A TAI is comprised of the following codes:

- TAC – Tracking Area Code
- MNC – Mobile Network Code
- MCC – Mobile Country Code

The TAC is a 16 bit integer that represents a unique tracking area within the mobile operator's network. The TAC can be encoded or constructed so that it can identify a specific market and the TA number# within the market.

The MCC and the MNC are also a 16 bit integer and together they define the mobile operator public land mobile network (PLMN) ID.

The TAI is used for an S-GW/MME selection and discovery. The MME selection/discovery of a target MME/S-GW is based on domain name server (DNS) configuration. A serving MME/S-GW that is associated with each TAI needs to be configured in the DNS server name authority pointer (NAPTR) records. The MME does a DNS query based on the TAI that is associated with a serving/target cell. The MME forms a fully qualified domain name (FQDN) based on low/high bytes from the TAC.

Each eNodeB Cell-id is configured with a TAI that is broadcast in the System Information Block (SIB). All cells in the same eNB can be configured with the same or different TAI.

Tracking area update timer

TAU is used to notify the availability of the UE to the network. The procedure is controlled in the UE by the periodic tracking area update timer (T3412). The value of the timer T3412 is sent by the network to the UE in the Attach Accept message and can be sent in the TAU Accept message. The UE applies this value in all tracking areas of the list of tracking areas

assigned to it until a new value is received.

The timer T3412 is reset and started with its initial value, when the UE goes from EMM-CONNECTED to EMM-IDLE mode. The timer is stopped when the UE enters EMM-CONNECTED mode or EMM-DEREGISTERED state.

Paging strategy

The MME provides mobile operators with the flexibility to design a paging strategy that controls various aspects of paging such as:

- Maximum number of paging attempts (up to four attempts)
- Timer interval (interval to wait for page response) used for each page attempt
- Paging method used (four methods currently available)
- eNBs and the number of tracking areas to include in the page attempt

The overall goals and objectives of developing a paging strategy are threefold:

- Increase the effectiveness of paging by:
 - reducing the number of failed connection attempts because of paging failures
 - getting a response from the UE within the fewest possible number of page attempts
- Increase the efficiency of paging by:
 - reducing number of paging messages sent to each UE (that is, reducing downlink (DL) traffic)
 - avoiding overloads on the downward link whenever possible
 - developing a comprehensive strategy for handling DL overloads when they do occur
- Increase the efficiency of determining UE location (that is, tracking area updates) by:
 - reducing number of TAU Requests generated by each UE (that is, reducing uplink (UL) traffic)
 - avoiding overloads on the upward link whenever possible
 - developing a comprehensive strategy for handling UL overloads when they occur

These three objectives are interrelated and finding the correct balance between them has historically been a challenge.

The MME supports paging of up to 2000 eNBs for a single page attempt. In addition, the MME supports paging up to 1200 eNBs per TAI and a TAI list of up to 15 TAs. However, it is expected that UEs will be paged using a much smaller sized TAI list. If TAs are added to the TAI list using the automatic method (as specified with the autoAddTaiToTaiList global parameter), UEs will typically be paged in only 1 TAI and can be paged in a maximum of 3 TAs.

The paging policy defines the paging methods and procedures used by the MME to page the

UE. The paging policy is configured at the time of installation but it can also be modified post-installation. The MME executes the paging procedure in accordance with the paging policy as currently provisioned by the MSP.

The following are required and optional paging parameters that can be provisioned as part of the MME paging policy.

Page type

The `pagingType` is an optional parameter that describes a service attribute associated with the paging policy (`pagingPolicy`). The default value is none.

By defining a page type and its associated paging parameters for specific service as part of the overall paging policy, the MSP can both improve the probability of locating the UE in fewer attempts while reducing the net amount of paging in the network.

Page attempt

The paging attempt (`attempt`) refers to ordinal position (first, second and so on) as well as the count (number of times the MME tries to page the UE) within the current paging policy before the UE is deemed unresponsive. Up to four page attempts can be defined for a paging policy and if the page attempts are defined they must start with 1 and they must be sequential. The default value for the page attempt is none.

Paging method

With each page attempt the following paging methods (`method`) are supported:

- `LastSeenENB`
- `LastSeenENBList`
- `LastSeenTAI`
- `LastSeenTAINBTAI` (last seen TAI and neighboring TAIs)

In the last seen eNB paging, the MME sends a Paging message to the eNB that sent the last TAU Request or Service Request for the UE.

- If the extended range parameter (`extRangeFlag`) of the paging policy is `false`, only the TAI of the last seen TA is included in the Paging message.
- If the extended range parameter is set to `true`, the TAI's of all TAs served by each eNB are included.

 **Note:**

The last seen eNB field is set by the attach, TAU, and service request procedures.

The last seen eNB list method pages the last seen eNB plus 1 to 4 previously visited eNBs.

- As with other paging methods, the existing extended range flag field is used to provide additional control over how the paging method operates.
- If the extended range parameter is set to `false` and the last seen eNB list paging method is used, the eNB paging list is filtered to include only TAs from the UE's registered TA list (that is, the TAI List in last Attach Accept or TAU Accept message).
- If the extended range parameter is set to `true` and the last seen eNB list paging method is used, the eNB paging list is not filtered based on the UE's registered TA list. In other words, the UE can be paged in TAs where it is not currently registered.
- The maximum eNBs paged field (`maxEnbsPaged`) in the paging policy table defines the maximum number of eNBs that can be paged for this page attempt. A value of 0 indicates that the default limit of eNBs to be paged should apply. The default limit of eNBs to be paged for the last seen eNB list paging method is 5.

In the last seen TAI paging, the MME sends Paging messages to all eNBs associated with the last seen TA for the UE (that is, the TA associated with the last TAU Request or Service Request).

- If the extended range parameter of the paging policy is `false`, only the TAI of the last seen TA is included in the Paging messages.
- If the extended range parameter is `true`, the TAI's of all tracking areas served by each eNB are included.

In last seen TAI and neighboring TAI's paging, the MME sends Paging messages to all eNBs associated with the tracking area specified in the last seen tracking area for the UE and all eNBs associated with TAs that are defined to be neighbors of the last seen TA:

- all TAI's where the UE is registered, and the TAI's in the provisioned TAI neighbor list for the last registered TAI (if any)
- If the extended range parameter of the paging policy is `false`, only the TAI's of the last seen TA and the neighboring TAs are included in the Paging message.
- If the extended range parameter is `true`, the TAI's of all TAs served by each eNB are included.

The default value for page method is last seen eNB. The MME uses the paging method that is provisioned within the paging policy for the current page attempt.

Page timer (T3413)

The page timer (`t3413Timer`) specifies the value for the T3413 timer that is used to wait for a response to a paging request. When this timer expires, it triggers the MME to proceed with the next paging attempt as provisioned in the paging policy. This timer value (from 1-60 seconds with a default value of 6 seconds) should be set according to the maximum time it takes a UE to respond to a paging message under normal operating conditions.

Extended range flag

The extended range flag (`extRangeFlag`) is a value that is set to either `true` or `false` for each paging method defined within the paging policy. The setting of the extended range flag determines the TAI values sent in the page message to each eNB for the paging method specified in that page attempt. If the extended range flag is set to `true`, the page message includes all of the TAIs associated with the last known eNB or served by each eNB. If extended range flag is set to `false`, the TAI list is limited to only the last seen TA or last seen TAI's neighbor TAIs.

The MME sends a separate page message to every eNB in the paging broadcast with the following information elements that are encoded as specified in 3GPP TS 36.413 section 9.1.6:

- UE Identity Index value (IMSI mod 1024)
- UE Paging Identity (IMSI or S-TMSI)
- CN Domain (default: PS)
- List of TAIs

The list of TAIs included in each Paging message only refer to TAs associated with the eNB receiving the message.

- Optional: MS Network Capability information element (IE)
- Optional: Paging DRX IEs

If the discontinuous reception (DRX) parameters available flag is set to True in the current UE Context, the MME examines the DRX value for S1 mode stored in the UE context to determine if the Paging DRX parameter should be populated in the S1AP Paging message.

 **Note:**

The optional MS Network Capability and Paging DRX IEs are not sent if no S-TMSI exists for a UE context, the MME sends the IMSI value as specified in C1-84343.

The Paging DRX value is determined as follows:

Table 11: Paging DRX value

Bit of octet 3				Paging DRX 8 7 6 5 value (T)
8	7	6	5	
0	1	1	0	32
0	1	1	1	64
1	0	0	0	128
1	0	0	1	256

If the DRX parameters available flag is set to False or if any other bit pattern than the one shown above is present for the DRX value for S1 mode field, then no Paging DRX parameter is populated in the S1AP Paging message.

Specific MME responses to the receipt of paging related messages:

- Upon receipt of a Service Request message sent as part of the dynamic domain name (DDN), the MME retires the T3413 (wait for page response) timer.
- Upon receipt of multiple DDNs while the paging procedure is still in progress, the ongoing paging procedure is not affected.
- Upon receipt of a Cancel Location Request (CLR) from the HSS, the MME queues the CLR.
- Upon receipt of any NAS message other than Service Request from the UE while the paging procedure is in progress, no further page attempts are made for the current network-initiated service request and the MME sends a Downlink Data Notification Failure message to the S-GW with a cause code of Service denied.
- Upon receipt of a Downlink Data Notification message while a UE triggered service request procedure is in progress, the MME does not page the UE. It responds with a Downlink Data Notification Ack and proceeds with the UE triggered service request procedure.

Old GUTI paging

Release 12 and Release 13 standards update for MME (Feature f10001-01) introduces provisioning of global parameter `enableOldGutiPaging` to allow old GUTI paging per MME. MME sends S1AP PAGING message for each paging attempt using S-TMSI from old GUTI and also S-TMSI from the new GUTI. MME is not required to page UE with IMSI if paging

with old and new S-TMSI fails.

Automatic paging suppression

When a UE loses contact with the LTE network but is still registered on the MME, all paging operations to reach that UE will fail after all configured page attempts timeout. This situation can lead to repeated paging failures and result in generating a significant amount of paging message traffic for a single UE. A relatively small percentage of UEs that repeatedly fail to respond to pages can lead to excessive paging message traffic on the MME.

In order to prevent excessive MME paging message traffic from creating a critical overload condition on the CMM, the following paging suppression methods are supported:

- Paging suppression based on extended UE inactivity.
- Paging suppression based on repeated paging failures.
- Restricted paging during overload.

Paging suppression based on extended UE inactivity

Each UE in the ECM_IDLE state is expected to initiate a periodic TAU procedure when its T3412 timer expires. The MME continually searches for UEs that have not performed a periodic TAU procedure after expiration of the T3412 timer. If the time interval since T3412 timer expiration exceeds the configured mobile reachability timer interval, the MME will suppress paging for that UE until the UE reconnects with the LTE network. For normal UEs, the `mBReachable` timer is used for this purpose. For low priority access (LPA) UEs, the `mobileReachableLpa` timer is used.

When a Downlink Data Notification is rejected by the MME because paging is suppressed due to extended UE inactivity, an SCFCQ value of 907 will be specified.

If the UE continues to remain inactive from the perspective the MME beyond this point, the MME will eventually trigger an implicit detach operation and then finally trigger a purge operation for the UE.

Paging suppression based on repeated paging failures

Although paging suppression based on extended UE inactivity reduces unnecessary MME paging, UEs that have lost connection to the LTE network can still cause a significant amount of paging traffic until the mobile reachability timer expires. In order to address the generation of excess paging within this earlier time interval, the MME also supports paging

suppression based on repeated failures.

This paging suppression method is also known as the paging gap timer feature. This feature allows the service provider to suppress excessive paging that may result when the MME attempts to reach UEs that repeatedly fail to respond to pages and have lost contact with the LTE network.

When the `pagingGapTimer` timer is set to a non-zero value, paging will be suppressed by the MME for the provisioned interval of time after three (3) consecutive ‘no page response’ failures have occurred while attempting to reach a specific UE. A ‘no page response’ failure occurs when the MME has exhausted all provisioned page attempts as specified in the MME paging policy table. After the paging gap timer interval has ended, the MME will resume paging of that UE. However, another ‘no page response’ failure will trigger another round of paging suppression for the duration of the paging gap timer interval.

Note that the default value of the `pagingGapTimer` timer is 0. As a result, a service provider must change the timer value in order to activate the paging gap functionality.

Restricted paging during overload

Additional protection against excessive MME paging traffic is provided through support of restricted paging during overload.

When the global parameter `restrictPagingDuringOverload` is set to `Yes`, the MME will automatically direct MME paging to exclusively use the restricted paging type when one or more the following conditions are present:

- A major CPU overload alarm has been raised on the IPDS or CPPS.
- A minor memory overload alarm has been raised on the IPDS or CPPS.
- The active IPDS was initialized as a result of IPDS switchover or an IPDS fault in the last 2 minutes.
- An aggregate service unlock occurred for the MME in the last 5 minutes.

The service provider can provision paging policy (`cmm pagingPolicy`) database records for the restricted paging type. However, if no paging policy records have been provisioned for the restricted paging type, the MME will perform a single page attempt using the `LastSeenENB` paging method when restricted paging is triggered during an overload.

Prior to CMM20 M2, the default value of the `restrictPagingDuringOverload` parameter is `No`. As a result, a service provider must change the parameter value in order to activate the restricted paging functionality. Post CMM20 M2, `restrictPagingDuringOverload` defaults to `Yes`.

3.6.1 Impact of paging policy provisioning

The provisioning of paging policy records and the sizing of tracking areas should be made with a full understanding of resulting impact to the message traffic level in the network.

While selective use of aggressive paging methods such as LastSeenTAI is necessary and appropriate, the overuse of aggressive paging methods can lead to overload conditions on both the CMM and eNB. While the CMM will react to mitigate the impact of overload conditions, the existence of these overload control mechanisms does not preclude the need to understand the consequences of choices when sizing tracking areas and provisioning of paging policy records. The paging channels of the eNBs are a limited resource. A well-designed paging policy will prioritize the use of MME paging so that the aggressive paging methods are utilized only in cases where less aggressive paging methods have failed to reach the UE or are used in limited cases where it is critical to reach the UE quickly (for example, for VoLTE calls).

The impact of paging policy provisioning can be demonstrated with the following general formula:

$$\begin{aligned} \text{Number of paging messages generated for paging type=} \\ (\text{Number of UEs served by MME}) \times \\ (\text{Scenario frequency}) \times \\ (\text{Average number eNBs paged for paging type}) \end{aligned}$$

The factors of the equation can be described as follows:

Number of UEs served by MME The value indicates the number of registered UEs attached to a specific CMM MME.

Scenario frequency The value indicates how often a scenario that results in MME paging with that paging type will occur for a UE. This metric can be expressed in terms of events per second. However, it is expected that the event rate would be significantly less than one event per second. Please note that the scenario frequency will vary depending on time of day.

Average number of eNBs paged for paging type	The value depends on the following: <ul style="list-style-type: none"> • Number of paging attempts provisioned for paging type • Paging method selected for each paging attempt • Number of eNBs per TAI (if using LastSeenTAI or LastSeenTAINBTAl paging methods) • UE movement patterns • Paging success rate
---	--

The impact of use of a more aggressive paging method such as LastSeenTAI will depend greatly on factors such as:

- scenario frequency
- page attempt where this paging method is used
- number of eNBs associated with the last seen TAI

For example, use of LastSeenTAI paging for the second page attempt is normally not an issue because the UE is typically reached by the first page attempt. In addition, use of LastSeenTAI paging has been safely used on the first page attempt for rarely used paging types. However, it is suggested that service providers consider the use of LastSeenEnbList paging since this paging method generates a fraction of the paging message traffic while yielding a significantly better paging success rate than LastSeenENB.

The impact of the more aggressive paging methods such as LastSeenTAI is directly proportional to the average number of eNBs associated with tracking areas. If the number of eNBs per tracking area is limited to 60 to 80 (as per long-standing recommendations), then the impact of aggressive MME paging will be significantly less (for example, ~10%) than if tracking areas are configured with 600 to 800 eNBs. If larger tracking areas must be used in a network, then it is strongly recommended to employ aggressive paging methods for lesser used paging types or when less aggressive paging fails to reach the UE

The total page message traffic level would be calculated as follows:

```
Total number of paging messages generated=
(Number of paging messages generated for Basic paging) +
(Number of paging messages generated for QCI 5 paging) +
(Number of paging messages generated for SGS CS paging) +
(Number of paging messages generated for SGS PS paging) +
(Number of paging messages generated for other paging)
```

The CMM's total paging message traffic level needs to be considered in conjunction with the CMM's overall message transmission rate limit (for example, 500K messages per second on a CMM with a single pair of IPDS VMs). If most of a CMM's message capacity is consumed with paging message traffic, overall MME call processing will suffer and the risk of overload is greatly increased. Furthermore, excessive MME paging affects the eNBs as well as the MME. If the MME generates excessive paging message traffic, the eNB's paging channel can be overloaded and paging failures can result. In addition, an increase in the paging failure rate will typically lead to additional paging attempts and will lead to even more paging message traffic.

3.6.2 Monitoring of paging message traffic

Recommended procedures for analyzing the impact of MME paging traffic.

The following procedure is suggested for analyzing the impact of MME paging traffic:

1. Calculate the total number of eNBs paged for the PM reporting interval using the counters:
 - `VS.EnbsPagedTotalFirstAttempt`
 - `VS.EnbsPagedTotalSecondAttempt`
 - `VS.EnbsPagedTotalThirdAttempt`
 - `VS.EnbsPagedTotalFourthAttempt`
2. Calculate the MME paging message rate by dividing the sum calculated in step 1 by the PM reporting interval (expressed in seconds).
3. Determine the maximum CMM message rate for the current configuration. For an Openstack large CMM or an A8 CMM with a single pair of IPDS VMs, the maximum rated CMM IPDS message rate is 500 000 messages per second.
4. Calculate the MME paging percentage of CMM message capacity using the MME paging message rate calculated in step 2 and the maximum CMM message rate determined in step 3.
5. If the MME paging percentage of CMM message capacity is 50% or more, it is recommended that proactive measures be taken to reduce the overall paging traffic level (for example, adjust paging policy). See below.
6. An ideal value for the MME percentage of CMM message capacity is 25% or less. It is desirable to engineer the network so that there is normally spare capacity to handle bursts of call processing activity that will occur over time.
7. Other metrics such as the current IPDS memory consumption should also be monitored. See below.

If the MME paging percentage of CMM message capacity (as calculated in step 4) is

determined to be too high, the following is recommended:

1. Use the CMM MME paging PM counts to determine which paging types are responsible for most of the MME paging message traffic.
2. Review the MME paging methods selected for these high runner MME paging types. Special attention should be paid to the paging method selected for the first page attempt.
3. Suggest using the LastSeenENBList paging method on first page attempt instead of the LastSeenTAI paging method (if possible).
4. Suggest eliminating redundant page attempts from paging policies. Repeating the same paging method for a paging type does not typically result in any significant additional paging success.
5. Recommend enabling the Paging Gap timer for reducing the level of ineffective page attempts.
6. Check if the relative number of idle UEs is higher than expected. If so, verify that the UE inactivity timer used by eNB is appropriate.
7. Check if the MME paging success rate is lower than expected. The paging message traffic will increase as more paging operations are forced to utilize the second and third page and fourth page attempts.

3.7 Paging

Paging and paging policy features.

3.7.1 MME support for 23.272 CR 706 (Feature m30101-06)

The MME support for 23.272 CR 706 feature helps restoring the UE SGs association.

With implementation of this feature the MME triggers international mobile subscriber identity (IMSI) detach after the UE responds to the S1 paging with the IMSI, which was triggered by the SGS paging without either temporary mobile subscriber identity (TMSI) or location area identification (LAI). This CR specifies not to IMSI detach for SGS paging without TMSI.

3.7.2 Paging policy selection based on QoS Class Identifier (QCI) (Feature m10202-01)

The **Paging policy selection based on QoS Class Identifier (QCI)** feature provides an MME capability to support different paging strategies for best effort calls and real-time calls (for example, voice over long-term evolution (VoLTE) or video). It provides quicker and higher overall success rate for network originated VoLTE calls without massive increase in the MME and eNB signaling load.

 **Note:**

Initial voice call set up, when network originated is a session initiation protocol (SIP) message and typically QCI-5 for the default bearer, QCI-1 is used for the dedicated bearer once paging sequence has resulted in a service request.

 **Note:**

Downside of using QoS class indicator (QCI)-based paging discrimination is that Downlink Data Notification (DDN) for a voice call cannot be distinguished from SMS DDN as both are established using QCI-5 for default bearer. For discrimination of voice from SMS, other paging methods, like paging priority indicator (PPI) paging, should be used.

The MME supports for each QCI value (or a set of QCI values) provisioning of paging as follows:

- Number of page attempts (up to 4)
- Paging method for each attempt (Last seen eNB, Last seen eNB list, Last seen tracking area (TA), Last seen TA and neighbor TAs)
- Extended range support
- Provisioning of separate T3413 for each attempt

This feature requires the S-GW to send evolved packet system (EPS) bearer ID/IDs in an DDN message.

The MME obtains QCI of a bearer from the UE context and selects provisioned paging strategy for the QCI.

If the MME receives multiple bearer IDs, the MME selects paging policy provisioned for the lowest QCI value of the received bearers.

The MME also provisions a paging policy based on the QCI of the bearers in the UE context if

the S-GW does not send bearer IDs.

The S-GW must provide bearer ID in DDN as defined in 3GPP standards (Rel 10).

3.7.3 Paging discrimination by Paging Priority Indication (Feature m11004-04)

The *Paging discrimination by Paging Priority Indication* feature supports additional discrimination of downlink data delivered in the Downlink Data Notification (DDN) from the S-GW to provide differentiated level of paging aggressiveness between data types (such as discrimination between downlink data for voice over long-term evolution (VoLTE) and SMS through IP multimedia subsystem (IMS)).

This is a Release 13 capability.

A Paging and Service Information IE is introduced in S11 DDN message. The IE includes

- Bearer ID
- Paging policy Indication (PPI): note that the PPI value is a 6 bit encoding of differentiated services code point (DSCP) in trunk offering start message (TOS) (IPv4) or TC (IPv6) information received in the IP payload of the GPRS Tunneling Protocol - user plane (GTP-U) packet from the P-GW.

The MME provides an ability to provision a paging policy for each PPI value (0 to 63).

The MME first checks the Paging Policy Indication flag in the Paging Service Information IE, and if the value is set to 1, it reads the Paging Policy Indication value, maps to a PPI paging policy (if provisioned), and validates whether differentiated paging service is allowed by checking the Paging Policy Indication value with provisioned access point name (APN) to QoS class indicator (QCI) to PPI mapping profile for the served public land mobile network (PLMN).

The feature provides quicker and higher overall success rate for network-originated VoLTE calls without massive increase in the MME and eNB signaling load, in particular without increasing paging load because of an SMS.

For this feature to work the S-GW must provide (R12) PPI indicator and value in DDN.

3.7.4 MME support for 6 byte UE Radio Capability for Paging IE (Feature f10925-01)

MME supports UE Radio Capability for Paging IE of maximum size of 6 octets, excluding the header, if received in the UE Capability Info Indication message.

MME stores the contents of the UE Radio Capability for Paging IE in UE context and includes it in the S1AP Paging message. MME also always includes the Extended UE Identity Index IE set to UE IMSI mod 16384 in the S1AP Paging message. The IE is used by the eNB in determining paging occasions for CAT-M1 devices.

3.7.5 SGs paging enhancements (Feature m30114-01)

The SGs paging enhancements feature supports automatic paging retries for a single SGs paging request to eliminate need to MSC retries of SGs paging message and to reduce SGs paging messages.

This feature supports SGs paging enhancement and queuing of SGs paging message from MSC/VLR if the paging message is received while the MME is handling a mobility management procedure. It supports automatic page retries for SGs Page Requests.

This feature can be enabled via provisioning. If the feature is enabled, the MME proceeds with the next page attempt when a time-out occurs for the earlier page attempt for that UE. If no response is received from the UE, then additional page attempts are done until all of the attempts provisioned in the paging policy are exhausted. If this feature is not enabled, only one page attempt is triggered by each SGs page request from the MSC. In this case, the trigger for moving on to the next page attempt is another SGs page request from the MSC.

The second enhancement to the current queuing of SGs paging message for a UE if the MME is busy handling a mobility management procedure. The MME handles the SGs paging request after the completion of the procedure. The procedures for which SGs paging message is queued include service request, tracking area update (TAU) request, S1 release, and paging.

3.7.6 MME support to add S1-AP paging priority to paging profiles (Feature f10203-01)

The MME provides the possibility to provision specific paging priority for low access priority UEs.

For a UE that has provided low access priority indication, the MME triggers paging with the paging priority level value provisioned for low access priority paging type.

A single paging priority level value can be provisioned for all pagings related to UEs indicating low access priority.

3.7.7 Paging 1200 eNBs (Feature f10204-01)

This feature increases the CMM's capacity related to MME paging. The MME is enhanced to send page requests up to 1200 eNBs for a single tracking area and up to 2000 eNBs for a single page attempt. CMM overload control is also enhanced to prevent overload conditions due to this greater paging capacity.

The increased paging capacity introduced by this feature is related to the following types of paging:

- Paging attempts using either the LastSeenTAI or LastSeenTAINBTAl paging methods
- IMSI paging for SGS page requests

It should be noted that MME's use of these paging types is limited. The LastSeenTAI and LastSeenTAINBTAl paging methods are typically used when the UE does not respond to the first page attempt. Furthermore, IMSI paging is only performed when no UE context data is available for the UE.

The following existing counts can be used to observe the impact of this feature:

- `VS.EnbsPagedTotalFirstAttempt`: number of eNBs paged during first page attempt
- `VS.EnbsPagedTotalSecondAttempt`: number of eNBs paged during second page attempt
- `VS.EnbsPagedTotalThirdAttempt`: number of eNBs paged during third page attempt
- `VS.EnbsPagedTotalFourthAttempt`: number of eNBs paged during fourth page attempt

In addition to the existing MME paging throttling supported for the major and critical overload levels, the MME now can perform limited paging throttling during a minor overload. The global parameter `maxEnbsPagedDuringMinorOverload` can be used to adjust the paging throttling level. This parameter specifies the maximum number of eNBs that are allowed for a single page attempt. Lowering the value of this parameter increases the amount of paging throttling during a minor overload while raising this parameter to 2000 effectively eliminates paging throttling during minor overload.

The following new counters can be used to observe the level of paging throttling performed during overload conditions:

- `VS.PagingEpsRestrictedByMinorOverload`: number of page attempts in which number of eNBs paged was received due to throttling during a minor overload
- `VS.PagingEpsRestrictedByMajorOverload`: number of page attempts forced to

use the restricted paging method due to throttling during a major or critical overload

3.7.8 Extending PPI paging to include QCI 65, 66, 69, and 70 (Feature f10201-02)

This feature extends the range of QCIs that can be provisioned for PLMN/APN/QCI cross check and mapping to paging priority indicator (PPI) used to provide unique paging policies per PPI value received in the DDN from MME.

Prior to implementation of this feature, the provisioned range of QCIs that can be mapped to PPI are limited to QCI1 - QCI9. With this feature, the following QCIs are added:

- QCI65: GBR mission critical push to talk voice (MCPTT)
- QCI66: GBR non-mission critical push to talk voice
- QCI69: non-GBR mission critical delay sensitive signaling service
- QCI70: non-GBR mission critical data

It is possible to use separate paging policies for each of the new QCIs.

For more information on PPI paging, see *Paging discrimination by Paging Priority Indication (Feature m11004-04)* and 3GPP TS 23.401 Release 13.0, section 4.9.

3.7.9 MME support for QCI 67 to support push-to-talk video (MCVideo) (Feature f10220-02)

With this feature, the MME supports QCI 67 as specified in 3GPP Rel 15 for the push-to-talk video.

The following QCIs are already supported in *Extending PPI paging to include QCI 65, 66, 69, and 70 (Feature f10201-02)*:

- QCI65
- QCI66
- QCI69
- QCI70

In this feature, the MME supports and complies with 3GPP-specified QCI value 67 for the GBR mission critical video service. The MME validates and checks the received QCI values from the network during the network-initiated bearer setup procedure. Handling of the invalid QCI does not change the current behavior. These QCI values are only assigned upon the request from the network side.

The UE and any application running on the UE are not allowed to request this QCI value. If the UE requests any of the specified QCI values, the request is rejected with the ESM cause #59 'Unsupported QCI value'.

3.7.10 MME support for Assistance Data for Recommended Cells (Feature f10221-01)

The MME will include the Assistance Data for Recommended Cells IE in the Paging message if Information on Recommended Cells and eNBs for Paging IE is received within the UE Context Release Complete message.

The feature supports Information on Recommended Cells and eNBs for Paging IE within the UE Context Release Complete message. When the MME triggers paging of a UE after the reception of the UE Context Release Complete with the Information on Recommended Cells and eNBs for Paging IE, the MME will include the Assistance Data for Recommended Cells IE in the Paging messages sent to the eNBs for that UE.

The global parameter `supportAsstData` controls this functionality. The default value is `No` (disabled).

3.7.11 Paging gap control based on paging type (Feature f10202-01)

This feature introduces additional control over existing MME paging gap feature that suppresses MME paging of UEs with three or more consecutive paging failures; for example, UEs that cannot be reached currently. With this feature, operators can specify that the paging gap feature is not applied for specific paging types or an alternate paging timer interval is used for specific paging types.

The MME supports automatically suppressing the of paging of UEs for which consecutive paging failures occurred. If three or more consecutive MME call processing procedures failed for the UE that cannot be reached, the MME paging of this UE will be suppressed for the duration specified by timer `pagingGapTimer`.

This feature provides more control over the paging gap functionality. The `pagingPolicy` database records can be configured to suppress the paging gap functionality for specific paging types. In addition, the `pagingPolicy` database records can be configured to override the value of timer `pagingGapTimer` for specific paging types.

This additional control allows operators to direct the MME to proceed with UE paging for

specific high priority paging types even if the MME could not reach the UE recently.

For example, an operator can update the pagingPolicy database records for Basic_QCI_5 paging type to suppress the paging gap functionality when that paging type is used. As a result, a UE would be paged when using Basic_QCI_5 even if there is a pattern of unsuccessful paging operations for that UE. This might be done because the Basic_QCI_5 paging type is used in their 4GLTE network for VoLTE calls and the operator has determined that maximizing voice call completion justifies any additional MME paging message traffic that may result from this change.

Alternately, an operator can choose to update the pagingPolicy database records so that a smaller value of timer pagingGapTimer is used for a specific paging type.

For example, the operator can opt to set the override paging gap timer to 5 minutes for the Basic_QCI_6 paging type while the general value of timer pagingGapTimer is set to 15 minutes.

The following paging types can be controlled by the paging gap control feature:

- Basic
- Basic_QCI_1 to Basic_QCI_9
- CoverageEnhancement
- LPA
- NB_EDRX_2 to NB_EDRX_15
- PGWRestart
- PPIO to PPI63
- Restricted
- UELB_PAGING
- UeMoinitLocationPaging
- UserDefPaging1 to UserDefPaging6
- WB_EDRX_0 to WB_EDRX_13

3.7.12 MME support for enhanced condition to trigger page gap timer (Feature f10227-01)

This feature enhances the paging gap functionality. The trigger for starting suppression of the MME paging was three consecutive failed procedures due to an inability to reach a UE with paging. With this feature, the number of consecutive failed procedures needed to trigger suppression of the MME paging can be modified using the new global parameter `pagingGapFailCountTrigger`.

The global parameter `pagingGapFailCountTrigger` can be modified to adjust the criteria for triggering the automatic suppression of the MME paging. The default value is 3. The value ranges from 1 to 5. In general, the paging gap functionality is triggered more often by an MME when this global parameter `pagingGapFailCountTrigger` is set to a lower value. When this global parameter `pagingGapFailCountTrigger` is set to a higher value, the paging gap functionality is triggered less often.

For example, if the global parameter `pagingGapFailCountTrigger` is set to 2, then the suppression of the MME paging is triggered after two or more consecutive MME call processing procedures have failed because the UE cannot be reached. Similarly, if the global parameter `pagingGapFailCountTrigger` is set to 5, then the suppression of the MME paging is triggered after five or more consecutive MME call processing procedures have failed because the UE cannot be reached.

3.7.13 Pre-emption of paging by overlapping DDN (Feature f10224-01)

With this feature, the MME supports downlink data notification (DDN) pre-emption in addition to the high priority paging for the MPS.

When the MME receives a DDN message while processing another ongoing DDN procedure, by default, the MME rejects the request by responding with a DDN ACK message with a cause of `S11_CAUSE_UNABLE_TO_PAGE_UE` (0x54). When a DDN message has high priority access, such as the MPS, the DDN message is allowed to pre-empt the ongoing DDN procedure and the MME accepts the second DDN and responds with a DDN ACK message with a cause of `S11_CAUSE_REQ_ACPT`.

Before this feature, the MPS DDN pre-emption was the only form of DDN pre-emption supported by the MME.

With this feature, the service provider can configure paging policy records to specify cases in which DDN pre-emption is supported based on the paging type. DDN pre-emption control is supported via the `preemptionLevel` parameter of the `pagingPolicy` command.

 **Note:**

An MPS DDN procedure still pre-empts any ongoing non-MPS DDN procedure. This means that DDN procedures with high priority paging for the MPS have the highest pre-emption level.

A DDN procedure pre-empts paging for a previous DDN procedure if the paging pre-

emption level of the paging policy associated with the DDN is higher than that for the previous DDN procedure.

When a new DDN pre-empts an ongoing DDN procedure, the MME responds with a DDN ACK message indicating “request accepted”. However, the ongoing paging operation is only restarted that is, proceed with attempt 1 for the new paging type, if the new DDN is associated with a paging type that would immediately trigger more aggressive paging. For example, if the ongoing paging operation is currently using the `LastSeenTAI` paging method, there is no benefit to restart the paging operation and use the less aggressive `LastSeenENBList` paging method.

On the other hand, if the ongoing paging operation is using the `LastSeenENB` paging method, restarting the paging operation to use the more aggressive `LastSeenTAI` paging method could result in reaching the UE sooner.

If the MME determines that restarting the paging operation to use the new paging type would not result in immediate use of more aggressive paging, the existing paging operation is allowed to continue.

The T3413 timer determines how long an ongoing DDN procedure is present.

3.7.14 MME support for paging when cause code received in UE Context Release Request with cause code = Inter-RAT Redirection (Feature f10226-01)

This feature enables the MME to allow paging to continue in the event that the MME receives a Downlink Data Notification message after handling of a UE Context Release Request with cause code "Inter-RAT Redirection".

In the feature, the following flow is covered:

1. In the event that the MME receives a Downlink Data Notification message after handling of a UE Context Release Request message with cause code "Inter-RAT Redirection", the MME allows paging to continue.
2. The MME is provisioned with the global parameter

`pagingAfterInterRatRedirection` to control whether the MME allows paging to continue. By default, the global parameter `pagingAfterInterRatRedirection` is disabled. When this parameter is enabled and the MME receives a Downlink Data Notification message, the MME allows paging to continue after handling of a UE Context Release Request with cause code "Inter-RAT Redirection".

3.7.15 MME support for paging upon T-ADS received in IDR message (Feature f10228-01)

This feature introduces MME support for paging upon receiving the terminating access domain selection (T-ADS) in the Insert Subscriber Data Request (IDR) message.

If the UE is in a 4G network while in EMM-REGISTERED or EMM-IDLE state, the MME answers with the Insert Subscriber Data Answer (IDA) message (with IMS-Voice-Over-PS-Sessions-Supported: SUPPORTED (1)) and starts immediately paging of the UE. The MME does not wait for the Downlink Data Notification (DNN) message from the S-GW to page the UE since the UE will be already in EMM-CONNECTED state and the Session Initiation Protocol (SIP) message will be delivered to the UE. The basic_QCI_5 paging type is used.

The feature is controlled by the `pagingUponTadsReceived` global parameter, which is by default disabled.

 **Note:**

There is no change to the current MME logic to determine the value of the IMS-Voice-Over-PS-Sessions-Supported AVP in the IDA message. If the AVP value is one, the MME immediately starts paging if the T-ADS bit is set in the IDR message. If the AVP value is zero, the MME does not start paging even if the T-ADS bit is set in the IDR message.

3.8 Tracking area management

Features related to tracking area management and the tracking area update procedure.

3.8.1 Intra-MME tracking area update (Feature m10001-01)

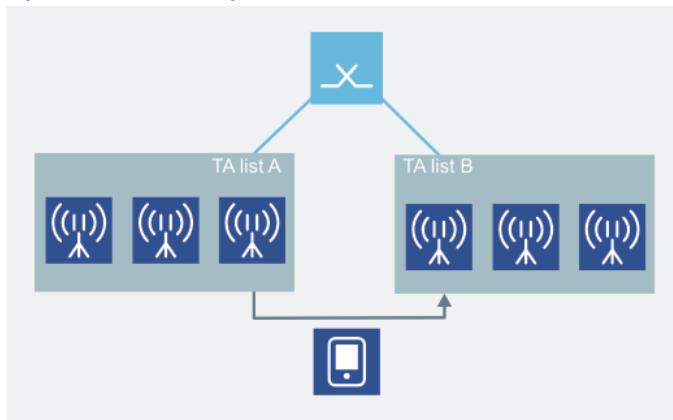
With the *Intra-MME tracking area update* feature, the MME can get information on the UE's location when the UE is in idle state.

The UE knows the tracking area it currently belongs to by listening to the channel that the eNB broadcasts. It contains the tracking area identity (TAI) code.

Upon registering to an LTE network, the MME provides the UE with a tracking area (TA) list.

When the UE moves within the LTE network, it is possible that the UE cannot hear any of the eNBs that broadcast the TAIs assigned to it. In this case, the UE initiates a tracking area update (TAU) procedure. This triggers the MME to update the UE with a new TA list containing new TAIs.

Figure 10: Tracking area update



The UE also triggers periodic tracking area updates to maintain registration when it is not moving and is in idle state.

Multiple eNBs can belong to a single tracking area.

A subscriber has reliable access to the network while moving and the network can reach it.

3.8.2 Static tracking area lists (Feature m10001-02)

The *Static tracking area lists* feature makes it possible to manage the tracking area (TA) lists that are delivered to the UE and to register the UE under multiple TAs in the MME.

The list is delivered to the UE in the attach and tracking area update (TAU) procedures based on the current TA. The list is not updated or delivered to the UE in a periodic TAU procedure. The UE is able to roam within the TAs delivered to it in the TA list without doing a TAU.

Operators can register UEs in multiple TAs and thus minimize the amount of TAU signaling even though TAs are small. However, a significant increase in paging signaling can result from using this feature. UEs will be paged by all eNBs of neighboring TAs (in addition to all eNBs of the current TA) whenever the `LastSeenTAINBTAI` paging method is used.

Command `taiNb` is used to provision the statically defined tracking area lists by specifying neighbor relationships between TAIs. The provisioned neighbor TAIs of the UE's current TAI will be included in the UE's tracking area list if the following conditions are met:

- global parameter `includeNeighborListInTaiList` is set to `Yes`

- neighboring TAI is compatible with UE's current TAI (for example, supports the same feature set).



Use of static tracking area lists is generally not recommended. Please consult with Nokia technical support before using this feature. Misuse of static tracking area lists can trigger a significantly higher MME paging traffic level and lead to an overload condition on the MME or the eNBs or both.

3.8.3 Removing static provisioning of TAC on MME for eNB access (Feature m10916-01)

The **Removing static provisioning of TAC on MME for eNB access feature provides a capability to learn tracking area identities (TAIs) as the eNB sets up S1 connection to the MME as opposed to the method of pre-provisioning all TAIs serviced by the MME. It also removes cross-checks on TAIs using the pre-provisioned TAI table.**

The eNB's role is a client in the relationship with the MME. This means that the eNB initiates initial communication and link establishment with the MME through the S1 setup procedure (3GPP TS 36.413).

In the S1 setup procedure, the eNB sends the following information to the MME:

Table 12: IEs sent to MME in S1 setup procedure

Message Type	M
Global eNB ID	M
eNB Name	O
Supported TAs	
>TAC	M
>Broadcast PLMNs	
>>PLMN Identity	M
Default paging DRX	M
CSG Id List	
>CSG Id	M

Before the implementation of this feature, the MME validates two items to successfully complete the procedure:

- Broadcast public land mobile networks (PLMNs): the MME checks this against locally provisioned home/shared PLMN. If it exists, the procedure continues, otherwise the MME sends S1 Setup Failure in response to the S1 Setup Request from the eNB.
- Supported tracking areas (TAs): the MME checks this against locally provisioned list of valid TAs. If it exists, the procedure continues, otherwise the MME sends S1 Setup Failure in response to the S1 Setup Request from the eNB.

This feature maintains the PLMN check, but if this feature is enabled (through provisioning), then if the eNB includes a TA unknown to the MME in the S1 Setup Request, the MME dynamically adds the TA to its list of TAs and successfully completes the S1 setup procedure.

There are a number of additional (or subtended) parameters the MME must know about a particular TA:

Table 13: Information elements (IEs) sent to TA parameters

Parameter	Description	Default
esmlc-1	Identity of primary Enhanced Sending Location Mobile Center for location services	No
esmlc-2	Identity of primary Enhanced Sending Location Mobile Center	No
esmlc-selectionalgorithm	Selection algorithm for selecting Enhanced Sending Location Mobile Center	primary-secondary
ims	Whether IMS services are enabled for the TA	No
emergency support	Whether E911 emergency services are enabled for the TA	No
time-zone	Time zone offset from MME time zone	MME time zone

Even though this feature allows a TA to be dynamically added to the list of TAs maintained in the MME, there is no way (non-proprietary) for the MME to auto-discover the additional parameters. When the MME auto-adds a TA, it sets these parameters at default values.

The operator must update these values with valid ones for the new TA to support normal service.

The main impact of this feature is to ensure that even in cases where new TAs are provisioned in eNBs before the MME, the S1 setup procedure is successful. Subsequent provisioning in the MME does not force rework in eNBs.

The MME is able to rely on the S1 auto-configuration method. Newly provisioned eNBs are also operable for basic service without configuring the new TA on the MME.

3.8.4 Basic and enhanced automatic neighbor list generation (Feature m10210-02, m10210-03)

Enhancements to the MME mobility management and paging are introduced to reduce ping-ponging scenarios at tracking area (TA) border areas. The *Basic and enhanced automatic neighbor list generation* feature reduces excessive network signaling because of re-registration that is tracking area update (TAU).

Ping-ponging is used to describe a situation in which UEs at the border of TAs would rapidly switch between cells located within adjacent TAs and thereby generate a high level of TAU Requests. These enhancements use the following tracking area identity (TAI) fields within the

UE context to record the UE mobility history:

- Last seen TAI:

This is the TAI received in the S1-AP message and set at the successful or failed completion of a mobility management or session management procedure. This is an existing UE context data field.

- Old last seen TAI:

This is the TAI where the UE was located before the last seen TAI. Whenever the last seen TAI field for a UE is changed to a new value, the old last seen TAI field is set to the previous value of the last seen TAI field.

- Last registered TAI:

This is the saved Last seen TAI value that is set at the successful completion of an attach or TAU procedure. This field of the UE context is used by the MME paging to reconstruct the set of TAs where the UE is currently registered. This value is preserved until the completion of the next successful attach or TAU procedure.

- Old last registered TAI:

This is the saved Old last seen TAI value that is set at the completion of an attach or TAU procedure. This field of the UE context is used by the MME paging to reconstruct the set of TAs where the UE is currently registered. This value is preserved until the completion of the next successful attach or TAU procedure.

These enhancements avoid the ping-ponging effect by automatically including the current TAI in the Attach Accept and current TAI and the previously seen TAI in the TAI list that is sent to the UE in the TAU Accept messages.

Note that additional TAIs are added to the TAI list if a TAI neighbor list is provisioned for the Last seen TAI. Also note that the previously seen TAI (that is, the Old last seen TAI) is not added to the TAI list for the following cases:

- A circuit-switched fallback (CSFB) capable UE that is registered with combined attach if the TAI is in a different location area (LA)
- Whenever the S-GW relocation occurs because of a UE moving to a new TA. If previously seen TAI is added to the TAI list, an idle UE does not send a TAU Request if it moves to the previously seen TAI. As a result, S-GW relocation does not happen causing potential failure of UE sessions as eNB in the TA might not have connectivity to the S-GW.

The last seen TA and neighboring TAs paging method is also enhanced to page eNBs associated with the Last registered TAI, the Old last registered TAI, and the Last seen TAI. This change is necessary to ensure that this paging method pages the UE in all of the TAIs where the UE is registered.

 Note:

Operators must select the last seen TA and neighboring TAs paging method in their MME paging policy to ensure that UEs moving to a neighboring TA are paged at their present location.

 Note:

Operators must ensure that provisioned TAI neighbor list only contain TAIs that can be serviced by the same S-GW. If a provisioned TAI neighbor list contains TAIs serviced by a different S-GW, the UE does not send a TAU Request when it moves from TAI serviced by a S-GW to another TAI serviced by a different S-GW resulting in no S-GW relocation causing potential UE session failures.

An additional enhancement (m10210-03) is added to this functionality to eliminate ping-ponging between three adjacent TAs.

This feature expands the list of registered TAs sent to the UE within TAU Accept messages to automatically include an additional TAI if cyclical movement among three TAs is detected. Similar to the *Basic automatic neighbor list generation* (m10210-02) feature, this feature also enhances the last seen TA and neighboring TAs paging method to ensure that the UE is paged within all TAs where it is registered when using this paging method. This feature introduces two fields, Previous old seen TAI and Previous old last seen registered TAI, in addition to the Last seen TAI, Old last seen TAI, Last registered TAI, and Old last registered TAI fields introduced by the *Basic automatic neighbor list generation* feature.

- Older last seen TAI:

The Older last seen TAI field is set to the Old last seen TAI value only when the last seen TAI field is set to a value that is different from the existing Last seen TAI and Old last seen TAI values to detect cyclical movement of UE between three TAIs.

- Older last registered TAI:

This field is set to the Old last registered TAI value if cyclical movement is detected between three TAs. The field is not used if Automatically add TAI to the TAI list parameter is set to None or Basic. This field of the UE context is used by the MME paging to reconstruct the set of TAs where the UE is currently registered. This value is preserved until the completion of the next successful attach or TAU procedure.

In addition to these parameters, the feature introduces provisioning of two parameters to allow control over the *Basic automatic neighbor list generation* and *Enhanced automatic neighbor list generation* features.

The parameter `autoAddTaiToTaiList` is used to control if tracking areas are automatically added to the registered tracking area list based on UE mobility history.

The parameter `includeNeighborListInTaiList` is used to include or exclude the provisioned TAI neighbor list in the TAI list sent in the Attach Accept and TAU Accept messages. If this parameter has the value `Yes` (default), the MME includes the provisioned set of neighbor TAIs in the list of TAIs that is sent to the UE when the UE registers at the MME (attach or TAU). If this parameter is set to `No`, the MME includes only the last seen TAI in the list of TAIs sent to the UE.

3.8.5 Automatic neighbor list generation for up to three TAs (Feature m10210-05)

The *Automatic neighbor list generation for up to three TAs* feature reduces the potential increase in signaling load and extends UE battery life by suppressing tracking area update (TAU) at tracking area (TA) borders when UEs bounce back and forth from adjacent eNBs because of poor coverage.

This feature adds a third mode to the existing automatic neighbor list generation functions. Where the UE can move across borders of up to three TAs without TAU based on the following (general) criteria without a detection of cyclical movement between TAs:

- older TAs' voice over long-term evolution (VoLTE) parameters (IMS voice over PS session indicator `imsSupported` and emergency bearer services indicator `emergencySupported`) provisioning matches the current TA
- older TAs have the same time zone as the current TA
- older TAs map to the same location area identification (LAI)
- older TAs are served by the same S-GW

These criteria apply to all of the different automatic neighbor list generation options (off, basic, enhanced, and update-three). However, unlike the others, the update-three option does not require detection of cyclical behavior of the UE between TAs.

Note:

Per 3GPP TS 24.301 section 9.9.3.21A, the external provisioning system (EPS) network feature support information element identifier (IEI) includes evolved packet core-location services (EPC-LCS) (not supported by CMM), emergency bearer services indicator (EMC BS), and voice over PS session indicator (IMS VoPS IMS).

Figure 11: EPS network feature support IEI

8	7	6	5	4	3	2	1
EPS network feature support IEI							
Length of EPS network support contents							
0	0	ESR PS	CS-LCS	EPC- LCS	EMC BS	IMS VoPS	
Spare							

In addition to the time zone and location area (LA) matching to the prior TA, the MME uses EMC BS and IMS VoPS to match VoLTE parameters.

This feature is controlled through the `autoAddTaiToTaiList` global parameter:

- If this parameter is set to value `Off`, the MME does not add tracking area identities (TAs) to the registered tracking area list based on a UE's mobility pattern.
- If this parameter is set to value `Basic`, the MME includes the previously visited tracking area and the current tracking area in the registered tracking area list sent to the UE within the TAU Accept message when cyclic movement between two tracking areas was detected for the current TAU procedure. This is the default value.
- If this parameter is set to value `Enhanced`, the MME includes also the two previously visited tracking areas and the current tracking area in the registered tracking area list sent to the UE within the TAU Accept message when cyclic movement between three tracking areas for the current TAU procedure.
- If this parameter is set to value `Update-three`, the MME adds the tracking area where the general criteria are met and no cyclical behavior is detected.

When a UE moves to a tracking area that does not meet these criteria, the MME sends only the new (current) tracking area to the UE.

This functionality applies to UE's in both ECM-IDLE and ECM-CONNECTED states.

3.8.6 Idle mode TAU handling enhancements (Feature m10144-02)

With the implementation of the *Idle mode TAU handling enhancements* feature, the MME enhances the current handling of inter radio access technology (IRAT) tracking area update (TAU) when the old S4-SGSN does not send the S-GW IPv6 S1-U Fully Qualified Tunnel End Point Identifier (FTEID) in the S3 Context Response message.

This enhancement involves saving the S-GW S1-U IPv4 and IPv6 addresses received in the S11 Modify Bearer Response and storing them in the UE bearer context so that a subsequent service request received from the eNB supporting IPv6 S1 interface succeeds.

The feature reduces IRAT handover failures.

3.8.7 Operator controlled TAU suppression (Feature m10215-01)

The **Operator controlled TAU suppression** feature reduces signaling because of tracking area update (TAU) requests when a UE is toggling between tracking areas (TAs).

This feature provides tuning for suppression of TA border crossing TAU when, because of poor coverage, the UE cyclically registers back and forth between adjacent TAs.

If the UE is located near the boundary between eNBs, the UE can rapidly switch between the eNBs as the signal strength fluctuates. If eNBs are associated with different tracking areas, this switching between the eNBs can generate many unnecessary TAU procedures. This unwanted behavior is commonly referred to as toggling or ping-ponging.

TAU suppression at tracking area borders occurs when the MME detects cyclical UE movement between neighboring tracking areas. This mechanism stops many unnecessary TAUs from UEs that are toggling, but it can also trigger TAU suppression when the UE makes a round trip that crosses a tracking area boundary. Because TAUs can trigger the MME to update the time zone information in the UE, unnecessary TAU suppression has the unintended consequence that time zone information updates to the UE are also suppressed.

This feature allows the operator to provision an MME timer parameter that indicates the maximum time interval for movement between TAs that triggers the MME's TAU suppression mechanism. The end result is that the feature optimizes the TAU signaling load by suppressing updates because of UE toggling between tracking areas while providing timely time zone updates to UEs that are truly moving between the tracking areas.

This feature also allows the operator to provision an alternate T3412 timer value to be used when the MME detects a toggling UE and automatically adds one or more tracking area identities (TAIs) to the registered tracking area list sent to the UE in the TAU Accept message to suppress future TAU procedures between the affected tracking areas.

This feature is an enhancement of the *Enhanced automatic neighbor list generation* feature. The original feature is controlled through the `autoAddTaiToTaiList` global parameter. The possible values of this parameter are:

- Off:
No TAIs are added to the registered tracking area list based on a UE's mobility pattern.
- Basic:
The previously visited tracking area and the current tracking area in the registered tracking area list sent to the UE. This is the default value.

- Enhanced:

The MME includes also the two previously visited tracking areas and the current tracking area. This is required for the cyclic movement between three tracking areas.

The original feature also supports the inclusion of provisioned TAIs that were manually provisioned for the Last seen TAI within the TAI neighbor list if the Include neighbor list in TAI list global parameter is set to True. Operators are advised to only provision the TAI neighbor list to address unique cases that cannot be adequately addressed by the *Automatic neighbor list generation* feature. In most cases, the TAI neighbor list is expected to be empty.

Since the introduction of the *Enhanced automatic neighbor list generation* feature the following areas for improvement have been identified:

1. TAU suppression occurs for any cyclic movement between tracking areas, not just rapid toggling between tracking areas.
2. Unnecessary TAU suppression can result in unintended suppression of time zone updates for UEs and higher paging traffic levels.
3. TAU suppression does not occur while the UE is in connected mode.

This feature provides the following solutions to the issues listed above:

1. This feature allows the service provider to determine the cyclic movement interval that is deemed to be rapid toggling and the MME triggers TAU suppression only when this type of movement is detected.
2. Because the MME triggers only TAU suppression if the cyclic movement observed meets the rapid toggling threshold, the issues of unintended suppression of time zone updates for UEs and higher paging traffic levels should be largely eliminated. Note that the setting of the rapid toggling threshold by the operator is an explicit trade-off between TAU signaling load and ignoring the side effects of TAU suppression (for example, missing time zone updates, possible heavier paging).
3. TAU suppression can now be triggered for UEs in either connected or idle mode.

Note:

This feature's support for an alternate T3412 timer interacts with *Periodic TAU timer override at attach* feature that provides the MME capability to override the local provisioned T3412 timer if Subscribed-Periodic-RAU-TAU-Timer as defined in 3GPP TS 29.272 is present and received as part of subscription data/profile from the HSS and is subsequently passed on to devices. The objective of the *Periodic TAU override at attach* feature is to improve a UE reachability and to allow the support for customized T3412 timer per IMSI or device profile. This capability can also be used to reduce the frequency of TAU procedure for machine type communications.

Specification

The MME supports provisioning of a TAU suppression threshold timer value. This timer indicates the maximum time interval for returning to a previously visited tracking area that should trigger TAU suppression. The allowed values are:

- 0 (indicating TAU suppression is not affected by interval of cyclic movement)
- 1 to 300 seconds (indicates maximum interval triggering TAU suppression)

The default value for this timer is 0. The recommended value is 180 (3 minutes).

The MME supports provisioning of a T3412 timer with TAU suppression timer value. This parameter indicates the T3412 timer value to be sent to the UE in a TAU Accept message if the MME is the source of the T3412 timer value and TAIs were automatically added to the registered tracking area list.

Allowed values are 0 to 31 seconds. The default value is 0 which indicates that the standard T3412 timer value should be used.

The MME records when the Last seen TAI was updated for each UE (that is, maintains a timestamp of when the Last seen TAI field was set). The MME also maintains timestamps of when the UE visited the Old last seen TAI and the Older last seen TAI.

The MME effectively tracks UE movement between tracking areas for all evolved packet system mobility management (EMM) procedures and records if rapid cyclic movement has occurred within an interval of time that is less than or equal to the TAU suppression threshold timer value.

Note:

The MME previously only attempted to detect cyclic movement between tracking areas during the TAU procedure.

Note:

Because timestamps cannot be preserved during control plane processing services (CPPS) switchovers, the MME is not required to detect rapid UE movement between tracking areas when that movement occurred before a CPPS switchover. Similar constraints already exist for features such as the *Paging gap* feature and the detection of extended UE inactivity.

When a TAU procedure is processed by the MME, the MME augments the preexisting TAU suppression mechanism as follows if the TAU suppression threshold timer is set to a nonzero value:

- If the MME detects no cyclic movement between tracking areas, only the Last seen TAI (and any provisioned neighboring TAIs from the TAI neighbor list) are included in the registered tracking area list transmitted to the UE in the TAU Accept message.
- If the MME detects cyclic movement between tracking areas (that is, A→B→A or A→B→C→A) as a result of the current TAU procedure and the interval since the start of the cycle (as determined by the Old last seen TAI timestamp or Older last seen TAI timestamp) is less than or equal to the TAU suppression threshold timer value, the TAIs involved in the cyclic movement are included in the registered tracking area list transmitted to the UE in the TAU Accept message. In this case, the reported movement is treated as abnormal toggling (or ping-pong) and TAU suppression is engaged by automatically adding the TAIs involved in toggling to the registered tracking area list.
- If the MME detects cyclic movement between tracking areas as a result of the current TAU procedure and the interval since the start of the cycle (as determined by the Old last seen TAI timestamp or Older last seen TAI timestamp) is greater than the TAU suppression threshold timer value, then only the Last seen TAI (and any provisioned neighboring TAIs from the TAI neighbor list) are included in the registered tracking area list transmitted to the UE in the TAU Accept message. In this case, the movement is treated as normal UE movement. TAU suppression is not engaged in this case. No additional TAIs are automatically added to the registered tracking area list.
- If cyclic movement between the tracking areas was detected by the MME during other procedures that update the MME's knowledge of the UE location (for example, handover) before the current TAU procedure, the TAIs involved in the cyclic movement are included

in the registered tracking area if the following conditions are present:

- The TAI reported by the current TAU Request is one of the TAIs involved in the cyclic movement.
- The interval since the start of the cycle (as determined by the Old last seen TAI timestamp or Older last seen TAI timestamp) is less than or equal to the TAU suppression threshold timer value.
- If either of the above conditions are not met, only the Last seen TAI (and any provisioned neighboring TAIs from the TAI neighbor list) are included in the registered tracking area list transmitted to the UE in the TAU Accept message.

Note:

The default TAU suppression threshold timer value is 0. A value of 0 causes the MME to do TAU suppression.

If the TAU suppression threshold timer value is set to 0, the MME utilizes the preexisting TAU suppression mechanism. In this case, TAIs are automatically added to the registered tracking area list regardless of the interval of the cycle. Furthermore, TAU suppression is only engaged when the cyclic movement is detected during a TAU procedure.

3.8.8 Rejecting node relocating TAU with update type periodic (Feature m10155-01)

The *Rejecting node relocating TAU with update type periodic* feature addresses scenarios of a combined-attached UE in which the new MME does not send a location update to MSC/VLR for a tracking area update (TAU) request with update type periodic and foreign globally unique temporary identity (GUTI).

One such scenario is as follows: A UE sends TAU request with update type periodic but the S1-MME link to the MME upon which the UE is registered is down. The request is routed by the eNB to another MME in the pool, where an inter-MME TAU procedure is executed.

Normally an inter-MME TAU procedure has a TAU Request with update type tracking area (TA) updating and the UE indicates whether the request is combined TA/location area (LA) updating (which triggers the MME to send Location Update over SGs to the MSC) or evolved packet system (EPS) only (in which case the MME does not send a Location Update).

Normally, TAU Request with update type periodic is not a trigger for sending Location Update to the MSC.

In such scenarios, the current MME behavior results in the UE becoming registered on the

new MME but without the MSC being notified. For a combined-attached UE this results in failure to deliver voice calls and text messages to the UE.

With this feature enabled, the MME sends TAU Reject when the TAU Request has update type periodic and the GUTI is foreign. This forces the UE to send an Attach Request and that triggers the MME to send Location Update to the MSC based on attach type.

The feature improves data synchronization on combined attach.

3.8.9 UE activity notification (Feature m10105-01)

The *UE activity notification* feature provides the MME with the ability to send UE-activity-notification message to the HSS about the UE reachability if the UE subscription data contains the URRP-MME flag set by a previous request of the HSS.

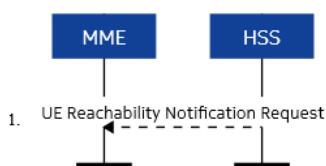
This feature supports following two messages:

- HSS to MME: UE- Reachability-Notification-Request (URRP-MME)
- MME to HSS: UE-Activity-Notification

UE reachability notification request procedure

The UE reachability notification request procedure is shown in the figure.

Figure 12: UE reachability notification request procedure

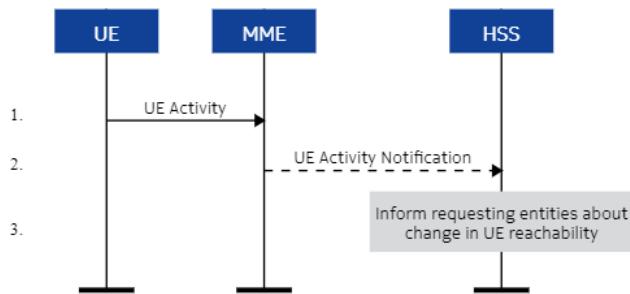


1. If a service-related entity requests the HSS to provide an indication about the UE reachability on the evolved packet system (EPS), the HSS stores the service-related entity and sets the URRP-MME parameter to indicate that such request is received. If the value of the URRP-MME parameter has changed from Not set to Set, the HSS sends a UE-REACHABILITYNOTIFICATION- REQUEST (URRP-MME) to the MME. If the MME has a mobility management (MM) context for that user, the MME sets URRP-MME to indicate the need to report to the HSS information about changes in the UE reachability, for example, when the next non-access stratum (NAS) activity with that UE is detected.

UE activity notification procedure

The UE activity notification procedure is shown in the figure.

Figure 13: UE activity notification procedure



1. The MME receives an indication about the UE reachability, for example, an Attach Request message from the UE or the MME receives an indication from the S-GW that the UE has done a handover to the non-3GPP coverage.
2. If the MME contains an MM context of the UE and if URRP-MME for that UE is configured to report once that the UE is reachable, the MME sends a UE-Activity-Notification (IMSI, UE-Reachable) message to the HSS and clears the corresponding URRP-MME for that UE.
3. When the HSS receives the UE-Activity-Notification (IMSI, UE-Reachable) message or the Update Location message for an UE that has URRP-MME set, it triggers appropriate notifications to the entities that have subscribed to the HSS for this notification and clears the URRP-MME for that UE.

3.8.10 Configuration of MME relative capacity per tracking area (Feature m10725-01)

The *Configuration of MME relative capacity per tracking area* feature supports provisioning of MME relative capacity per tracking area to implement a configuration of primary and secondary MMEs within an MME pool without any eNB configuration changes.

All the eNBs in a tracking area (TA) get the MME relative capacity provisioned for that TA either through a S1 Setup Response or MME Configuration Update. The MME uses the default MME relative capacity if a TA is not provisioned with the relative capacity.

This feature also includes capability to provision TA-related parameters for a range of TAs, all TAs, or a saved TA list including:

- IMS voice
- Emergency

- E-SMLC (whether they will load share or function as primary/secondary)
- S-GW pool id
- Relative capacity
- Time zone

The following can be provisioned:

- Enable/disable the feature
- Relative capacity per tracking area
- Selection of maximum or minimum tracking area identity (TAI) capacities of TAI supported by an eNB
- Updating an attribute for all or a subset of TAIs

If this feature is activated, the MME sends the MME relative capacity in S1 Setup Response message if the auto-adjust capacity is enabled.

If the auto-adjust capacity is not enabled, the MME sends either maximum or minimum of provisioned relative capacities of all the TAIs supported by the eNB.

The MME sends the provisioning change to the MME relative capacity in the MME Configuration Update in less than 180 seconds to all the eNBs requiring an update for the following cases:

- Auto-adjust capacity is disabled from enabled: the MME sends the relative capacity to all the eNBs in the tracking area if the tracking area relative capacity is different from the node level capacity and if the feature is enabled.
- Auto-adjust capacity is enabled from disabled: the MME sends the node level capacity to all the eNBs.
- Tracking area relative capacity is changed: the MME sends relative capacity of the tracking area to all the eNBs in the tracking area if the feature is enabled and the auto-adjust capacity is disabled.

The MME relative capacity maximum value per tracking area cannot be greater than the node level MME relative capacity.

If the feature is disabled and also if the auto-adjust capacity is disabled, the MME sends the relative capacity provisioned for the MME to only those eNBs that require updates. Similarly, if this feature is activated, the MME sends the relative capacity to only the eNBs that require updates.

Operator is able to direct users on certain areas into specific MME(s) in the pool. The pool balancing can be done on the area basis.

3.8.11 TAI/LAI mapping so that MME can select LAI from PLMN not matching UE PLMN (Feature f11811-01)

This feature supports mapping of an operator's TAIs to another operator's LAI so that TAI mapping can select LAI even if LAI PLMN ID does not match the UE PLMN ID.

The feature applies when the MME selects an MSC for combined attach or TAU. The MME has provisioning to map its own TAI to an LAI in another operator's network. This new LAI is included in the relevant SGs messaging to the target MSC.

The Sv interface is not affected by this feature. The eNB initiates the SRVCC handover procedure and includes the Target ID IE in the Handover Required message. The target ID includes the LAI (PLMN and LAC).

This feature is controlled by global parameter `supportNonhomeTaiLaiMapping` (by default, set to `No`). Provisioning of PLMN and TAI/LAI mapping is also required.

3.8.12 Adding default TAC mapping to TA discovery provisioned parameters (Feature f11813-01)

This feature adds support for default TAC mapping to TA discovery provisioned parameters and supports a wildcard TAC by enhancing the auto-discovery feature.

The MME uses the wildcard TAC if there is not a specific TAC match.

The wildcard TAC provisioning includes at least:

- esmic-1
- esmic-2
- esmic-selectionalgorithm
- ims
- emergency support
- time-zone

Location services (value added, operator or LI) are not applicable for this feature and will be set to standard auto-discovery defaults of off. The auto-population between the TAI and the LAI is not supported as part of this feature.

After creating a home or a shared PLMN, the corresponding `taiDiscoveryDefaults` record is auto-created regardless of the feature activation (global parameter `discoverTaiDefaults`) with the default values. This also applies to the deletion of the

records. You can modify, list or show the related `taiDiscoveryDefaults` records, but cannot create nor delete.

The following crosschecks are the same as they are in the `tai` command:

- `upClot` can only be enabled when `s1DataTrans` is enabled.
- `s1DataTrans` cannot be disabled when `upClot` is enabled.
- Parameters `esmlcIdentity1`, `esmlcIdentity2`, `esmlcIdentity3`, `esmlcIdentity4` of command `esmlc` must be configured.
- Parameter `vdpProfileName` of command `vdpProfile` must be configured.

Global parameter `discoverTaiDefaults` must be first disabled in order for global parameter `discoverTais` to be disabled.

Global parameter `discoverTais` must be first enabled in order for global parameter `discoverTaiDefaults` to be enabled.

When you try to delete a `vdpProfile` or an `esmlc` which is used by a `taiDiscoveryDefaults` record, the operation will fail. You must remove the corresponding reference on `taiDiscoveryDefaults` command related record in order to delete the record.

When `areaList` record is used by command `taiDiscoveryDefaults`, the `areaList` record cannot be deleted till `taiDiscoveryDefaults` record is modified.

If a profile template is updated after TAI(s) are auto-discovered, you need to either update those TAI(s) explicitly or force a data push using command `multiTacOperation`.

3.8.13 MME support for enhanced TA discovery auto-provisioning (Feature f11813-02)

This feature enhances the default TAC mapping to the TA discovery function implemented in feature f11813-01 by allowing the operator to configure a TA range profile that includes a TAC range.

The TA range profile re-uses many parameters from commands `tai`, `taiEsmlcList`, and `mmeGrpTai`. Once the feature is activated, and an eNB with an unknown TAC that is in a TAI range of a TA range profile connects, the MME automatically populates the corresponding `tai`, `mmeGrpTai`, and `taiEsmlcList` relations from the profile.

With this feature, the operator can configure a profile one time without changing any configuration in the MME as other TACs are added.

3.8.14 MME support for increased number of region TAC and LAC groups (Feature f80015-01)

This feature increases the maximum number of regions for TAC and LAC groups to 3000.

3.8.15 MME support for increased number of TAI of 20K (Feature f10567-01)

This feature supports increased number of TAI to 20K for the MME.

3.8.16 MME support for sending configuration update on data changes (Feature f10934-01)

This feature enables the operator to send the S1AP MME Configuration Update message to the eNBs on demand.

The MME supports updating a single eNB or all the eNBs with active links via an MME S1AP Configuration Update procedure with shared PLMNs and associated TAs when new shared PLMNs and associated TAs are provisioned on the MME. The update is achieved through the `s1ConfigUpdate` CLI command. When the MME sends a Configuration Update message to the eNB, it expects to receive an Update Acknowledgment Response message from the eNB. If the `mmeCnfgUpdate` timer expires while waiting for this response, the MME considers that this procedure has been failed.

The global parameter `s1SendAllServedPlmnsToEnb` controls whether the MME will include all the configured home and shared PLMN IDs in the PLMN list in the following cases:

- when the MME sends the S1AP Configuration Update message
or
- in the S1AP Setup Response message when the MME responds to the eNB S1AP Setup Request message

By default, the global parameter is disabled.

3.8.17 MME support for preserving VLR for sending NOR to HSS for SGSN to MME tracking area update procedure (Feature f10425-02)

With this feature, the MME preserves the UE subscription data in VLR at the end of the IRAT (source) mobility procedure so that the ULR procedure is skipped and the NOR procedure is performed in the next IRAT (target) mobility procedure.

The feature introduces a modification in the Gn/Gp SGSN to MME tracking area update procedure (both connected and idle mode) with the single registration flag, as specified in 3GPP TS 23.401, by sending the NOR message to the HSS.

Currently, the MME sends the ULR message to the HSS at the end of the TAU procedure. When this feature is enabled, the MME preserves the UE subscription data in the VLR at the end of IRAT (source) mobility procedure so that the ULR message is skipped in the next IRAT (target) mobility procedure and a NOR message is sent to the HSS. The feature is controlled by the global parameter `skipUlrForSgsnToMmeTau`. By default, the feature is disabled.

The feature is applicable to handover and TAU scenarios across Gn and S3 interface.

Additionally, the `reserveUeSubscriptionIratMob` timer is introduced to provision the duration of preserving the UE subscription data. Specifically, the UE's subscription data is kept until the timer expires. If the UE comes back before the timer expiration, the NOR message is sent to the HSS, instead of the ULR message, at the end of the SGSN to MME TAU procedure over Gn and S3 interface. Otherwise, the ULR message is sent. The timer restarts when the UE transitions back to the MME.

3.8.18 CMM support for multiple TAC operation trigger enhancements (Feature f14622-01)

This feature increases the maximum number of supported tracking areas in one operation to 2000.

The following command sets the maximum number of tracking areas:

```
cmm multiTacOperation modify --plmnName <string> --minTac <integer>
-- maxTac <integer> --lcsType {Operator,Value Added,LawfulIntercept}
```

3.8.19 MME support for combined attach without CS (Feature f10426-01)

This feature adds MME support for an option to provide a combined registration result (combined EPS/IMSI attach or combined TA/LA updated) for a provisioned IMSI range or UE PLMN/serving PLMN combination.

If a UE requests a combined attach/TAU from an MME that does not have access to the CS domain for the UE, the MME accepts the combined attach/TAU and provides a locally provisioned TMSI and non-broadcast LAI on the Attach/TAU accept. The MME internally maintains attachment information to avoid any issues, specifying that the UE is actually attached by EPS-only and is not really combined attached.

When this feature is enabled via a global parameter, the MME supports this option to fake a combined attach/TAU towards provisioned UEs by sending a combined attach/TAU result towards the UE without having the actual CS domain provisioned.

The MME supports a profile for each UE PLMN/serving PLMN combination or IMSI range, which includes a parameter to enable this feature's functionality for the UE, and the Extended Service request rejection cause.

The functionality to allow combined attached without the CS domain only applies when SGs is not enabled for the UE; that is, where the service agreement profile indicates "SGS none" for the "CS capability supported" value.

3.8.20 MME support for ignoring malformed PDN connection in mobility scenario(s) (Feature f13501-08)

With this feature, the MME ignores the malformed PDN connection(s), including the Services Capability Exposure Function (SCEF) PDN connection, received by the target MME node during the S10, S3 and N26 mobility procedure and allows the successful completion of the respective procedure.

During the handover or the tracking area update procedure where the MME acts as a target node, the MME allows the successful completion of the mobility procedure when at least one received PDN Connection IE (including the SCEF PDN connection) has been successfully decoded. The target MME will drop the PDN connection that failed decoding without any further impact in the procedure. This functionality applies to S10/S3/N26 mobility procedures where the source node may be a MME, an AMF or an S4-SGSN.

The feature is enabled by default.

Note:

- The tracking area update procedure continues when the attach without PDN connection is enabled for the UE even if all the received PDN Connection IEs are dropped.
- The PCMD record indicates that the PDN connection was dropped at the target MME due to some missing/incorrect mandatory/conditional fields.

3.9 Handovers

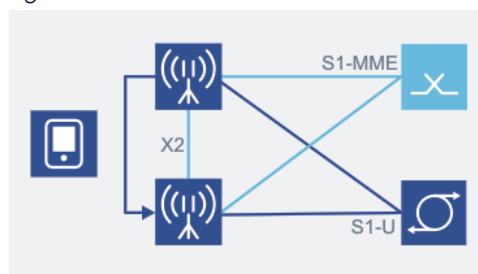
Features related to S1-based and X2-based handovers.

3.9.1 Mobility and intra-MME handover with X2 interface (Feature m10001-01)

With the **Mobility and intra-MME handover with X2 interface feature**, a subscriber can move between eNBs during an active data session, and the data path is maintained between the current eNB and the S-GW.

The handover is prepared and executed between the eNBs without involving the core network. During the handover, the source eNB acts as a temporary relay between the S-GW and the target eNB, forwarding user data. Once the handover has been executed over the radio access network, the MME is informed and it updates the data path between the target eNB and the gateway. Finally, the forwarding function of the source eNB is released.

Figure 14: Subscriber moves between eNBs



This feature enables undisturbed data transfer when a subscriber is moving.

3.9.2 MME-assisted S1-based eNB handoff (Feature m10900-01)

The MME-assisted S1-based eNB handoff feature provides a solution to a situation where eNBs are not interconnected with X2 and the Mobility and intra-MME handover with X2 interface feature cannot be used.

This feature supports intra-LTE S1-based handover procedures. The S1-based handover procedure is selected by the eNB if X2-based handover cannot be used. The S1-based handover requires the MME to forward messages between source eNB and target eNB and also select a new MME if the eNB is served by a different MME. For this feature, the MME supports the following handover scenarios:

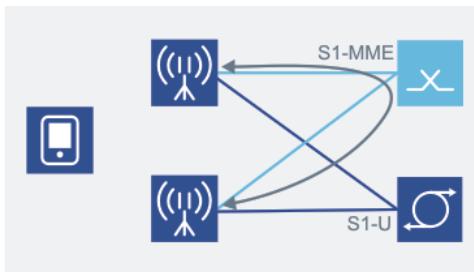
- Without the MME and S-GW relocation
- Without the MME relocation and with the S-GW relocation
- With the MME and S-GW relocation
- With the MME relocation and without the S-GW relocation

For all these scenarios, there can be two ways of data forwarding from the source eNB to the target eNB during the handover procedure: direct forwarding and indirect forwarding. The availability of a direct forwarding path is determined by the source eNB and indicated to the MME if X2 connectivity is available between the source and target eNBs. If there is no X2 connectivity, the source eNB indicates indirect data forwarding and the MME sets up an indirect forwarding path that is, the traffic is forwarded from the source eNB to the target eNB via the S-GW. The MME implementation always sets up indirect forwarding paths if both the source eNB and target eNB indicate indirect data forwarding.

The decision to relocate the MME is done by the source MME. If the target eNB is not in the source MME serving area then it selects an MME serving the area of the eNB.

The MME also determines (the target MME if the MME is relocated) whether the S-GW relocation is required or not. If the tracking area (TA) of the target eNB is not served by the S-GW, the MME selects another S-GW that is assigned to serve the TA.

Figure 15: Subscriber moves between eNBs through S1



Intra-MME handover with the S1 interface enables undisturbed data transfer when a subscriber is moving when the X2 interface is not available.

This feature requires support from eNBs.

3.9.3 MME continuation of S1 handover procedure due to CIDF/failure/no response (Feature m10915-01)

With the *MME continuation of S1 handover procedure due to CIDF/failure/no response* feature, the MME continues the S1 handover procedure even if there is a CIDF, failure, or no response.

With this feature, the MME ignores any error received for S11 Create Indirect Data Forwarding (CIDF) Tunnel Request and proceeds with the handover.

The MME also ignores no response from the S-GW after all the attempts for the S11 Create Indirect Data Forwarding Tunnel Request and proceeds with the handover.

Operators can use global parameter `s11sendCidfDuringS1ho` to enable or disable indirect forwarding of user traffic during S1 handover. If the indirect forwarding of data is disabled, the MME does not set up indirect forwarding tunnels irrespective of the presence of bearers requiring indirect forwarding in S1AP Handover Request Ack message.

The MME continues with S1 handover for the following error conditions:

- Cause value is set to any value other than Request Accept in the S11 Create Indirect Data Forwarding Tunnel Response.
- No response to the S11 Create Indirect Data Forwarding Tunnel Request after all the attempts for the S11 Create Indirect Data Forwarding Tunnel Request message.

These error conditions indicate that S-GW failed to set up indirect forwarding tunnels. The forwarding paths are not needed to complete the S1-based handover. The user traffic is lost until the UE notifies handover complete to the target eNB without the forwarding paths. The MME logs these error conditions.

With this feature, handover success does not depend on data forwarding tunnel setup success. Better handover success ratio can be ensured.

3.9.4 Include Handover Restriction List always (Feature f10505-01)

This feature supports provisioning of a global parameter to include the Handover Restriction List even if equivalent PLMN or TA and LA restrictions are not provisioned.

When the feature is enabled, MME includes the Handover Restriction List IE in S1AP messages irrespective of EPLMN, forbidden TA or forbidden LA provisioning. If EPLMN and forbidden TA and LA are not provisioned, MME only includes the serving PLMN IE in the HRL IE.

The global parameter `includeHrlAlways` is by default disabled.

3.9.5 CMM support for sending HRL in all messages where CMM supports HRL IE (Feature f10910-03)

The MME only includes the handover restriction list (HRL) in specific cases typically when restrictions change. When the feature is enabled by setting the global parameter `unconditionallyAddHrlIE` to Yes, the MME unconditionally includes the Handover Restriction List IE in all S1AP messages, as described in the 3GPP specifications.

3.9.6 Change retransmission timer for E-RAB setup request (f10931-01)

This feature introduces the timer, `erabHoFailureTimer`.

Upon receiving an E-RAB setup, modify, or release request, if the RAN is busy with a handover operation, the RAN can respond with “X2 handover triggered” or “S1 intra system handover triggered”. The handling of the these handover-triggered responses is dependent on CMM MME implementation. The MME starts the `erabHoFailureTimer` timer when it receives an E-RAB setup, modify, or release response with S1AP cause code X2 handover triggered or S1 intra system handover triggered. When the handover completes or timer expires, the MME retransmits the initial E-RAB request.

By default, the `erabHoFailureTimer` timer is set to 300 ms. If global parameter `nrCcDoubleS1PsAck` is set to Yes, the timer is set to fixed value of 1000s. Additionally, the CMM only attempts a single retry of any E-RAB request queuing during the handling of this scenario.

3.9.7 Error handling in Create Session Response for PDN Connectivity Request type of handover (Feature f10565-01)

With this feature, the MME supports error handling in Create Session Response message for the PDN connectivity request type of handover. If the Create Session Response message does not indicate success and the Cause Source (CS) bit indicates the P-GW, the MME sends PDN Connectivity Reject with cause #54 PDN connection does not exist.

This feature applies only to standalone PDN connectivity request and gateway selection mode 2.

This feature is controlled by global parameter `sendPdnConnRejWithReactReq` (the default value is `No`).

3.9.8 MME support for QCI1 HO attempt rejection (Feature f10502-04)

With this feature, the MME supports the global parameters `qci1HoRejectionUtran` and `qci1HoRejectionGeran` to reject the PS handover for a QCI1 bearer in the specific scenarios.

The MME supports the `qci1HoRejectionUtran` global parameter to reject the PS handover, when the Handover Required message does not include the SRVCC HO Indication IE, and the UE currently has a dedicated bearer with QCI1 established, and the handover attempt is towards 3G, that is, the Handover Type IE is set to `LTEtoUTRAN`. Then, the MME sends the Handover Preparation Failure message with the cause 'Handover Failure In Target EPC/eNB Or Target System' and does not proceed further with the handover.

The MME supports the `qci1HoRejectionGeran` global parameter to reject the PS handover, when the Handover Required message does not include the SRVCC HO Indication IE, and the UE currently has a dedicated bearer with QCI1 established, and the handover is towards to 2G, that is, the Handover Type IE is set to `LTEtoGERAN`. Then, the MME sends the Handover Preparation Failure message with the cause 'Handover Failure In Target EPC/eNB Or Target System' and does not proceed further with the handover.

If the SRVCC HO Indication IE is included, the SRVCC handover is performed to the circuit-switched side for the QCI1 bearer.

3.9.9 MME support for fail HHO with SRNS if indirect forwarding tunnel cannot be established (Feature f11816-01)

This feature adds the handover (HO) abort option in case a hard handover (HHO) with the serving radio network subsystem (SRNS) is performed from a 4G CMM to a 3G non-CMM with the indirect handover configured and the S-GW fails to establish the Indirect Data Forwarding Tunnel Request message (response is received with overall cause code #69).

In this case, the MME aborts the HHO by sending the Forward Relocation Cancel message to the target SGSN and the Handover Preparation Failure message to the source eNB. The feature is activated through the `sendFwdRelCancelAndHoPrepFailure` gParm to control the behavior of the indirect forwarding failure.

By default, the feature is disabled. When it is enabled, the MME, upon failure of the indirect forwarding, sends the Forward Relocation Cancel message to the SGSN and the Handover Preparation failure message to the eNB.

Note:

This feature impacts only the non single radio voice call continuity (SRVCC) 4G to 3G over Gn HO cases.

3.9.10 MME support for adding s1hoResourceReleaseWithNoMmeSgwRel timer (Feature f10568-01)

This feature supports a new timer `s1hoResourceReleaseWithNoMmeSgwRel` instead of existing `s1hoResourceRelease` timer, which is used to guard in intra-MME and intra-S-GW HO scenarios to initiate release towards the source eNB. This feature also supports increase in the resolution of the MME and the AMF timers from 100 milliseconds to 50 milliseconds.

When `s1hoResourceReleaseWithNoMmeSgwRel` timer is set to 0, the MME falls back to use the old `s1hoResourceRelease`.

This timer is used in case of intra-MME HO with or without TAU, and intra-MME HO without S-GW relocation.

3.10 Time zone management

Features related to time zone management and distribution, such as network identity and time zone (NITZ).

3.10.1 EMM information procedure (Feature m10102-01)

With the *EMM information procedure* feature, the network can provide network name and time zone for the UE.

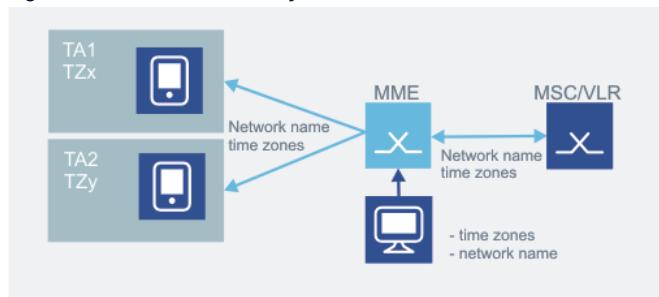
The user must see the current network name in his terminal. The user must also know the local time zone.

The MME receives the network name and time zone from the MSC, or the time zone or several time zones are configured locally in the MME. If multiple time zones are configured under one MME, the time zones are configured per tracking area (TA) or TA range.

The operator can use parameters to control whether the network identity and time zone (NITZ) is received through SGs, or whether the NITZ data is configured locally in the MME. If the NITZ values are local, the locally configured values override the information that comes from the SGs interface.

The MME sends the information to the UE in the EMM Information message.

Figure 16: NITZ delivery to UE



With this feature, the MME can send its time zone, universal time and day light saving time to UE using the EMM information procedure. In addition, the MME sends the network name, if provisioned. The MME sends the EMM Information message immediately after receiving the Attach Complete message and also after sending the TAU Accept message. The feature provides the following provisioning capabilities:

- Send time zone to UE (default is false)
- Send network name (default is false)

- Network name
- Network short name
- Include country initials (default is false)
- Name encoding (GSM default alphabet (default)/UCS2)

Table 14: Information elements related to NITZ

IEI	Information element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	EMM information message identity	Message type 9.8	M	V	1
43	Full name for network	Network name 9.9.3.24	O	TLV	3-n
45	Short name for network	Network name 9.9.3.24	O	TLV	3-n
46	Local time zone	Time zone 9.9.3.29	O	TV	2
47	Universal time and local time	Time zone and time 9.9.3.30	O	TV	8
49	Network daylight saving time	Daylight saving time 9.9.3.6	O	TLV	3

Support is required from the MSC if network and time zone information is delivered over the SGs interface.

3.10.2 Additional time zone distribution functionality (Feature m10102-04)

The **Additional time zone distribution functionality** feature provides the time zone change notification to the S-GW when the UE moves to a new tracking area (TA) with a new time zone.

Time zone information is sent through the S-GW to the charging entity in Create Session

Request, Delete Bearer Response, and Modify Bearer Request during time zone changes in the MME, MME relocation, or service request.

This feature also includes the provisioning enhancements for resolving the correct time zone for each eNB: a list of eNBs within the MME pool region that are not in the same time zone is provisioned with the time zone offset so that the correct time zone for each eNB within the pool can be resolved.

3.10.3 TAI/RAI-based time zone distribution (Feature m10102-05)

The *TAI/RAI-based time zone distribution* feature provides capability to define a default time zone for a mobile network and then specify time zones on a per routing area (RA) or per tracking area (TA) basis.

All RAs and TAs that have no specific time zone configuration are considered to be in the default time zone. As part of the support for network sharing, it is also possible to define a default time zone by PLMN. Provisioning of TA/RA that is different from the default can be done either by TA/RA or by ranges of TA/RA.

The information on time zone is propagated to the P-GW or GGSN or both in the GTP-C messages as defined by respective 3GPP standards. If charging gateway is configured (applicable to the 2G/3G) the information is also included in S-CDR records.

3.10.4 Delivering network name or network short name based on IMEI and TA (Feature f10418-01)

This feature allows the NITZ/EMM mechanism to be modified to enable CMM to send a separately-defined network name and/or short name based on UE IMEI-TAC/SV and tracking area (TA).

This feature is activated using the `uePlmnService` command. When this feature is active, if a UE performs a procedure, such as attach or TA update, that triggers sending the network name, the CMM attempts to match the UE to an entry in the IMEI-TAC/SV table. If a match occurs, the CMM sends the separately-defined network name or network short name, which is keyed by IMEI-TAC and SV. Otherwise, the CMM defaults to the PLMN-based network name or short name operation.

The basic CP logic is as follows:

- Read the `uePlmnService` table to determine if the `emmInfo` override can occur

(Boolean). If not, stop and proceed with legacy logic.

- Read the IMEI TAC/SV table to determine if the UE is eligible for override (profile name). If there is no profile, stop and proceed with legacy logic.
- Read the `emmInfoOverride` profile using the profile name as the key. If not found, stop and proceed with legacy logic.
- Read the `emmInfoOverride` in the tracking area identifier (TAI) table to determine if the `emmInfoOverride` profile is used and to select which network name and which network short name to use, then send the `emmInfo`.

3.10.5 MME support for sending network name to the UE after attach/TAU on an `imsiRangeServices` level (Feature f10418-02)

This feature enhances the NITZ/EMM mechanism to enable the MME to send a separately defined network name and/or short name on an `imsiRangeServices` level.

When a UE performs a procedure, such as attach or tracking area update (TAU), that triggers sending the network name, the MME chooses the network name and/or short name to send based on the following rules:

1. The MME uses the `emmInfoOverrideTacSv` parameter as configured in *Delivering network name or network short name based on IMEI and TA* (feature f10418-01).
2. If rule 1 fails, the MME uses the `emmInfoOverride` profile provisioned at the `imsiRangeServices` level for the UE.
3. If rule 2 fails, the MME uses the `emmInfoOverride` profile provisioned at the `uePlmnServices` level for the selected PLMN.
4. If rule 3 fails, the MME uses the legacy PLMN-based `emmInfo` information for the new TAI.

With this feature, the MME does not re-send the network name or short name if they were sent in the previous EMM Information message, as this has been done in *Delivering network name or network short name based on IMEI and TA* (feature f10418-01).

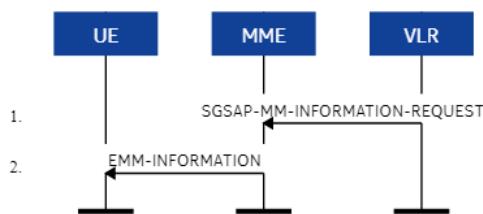
With this feature, the MME supports special characters in the network name and network short name per GSM encoding definition.

3.10.6 MME provisioning option to send or ignore MM info from MSC/VLR (Feature f10401-01)

The **MME provisioning option to send or ignore MM Info from MSC/VLR** feature enables operators to either use the mobility management (MM) info provided by the MSC over SGs or the MM info normally provided by the MME.

By default, the MME sends the SGSAP-MM-INFORMATION to a UE in ECM-CONNECTED state. The SGSAP-MM-INFORMATION contents are sent to the UE in the NAS EMM-INFORMATION message.

Figure 17: EMM information procedure



This feature enhances the current behavior of always sending the MM info received from the MSC/VLR to the UE by providing a provisioning option to select whether to send the UE the MM info from the MSC/VLR or ignore the MM info. The provisioning option is a global parameter `ignoreSGSapMMInfo` provided at the MME level and applies to the MME home network and shared network. By default, the provisioning is set to send the UE the MM information received from the MSC/VLR.

3.10.7 MME support for spreading time zone updates due to DST change (Feature f10102-03)

When UE time zone is changed and detected by the MME through mobility, UE-triggered service request, PDN disconnection or UE detach, the time zone is reported to the policy and charging rules function (PCRF) through the Gx interface, and to the OCS through the Gy interface. In the event of daylight saving time change, this is generating significant amount of signaling on the Gx and Gy interfaces, causing message storm to the core network, specifically to the PCRF and the OCS. This feature addresses the issue by a MME capability to spread the time zone updates to the network over a period of time.

In order to spread the time zone updates, the MME supports a configurable parameter for controlling rate of time zone updates to the network.

The MME includes the UE Time Zone IE to update the network whenever there is change of time zone (such as daylight saving time) in the following S11 messages:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Response
- Update Bearer Response
- Delete Bearer Command

The MME always includes the UE Time Zone IE in Create Session Request and Delete Session Request.

The MME keeps track of inclusion of the UE Time Zone IE in the S11 messages. if the inclusion rate exceeds the provisioned rate, the MME slows down the rate of the inclusion of the UE time zone in the S11 messages except for Create Session Request and Delete Session Request.

The MME keeps track of whether time zone update is made or not in the UE context data base and sends time zone updates of the skipped UE on a subsequent session management activity.

3.10.8 Periodical TAU triggered EMM Information with NITZ (Feature f10402-01)

This feature provides separate provisioning options to enable or disable sending of the EMM Information message after each successful attach, periodic TAU, intra-MME TAU, inter-MME TAU, or IRAT TAU procedure. The EMM Information message includes the network identity and time zone (NITZ) for the UE.

The `cmm emmInfo` command allows the operator to separately select the procedures after which the EMM Information message is sent to the UE.

This feature requires EMM Information to be provisioned with either `sendNetworkName` or `sendTzOffset` provisioned to `true`. Note that if `sendNetworkName` is provisioned, either `networkName` or `networkShortName` must be provisioned.

3.11 Cause code management

Features enabling cause code provisioning.

3.11.1 Enhanced NAS cause code functionality (Feature m10108-01)

With the *Enhanced NAS cause code functionality* feature an operator is able to adjust the network behavior as preferred. Operator can adjust charging based on NAS/S1-AP cause codes.

This feature supports three capabilities:

- Provisioning of a non-access stratum (NAS) cause value per public land mobile network (PLMN) to be sent if a UE-requested mobility management procedure (attach, tracking area update (TAU), and service request) is rejected due to an access restriction.
- Provisioning of a NAS cause value per PLMN to be sent if a UE-requested mobility management procedure (attach, TAU and service request) is rejected because of HSS errors (experimental Diameter error codes).
- Sending of S1-AP cause codes, EMM and ESM cause codes to the S-GW in S11 Create Bearer Response, Delete Session Request, Delete Bearer Command, Delete Bearer Response, Release Access Bearer Request, and Update Bearer Response messages. The S-GW includes these cause codes to populate diagnostic codes of CDRs.

This feature does not include provisioning of cause values to be sent for the UE rejection because of operator-determined barring (ODB), Roaming-Restricted-to-Unsupported Features or Network-Access-Mode.

Support is required from the S-GW/P-GW and charging system to support the receiving of the NAS/S1-AP cause codes.

3.11.2 Provisionable EMM and ESM cause code values (Feature f10403-01)

The feature provides the possibility to configure EMM/ESM cause codes for some already existing failure scenarios. In addition, it introduces some new failure scenarios with configurable EMM/ESM cause codes

MME's support for provisionable cause code values is controlled by global parameter `enableProvCc`. By default, the feature is disabled, and the existing implementation

remains unchanged with hard coded cause values used as ESM and EMM causes.

When the feature is enabled, MME supports provisionable EMM/ESM cause codes for the following scenarios:

Table 15: Provisionable EMM/ESM cause code values for existing scenarios before this feature

Scenarios	MME behavior with default ESM/EMM provisioned cause code	Internal error cause used in CLI to provision EMM/ESM cause code
Attach and standalone PDN connectivity procedures, MME receives Create Session Response with cause #104	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: APN restriction value incompatible with active EPS bearer context).	intErrorBearerSetupFailed
PDN Connectivity Request for an APN for which maximum number of allowed PDN connections are already existing	MME sends PDN Connectivity Reject (ESM cause: Multiple PDN connections for a given APN not allowed).	intErrorMaxNumOfPdnPerApn
Inter-MME or inter-RAT TAU procedure, none of the current APN(s) of the UE is allowed by HSS subscription	TAU Reject (EMM cause: ESM failure).	intErrorNoApnAllowedByHss
P-GW sends Delete Bearer Request with cause as 09 PDN reconnection to this APN disallowed	MME sends Deactivate EPS Bearer Context Request with ESM cause: APN Restriction value incompatible with active EPS bearer context or MME sends detach in case of Delete Bearer Request on last default bearer.	intErrorReqPdnNotAllowed
Attach and PDN connectivity procedures, no response from S-GW for Create Session Request	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: Insufficient resources).	intErrorNoRespFromSgwAttPdn
Service request procedure, no response from S-GW for Modify Bearer Request	MME sends Deactivate EPS Bearer Context Request with ESM cause: Network failure in case of partial PDN failure.	intErrorNoRespFromSgwSvcReq
TAU procedure, no Create Session Response from S-GW	MME sends TAU Reject (EMM cause: Implicitly detached).	intErrorNoRespFromSgwTau
Bearer resource allocation procedure, no response from S-GW for Bearer Resource Command	MME sends Bearer Resource Allocation Reject (ESM cause: Request rejected by serving GW or PDN GW).	intErrorNoRespFromSgwBrrAlloc

Scenarios	MME behavior with default ESM/EMM provisioned cause code	Internal error cause used in CLI to provision EMM/ESM cause code
Bearer resource modification procedure, no response from S-GW for Bearer Resource Command	MME sends Bearer Resource Modification Reject (ESM cause: Request rejected, unspecified).	intErrorNoRespFromSgwBrrMod
Decoding PDN Connectivity Request during attach - NAS decoding failure on EPS_ESM_PDN_CONNECTIVITY_R EQUEST ESM container	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: Invalid mandatory information).	intErrorMandlelnc
Attach and standalone PDN procedures, Create Session Response received with invalid Sender F-TEID for Control Plane IE	MME sends Attach Reject (EMM cause: ESM failure), or PDN Reject (ESM cause: Conditional IE Error).	intErrorOptlelnc
The QCI value for the APN that the MME selects for the attach is from 1 to 4 in the HSS subscription data	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: Network failure).	intErrorSystemFailure

In addition to the mentioned scenarios above, the feature introduces the following ones, with configurable cause codes:

Table 16: Provisionable EMM/ESM cause code values for scenarios introduced by the feature

Scenarios	MME behavior with default ESM/EMM provisioned cause code	Internal error cause used in CLI to provision EMM/ESM cause code
Non-emergency attach procedure, Create Session Response comes with emergency ARP	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM Cause: Request rejected, unspecified).	intErrorServiceDenied

Scenarios	MME behavior with default ESM/EMM provisioned cause code	Internal error cause used in CLI to provision EMM/ESM cause code
Attach and standalone PDN connectivity procedure, PDN type requested by UE is IPV4 but subscribed PDN type is IPv6, or PDN type requested by UE is IPV6 but subscribed type is IPV4	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: PDN type IPv6 only allowed) when UE requests for IPV4. MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: PDN type IPv4 only allowed) when UE requests for IPV6.	intErrorIpv6OnlyAllowed intErrorIpv4OnlyAllowed
Mismatch in the eNB IP address type and SGW S1/S11-U TEID IP address type	MME sends Attach Reject (EMM cause: ESM failure), or PDN Connectivity Reject (ESM cause: Network failure) in case of attach procedure or TAU Reject (EMM cause: Network failure) in case of TAU procedure.	intErrorIpVerMismatchAtt intErrorIpVerMismatchTau
NAS Security Mode Reject, MME receives the NAS Security Mode Reject message with cause #24	Attach/TAU/Service Reject (EMM cause: Illegal UE).	intErrorSmcFailed

Note:

In some scenarios, when the feature is enabled with global parameter `enableProvCc`, procedure failures can be caused; when the feature is disabled, procedures can be handled successfully.

3.11.3 EMM and ESM cause code mapping enhancements (Feature f10119-02)

This feature introduces enhancements for EMM and ESM cause code mapping.

This feature introduces customized EMM and ESM cause code mapping enhancements for the following cases:

- When the MME does not receive response from the HSS during attach or TAU procedure and the Attach Reject message is sent to the UE. The customized cause code is sent to the UE so that the UE can retry the attach. This enhances NAS EMM cause codes for Diameter codes diamNasMappingProfile.
- When the MME receives #92 Create Session Response Reject from the S-GW, the EMM cause code is re-mapped to network failure. And when the MME receives S11 Create Session Response with cause code #92 user authentication failed, the MME maps it to ESM cause code #33 Requested service option not subscribed. This enhances feature *Provisionable EMM and ESM cause code values (f10403-01)*.

3.11.4 Default cause code for roamer UE's PLMNs (Feature m10109-04)

The MME supports provisioning of default NAS codes to be used if a UE-requested mobility management (attach, TAU and service request) procedure is rejected because of an access restriction.

Currently the supported access restriction is international mobile subscriber identity's (IMSI) public land mobile network (PLMN) is not allowed.

These additional restrictions are supported in another feature:

- UE is not allowed in a tracking area identity (TAI) in home PLMN (HPLMN)
- Roaming UE is not allowed in the TAI
- E-UTRAN restricted in UE's HPLMN
- E-UTRAN restricted in a visited PLMN (VPLMN)

If the default NAS codes are not provisioned, the MME uses the current hard-coded default values. If the feature is not activated, the provisioning is used for all the PLMNs. If the feature is activated, the MME uses the default for those PLMNs with no provisioned NAS cause codes.

With this feature the network behavior can be adjusted per roaming PLMN.

3.11.5 MME support for change CC for UE attempting combined attach in TAI (Feature f10413-01)

This feature supports changing the cause code for UE attempting combined attach in TAI without 3G support.

The feature uses the EMM cause code specified by `attachSgsUnknownLaiEmmCause` and `tauSgsUnknownLaiEmmCause` in the EPS only Attach Accept and EPS only TAU Accept message if the MME failed to select a MSC due to provisioning errors in LAI to TAI to MSC selection provisioning for UE requested combined attach and TAU requests respectively.

3.11.6 MME support for provisonable cause code for Update Bearer Response during inter-RAT redirection (f11346-02)

This feature allows a specific GTPv2 cause to be used in the Update Bearer Response message sent back to the S-GW when the Update Bearer Request message is received during an inter-RAT redirection scenario.

When the feature is enabled, the MME sends the Update Bearer Response message with the provisonable cause code back to the S-GW when the Update Bearer Request message is received during an inter-RAT redirection scenario.

When the feature is disabled, the MME sends the Update Bearer Response message with GTPv2 cause 94 'Request Rejected' back to the S-GW when the Update Bearer Request message is received during an inter-RAT redirection scenario.

3.12 RFSP management

Features related to index to RAT/frequency selection priority (RFSP).

3.12.1 Connected mode mobility enhanced for reserved cells (Feature m10908-01)

With the *Connected mode mobility enhanced for reserved cells* feature operators can test newly installed eNBs with restricted access. Operators can adjust network behavior, for example, by making the UE prioritize the E-UTRAN access.

The aim of the eNB feature is to allow handovers towards cells reserved for operator use for UEs used by the operator's staff, and to block all other incoming handovers.

Before opening up newly installed eNBs to be used by commercial UEs, operators often have a period of time where access to these eNBs is restricted and the operator's teams verify that the eNBs are functioning properly and that radio parameters have been set properly. 3GPP standards have a mechanism to forbid idle mode reselection of commercial UEs

towards these restricted eNBs, but there is no mechanism to forbid incoming handovers of commercial UEs while allowing handovers of the operator's test UEs. This feature introduces a proprietary mechanism to permit this behavior.

Operators gain from this mechanism as they are able to test more in a controlled environment. To mitigate the fact that handovers to reserved cells are not allowed for commercial UEs, this feature also introduces a handover retry mechanism on the second best cell if the handover preparation to the best cell fails.

The solution involves a special RFSP Index used to allow handovers of operators' test UEs and the MME supports sending of this RFSP Index value to eNBs.

The Index to RAT/Frequency Selection Priority (RFSP index) parameter is an index referring to user information (for example, mobility profile, service usage profile). The RFSP Index is UE specific. The eNB receives the parameter for a UE from the MME through the S1 interface. Normally, this index is mapped by the eNB to locally defined configuration to apply specific RRM strategies to a UE (for example, to define RRC-IDLE mode priorities and control inter-RAT/inter-frequency handover in RRC-CONNECTED mode).

The RFSP Index has a value from 1 – 256. Values 1 – 128 are operator-specific values; values 129 - 256 are standardized reference values. Currently, three standardized RFSP Index values, 254, 255, 256, are defined in 3GPP TS 36.300, which specifies the mapping at the eNB of these values to their respective cell re-selection and inter-RAT/inter-frequency handover priorities.

For a particular UE, at most one subscribed RFSP Index value can be provisioned in the HSS. The MME receives the subscribed RFSP Index value from the HSS (for example, during the attach procedure). For a UE, the MME chooses a provisioned RFSP Index based on the UE voice capability. The MME provides provisioning of separate RFSP Index value for each of the following UE capability for voice-centric UEs:

- Circuit switching (CS) voice only
- IP multimedia subsystem (IMS) packet switching (PS) voice only
- CS voice preferred, IMS PS voice as secondary
- IMS PS voice preferred, CS voice secondary
- value to be used if UE voice capability is not known

This provisioning is supported for the MME's home public land mobile network (PLMN) and also for other PLMNs in the roaming agreement table. This feature expands this provisioning to also support separate RFSP Index values for data-centric UEs. If no values are provisioned, the MME uses the RFSP Index value if it is received from the HSS. The MME forwards the RFSP Index in use to the eNB across S1 in the Initial Context Setup Request message or UE Context Modification Request message. During X2 handover, the RFSP Index

in use is forwarded from the source eNB to the target eNB in the Handover Request message. During S1 handover, the source eNB includes the RFSP Index in use in the Source eNB to Target eNB Transparent Container in the S1 Handover Required message. This transparent container is then delivered to the target eNB by the MME in the S1 Handover Request message.

For this feature, the MME provides provisioning of an additional RFSP Index value termed as RFSP Index for voice capable UEs. This value is used for non-roamer UEs. If the value is provisioned, the MME uses an algorithm to select a RFSP Index value as specified in the table. It is assumed that the RFSP Index for voice capable UE (the `rfspIndexVoiceCapableUe` parameter in the `svcAgreementProfile` command) is set to value `abc`.

Table 17: RFSP Index

	RFSP Index provisioned in HSS	RFSP Index not provisioned in HSS
Voice domain preference and UE usage setting IE is present in Attach Request/TAU Request	If HSS RFSP Index = 'abc' for a non-roamer UE, the MME chooses RFSP Index based on a locally provisioned UE usage setting and voice domain preference RFSP Index and sends it to the eNB.	The MME chooses an RFSP Index based on a locally provisioned voice preference RFSP Index and sends it to the eNB.
(apply to voice-capable UE)	If the HSS RFSP Index is not 'abc', the MME chooses the HSS RFSP Index and sends it to the eNB.	
Voice domain preference and UE usage setting IE is not present in Attach Request/TAU Request	The MME chooses the HSS RFSP Index and sends it to the eNB.	The MME does not send the RFSP Index to the eNB (exception: if the MME receives the RFSP Index from an old MME/SGSN during TAU procedure, the MME sends this RFSP).
(apply to data-only UE)		

For a roaming UE, the MME selects the RFSP Index provisioned for the UE's home PLMN. If UE usage setting and voice domain preference are not known for a roamer, the MME selects the provisioned generic RFSP index (the `rfspIndex` parameter in the `svcAgreementProfile`

command) if it is configured.

The following is an example to illustrate the RFSP Index values provisioned in the HSS for a home UE and the RFSP Index value the MME sends to the eNB.

- RFSP Index provisioned in the HSS for voice-capable commercial UEs is 10 ('abc' in the table): RFSP Index value sent to eNB is chosen by the MME based on the UE voice domain preference and usage setting.
- RFSP Index provisioned in the HSS for data-only commercial UEs is standardized value 256:
 - Cell re-selection priority:
 - E-UTRAN – high
 - UTRAN – medium
 - GERAN – low
 - RFSP Index value sent to the eNB is 256.
- RFSP Index provisioned in HSS for testing UE is 50, when testing handover to a reserved cell:
 - RFSP Index value 50 is sent to source eNB and forwarded to the target eNB during handover request.
 - The target eNB accepts handover request if RFSP Index is 50; otherwise the target eNB rejects handover request.
- RFSP Index provisioned in HSS for testing UE is 10 or 256, when testing cell reselection priority: RFSP Index value sent to the eNB is the same as the respective commercial UE (see the first two bullets).

The HSS support for RFSP Index is optional.

3.12.2 Provisioning the RFSP in CMM based on IMEI/TAC (Feature f51024-02)

The MME provides configuration of RFSP index for MME home PLMN. The range is 1 to 256 and the default value is 1. This feature applies only to home UEs.

The MME attempts to match the UE's IMEI-TAC to an entry in the `imeiTacRfsp` table. If there is an IMEI-TAC match, the MME applies and uses the configured associated RFSP value that is sent to the eNB. If there is no match for IMEI-TAC, the RFSP is not included. Only eight-digit TAC value is considered. SNR and SVN are not required. This applies to the following procedures:

- initial/GUTI attach
- inter-MME TAU

- inter-MME S1-based handover
- IRAT (3G to 4G)

The MME includes RFSP index value in PCMD data for a UE when a value is sent in the following messages:

- Initial Context Setup Request
- UE Context Modification Request
- DL NAS transport
- Handover Request

The MME supports a global IMEI-TAC/RFSP table. 2K entries are supported. Each IMEI-TAC/RFSP entry will specify:

- IMEI-TAC (key): The full TAC eight digits are mandatory.
- RFSP: Digit value is mandatory, and the range is 0 -256, with a default value of 1.

Here is a sample of the table: IMEISV = AA-CCCCCC-EE:

- AA represents TAC
- CCCCCC represents SNR
- EE represents SVN

3.12.3 CMM support for RFSP override based on IMSI and TAC (Feature f51024-03)

This feature enhances the MME to override the RAT/frequency selection priority (RFSP) based on the IMSI or the IMEI TAC by supporting the combination of the IMSI and the IMEI TAC, giving priority to the IMEI TAC.

Before this feature, the MME was allowed to enable only the IMSI or the IMEI TAC.

When RFSP override by the IMEI TAC is enabled, but there is no matching IMEI TAC for the UE, the MME checks against RFSP override via the IMSI configuration to find the RFSP value for the UE.

RFSP override by the IMEI TAC has the top priority and only if there is no matching IMEI TAC, the MME checks against RFSP override via the IMSI configuration.

3.12.4 MME support for RFSP enhancement (Feature f51024-04)

This feature introduces a configuration option to define the way that the RAT/frequency selection priority (RFSP) index is assigned for the UE.

The configuration option is available via the `SvcAgreementProfile` command and based on the associated IMSI range and the UE PLMN services decides whether:

- The RFSP value received as part of the HSS subscription data will be sent to the eNB.
- To overwrite whatever value received from the HSS (even if no value is received) with the value locally provisioned.

This applies to the following procedures:

- initial/GUTI Attach
- inter MME TAU
- S1-based inter-MME handover
- IRAT (3G to 4G)

In case of the mobility scenario, it may be possible that the RFSP Index in use IE and the subscribed RFSP Index IE are received from the source node. When the current feature is enabled, the serving MME local configuration as defined in the current feature has priority against the values that are received from the source node.

When the feature is enabled and used to select the RFSP value, the selection of the RFSP value does not have dependency on the voice domain preference and UE's usage setting IEs that may be received in the Attach/TAU Request message.

Additionally, the new configuration option is available via the `svcAgreementProfileName` parameter in the `uePlmnServices` command. Typically, this configuration option in `UePlmnServices` command is used to ensure that the default RFSP value is assigned to all the UEs associated with the specific UE PLMN services profile, when an RFSP value is not assigned via the `ImsiRangeServices` command.

The feature is applicable in both IMSI range and UE PLMN services level and it applies to both home and roaming subscribers.

3.12.5 MME support for single IMSI group HSS unavailability/down declaration (Feature f11346-01)

This feature enables the MME to consider all HSS as unavailable "hssOrEirDown" (6002

diameter cause code) when a single IMSI group rule match is found and all HSS associations/links are unavailable.

If no IMSI group rule is found with a provisioned HSS association, the MME reports this as no provisioned HSS case "noProvisionedHss" (6001 diameter cause code).

The IMSI group rule is configured by using the `imsiToHss` command. HSS associations/links are configured by using the `rmtEndPtCfg` command.

The following table shows the MME behavior based on UE's PLMN, IMSI group rule settings, HSS associations/links, and whether the global parameter

`s6aReportPreviousHssSelectionForHssDown` is enabled or not:

Table 18: MME behavior based on related-settings

Index	PLMN	gParms <code>s6aReportP reviousHss SelectionF orHssDown</code>	IMSI group rule	HSS associations/li nks	Result
1	HOME UE + IMSI is in range	Enabled/Yes	Match	Down	<code>hssOrEirDown</code>
2	HOME UE + IMSI is in range	Disabled/No	Match	Down	<code>NoProvisioned Hss</code>
3	HOME UE + IMSI is not in range	Enabled/Yes	No Match	Down	<code>NoProvisioned Hss</code>
4	HOME UE + IMSI is not in range	Disabled/No	No Match	Down	<code>NoProvisioned Hss</code>
5	ROAMING UE + IMSI is in range	Enabled/Yes	Match	Down	<code>hssOrEirDown</code>
6	ROAMING UE + IMSI is in range	Disabled/No	Match	Down	<code>NoProvisioned Hss</code>
7	ROAMING UE + IMSI is not in range	Enabled/Yes	No Match	Down	<code>NoProvisioned Hss</code>
8	ROAMING UE + IMSI is not in range	Disabled/No	No Match	Down	<code>NoProvisioned Hss</code>

Index	PLMN	gParms s6aReportP reviousHss SelectionF orHssDown	IMSI group rule	HSS associations/li nks	Result
9	HOME UE + IMSI is not in range HOME ALL (no range)	Enabled/Yes	Match	Down	hssOrEirDown
10	HOME UE + IMSI is not in range HOME ALL (no range)	Disabled/No	Match	Down	hssOrEirDown
11	ROAMING UE + IMSI is not in range HOME ALL (no range)	Enabled/Yes	No Match	Down	NoProvisioned Hss
12	ROAMING UE + IMSI is not in range HOME ALL (no range)	Disabled/No	No Match	Down	NoProvisioned Hss
13	ROAMING UE + IMSI is not in range ROAMING ALL (no range)	Enabled/Yes	Match	Down	hssOrEirDown
14	ROAMING UE + IMSI is not in range HOME ALL (no range)	Disabled/No	Match	Down	hssOrEirDown

Index	PLMN	gParms s6aReportP reviousHss SelectionF orHssDown	IMSI group rule	HSS associations/li nks	Result
15	HOME UE + IMSI is not in range ROAMING ALL (no range)	Enabled/Yes	No Match	Down	NoProvisioned Hss
16	HOME UE + IMSI is not in range ROAMING ALL (no range)	Disabled/No	No Match	Down	NoProvisioned Hss

When this feature is enabled, there is a chance that more UEs may come back to the MME with S1 requests. For this situation, Nokia recommends to set the global parameter `s6aHssUpdateEnbCapacity` (introduced in *Feature m11318-01*) to either `AllHSS` or `HomeHSS`.

For *S6a fault handling enhancement* (*Feature m11318-01*), if there is an HSS outage which lasts more than 30 seconds, the MME updates the eNB with capacity 1. This results that UEs eventually move to a different MME.

3.12.6 MME support for sending RAT-Frequency-Selection-Priority-ID update to eNB received in IDR from HSS (Feature f10939-01)

This feature allows the MME to send an updated RAT-Frequency-Selection-Priority-ID that it receives in the IDR message from the HSS to the eNB in UE Context Modification Request messages.

After receiving a RAT-Frequency-Selection-Priority-ID (RFSP) in an IDR message from the HSS, the MME sends the updated Subscriber Profile ID for the RAT/Frequency priority IE to the eNB in the UE Context Modification Request message.

3.13 Roaming

In the home network (HPLMN), the HPLMN operator stores the subscription data in the network's home subscriber server (HSS). To ensure access to services also in other networks, roaming agreements are made between operators. When a roaming agreement exists and the subscriber moves to another operator's network, the visited network (VPLMN) fetches subscription data from the subscriber's home network.

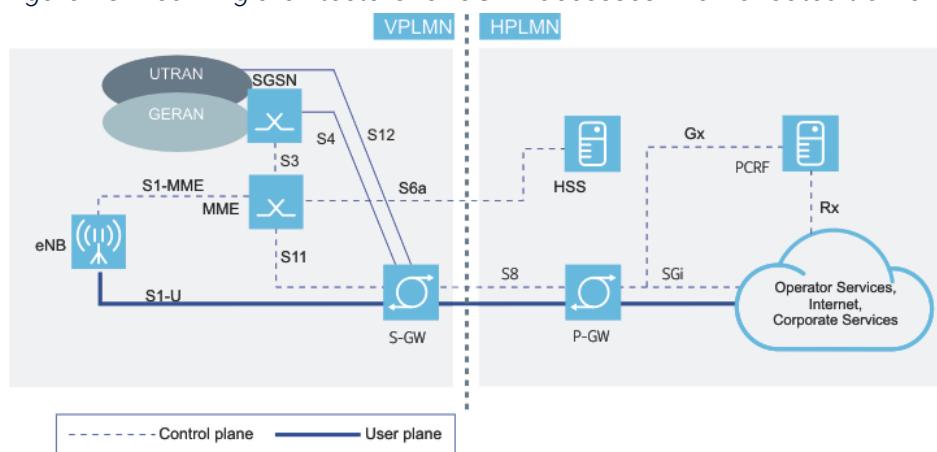
3.13.1 MME roaming support (Feature m10100-02)

The **MME roaming support** feature includes a series of checks on roaming UEs based on the UE subscription data and locally provisioned data to provide services in the MME serving area. In addition to the series of checks, the feature also supports equivalent public land mobile networks (PLMNs) and handover restrictions.

This feature supports roaming mobiles.

The figures show reference roaming architectures as described in 3GPP TS23.401.

Figure 18: Roaming architecture for 3GPP accesses - home routed traffic

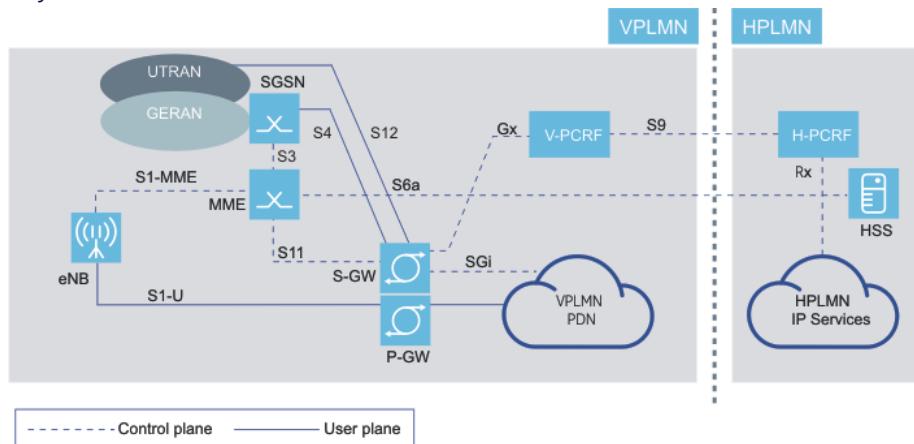


Additional interfaces/reference points for the 2G/3G network accesses are documented in 3GPP TS 23.060.

In the roaming architecture for 3GPP accesses, the MME in visited network (VPLMN) has S6a interface to the home network (HPLMN) of the UE. The bearers for a UE are anchored at the S-GW of the VPLMN. In this architecture, the bearer traffic is routed to the UE's HPLMN.

In the local breakout (LBO) architecture, the traffic is routed to the P-GW in the VPLMN.

Figure 19: Roaming architecture for local breakout, with home operator's application functions only



In the LBO architecture, the control plane signaling and the user plane for accessing the home operator's services traverse over the SGI reference point through the visited operator's packet data network (PDN). The application function is an entity in policy and charging control architecture that provides information to the charging rules function (CRF) of the policy and charging rules function (PCRF) for selecting appropriate charging rules.

Roaming agreements

The MME supports series of roaming checks when a roaming UE attempts to attach and do tracking area update (TAU) to the network. The MME considers a UE as a roamer if the PLMN ID indicated by the international mobile subscriber identity (IMSI) of the UE does not match the home PLMN ID of the MME. The MME does these checks by using a provisioned roaming agreement for the PLMN of the UE and subscription data of the UE obtained from the HSS of the UE's home network. The roaming agreement table consists of a set of capabilities allowed and restricted in the MME's HPLMN.

The MME allows provisioning of the following parameters per PLMN whose subscribers are allowed to roam. If these parameters are provisioned, the MME overrides the parameters in the UE's subscription data with the provisioned parameters.

Table 19: Per PLMN provisionable roaming parameters (*svcAgreementProfile*)

Parameter	Description
Network access mode	<p>The parameter specifies the type of access allowed for a UE of the PLMN. The values for the <code>networkAccessMode</code> parameter are <code>Packet</code> and <code>Circuit</code> and <code>Packet only</code>.</p> <p>The provisioned value overrides the subscription data for the UE only if the provisioned value specifies less capability.</p> <p>If the subscription data from the HSS is set to <code>Packet</code> and <code>Circuit</code>, and the provisioned value is <code>Packet only</code>, then the provisioned value overrides the subscription data.</p> <p>If the subscription data from the HSS is set to <code>Packet only</code>, and the provisioned value is <code>Packet</code> and <code>Circuit</code>, the provisioned value does not override the subscription data.</p>
Forbidden radio access technologies	<p>The parameters are used for the inter radio access technology (IRAT) handover restrictions.</p> <ul style="list-style-type: none"> • UTRAN not allowed (<code>accRestUtran</code>) • GERAN not allowed (<code>accRestGeran</code>) • E-UTRAN not allowed (<code>accRestEutran</code>) • CDMA 2000 not allowed (<code>accRestCdma2000</code>) <p>These parameters can be used to force access restriction of specific technologies when UE subscription data allowed the access. However, if an access restriction is already set in UE subscription, unsetting the access restriction in the svcAgreement table will not enable the access to that technology.</p>
Features allowed per PLMN	<ul style="list-style-type: none"> • CSoPS via Sv • Single Radio Voice Call Continuity (SRVCC) (<code>srvccPsToCs</code>) • 2G and 3G Circuit Switch Fall Back • Circuit Switch Fall Back DTR (<code>csfbDtr</code>) • Voice over IMS (<code>imsOverPs</code>) <p>Support to allow or not allow SMS is only supported when <code>SMS only</code> feature is supported (parameters <code>smsOnlyPlmnName</code> and <code>smsOnlyLac</code>).</p>
Radio Frequency Selection Priority ID	<p>If provisioned (parameter <code>rfspIndex</code>), the MME sends the provisioned value to the eNB. If not, the parameter received in the subscriber data is used.</p>

If provisioned, the MME uses these parameters:

- VPLMN Dynamic Address Allowed (`vplmnAllowed`)

This parameter indicates whether a roaming UE is allowed to use a PDN gateway for an access point name (APN) in the VPLMN or not. If the HSS subscription indicates that VPLMN

dynamic address is allowed, the MME checks this provisioned parameter to ensure that the MME's HPLMN restricts the use of P-GW in its HPLMN.

- Operator Determined Barring of all Packet Oriented Services (`odbAllApn`)

If this parameter is set to supported, the MME indicates to the HSS that the MME supports the ODB-ALL-APN and can take action if the HSS indicates ODB-ALL-APN in ULA and IDR. If this bit is set, the MME does not prevent a UE from accessing any packet services in HPLMN and VPLMN.

- Operator Determined Barring of all Packet Oriented Services (`odbHplmnApn`)

If this parameter is set to supported, the MME indicates to the HSS that the MME supports the ODB-HPLMN-APN and can take action if the HSS indicates ODB-ALL-APN in ULA and IDB. If this ODB bit is set, the MME does not allow the UE to access any packet services in the UE's HPLMN while roaming.

- Operator Determined Barring of all Packet Oriented Services (`odbVplmnApn`)

If this parameter is set to supported, the MME indicates to the HSS that the MME supports the ODB-VPLMN-APN and can take action if the HSS indicates ODB-VPLMN-APN in ULA and IDB. If this ODB bit is set, the MME does not allow the UE to access any packet services in the MME's HPLMN irrespective the provisioning of VPLMN dynamic address allowed and VPLMNDynamic-Address-Allowed attribute-value pair (AVP).

Support of equivalent PLMNs

An equivalent PLMN is used by a UE for cell reselection across PLMNs. The equivalent PLMNs are considered equivalent to the registered PLMN by the UE regarding PLMN selection, cell selection, cell re-selection and handover. A list of up to 15 equivalent PLMNs (networks) can be provisioned at the MME. If provisioned, the equivalent PLMNs are provided to the UE in the Attach Accept message or in the Tracking Area Update message. The PLMNs in the list are normally neighboring PLMNs with agreement of cell selection/reselection and handovers. These PLMNs must also be in the roaming agreement list.

Handover restriction list

The MME provides ability to provision a handover restriction list per each equivalent PLMN. A handover restriction list can also be provisioned for the MME's HPLMN or a network. The list basically consists of forbidden tracking area codes (TACs) or location area codes (LACs) or both for each PLMN. The list can contain up to 16 PLMNs, including the HPLMN. Each PLMN

can have up to 256 TACs and 256 LACs. The MME sends this list to the eNB and the eNB uses this information to determine a new cell for handover. If provisioned, the MME sends the list in the following S1-AP messages:

- INITIAL CONTEXT SETUP REQUEST
- HANDOVER REQUEST (to the new eNB)
- Optionally in DOWNLINK NAS TRANSPORT message if there are changes to the list.

See 3GPP TS 36.413 for specification on eNB's use of the handover restriction list. In addition to the forbidden TAC and LAC for each equivalent PLMN, the handover restriction list also contains forbidden inter-RAT handovers.

3.13.2 Roamer UE's HSS selection based on IMSI range (Feature m11314-01)

MME supports and allows roamer UEs to use IMSI range to select HSS/DRA. With this feature, roaming users that are not in equivalent PLMN are allowed.

The MME's HSS/DRA selection functions apply to roamers as well. IMSI routing can be defined per supported PLMN: home PLMN, shared network PLMN, or a roaming PLMN.

IMSI to HSS (`imsiToHss`) rule type ALL PLMN supports roaming/roamer PLMNs. It is a mapping without minimum and maximum MSIN defined. Up to 4096 different PLMNs and ALL PLMN rules can be defined.

Related descriptions

- [IMSI range-based routing to the HSS \(Feature m11008-01\)](#)

3.13.3 P-GW selection for IRAT mobility of roamers (Feature m30113-01)

The P-GW selection for IRAT mobility of roamers feature provides checks to determine if the old P-GW supports appropriate service types so that sessions are continued when the UE moves from the 2G/3G network to the LTE network. If appropriate service types are not supported, the UE is detached so that it can attach to the LTE network and a P-GW supporting correct service types is selected.

This feature supports the selection of a P-GW that supports appropriate service types for a roamer at initial attach or for a subsequent packet data network (PDN) connection. This

feature also supports changes to checks done on an already assigned P-GW when the UE is relocated from the Gn-SGSN to the MME. At the initial attach or for a subsequent PDN connectivity request, the MME selects a P-GW as follows: the MME always selects a P-GW with the collocated GGSN, that is, a P-GW supporting service types x-gn and x-s5-gtp for home subscribers and roamers that are allowed local breakout. The MME selects a P-GW that supports service types x-gp and x-s8-gtp for roamers with home routed traffic (that is, local breakout is not allowed).

For a roamer UE relocating from the Gn-SGSN to the MME, the MME does checks as follows:

1. First the MME selects a P-GW supporting SOS access point name (APN).
2. If SOS APN is not used, the MME selects a P-GW supporting IP multimedia subsystem (IMS) APN.
3. If IMS APN is not used, the MME simply picks the first P-GW in the list of packet data protocol (PDP) contexts received from the Gn-SGSN.

The MME does domain name system (DNS) query to determine the service types supported by the selected P-GW. If the P-GW is in the visited network (VPLMN) and if it does not support both service types x-s5-gtp and x-gn, the MME rejects the inter radio access technology (IRAT) tracking area update (TAU) procedure with implicit detach. If the P-GW is in the UE's selected network or in a remote network and if it does not support the service types x-s8-gtp and x-gp, the MME rejects the IRAT TAU procedure with implicit detach. If the P-GW supports appropriate service types, the MME proceeds with the IRAT TAU.

There is a dependency to the *Mode 2 DNS selection of GWs* feature.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

3.13.4 Roaming enhancement (scale, imsi-ta restriction, auth policy) (Feature m10109-02)

The *Roaming enhancement (scale, imsi-ta restriction, auth policy)* feature extends the current configuration and enforcement of roaming restrictions per public land mobile network (PLMN) that is based on the international mobile subscriber identity (IMSI) range and location area identity (LAI) and tracking area identity (TAI) to support more granular area restrictions and different roaming restrictions to different groups of subscribers of the same PLMN.

This feature provides an ability to create multiple service agreement profiles that can be

assigned to a roaming partner IMSI range and area (tracking area code (TAC) and location area code (LAC)). A service agreement profile consists of various parameters to enable/disable features and access restrictions. Additionally, this feature supports a creation of multiple access restrictions to non-access stratum (NAS) cause code mapping profiles and Diameter error code to NAS cause code mapping. Using this feature, an operator can configure per IMSI range and LAC and TAC basis:

- service agreement profile
- ability to enable local breakout per IMSI series
- NAS cause value to be sent if a UE-requested mobility management procedure (attach, tracking area update (TAU), and service request) is rejected because of an access restriction.
- NAS cause value to be sent if a UE requested mobility management procedure (attach, TAU and service request) is rejected because of HSS errors (experimental Diameter error codes).

Additional capabilities supported by this feature are

- Increase in the number of PLMNs for roaming agreements to 4096. However, the maximum number of roaming agreements supported across all the MME home PLMN and shared PLMNs is 9216 minus the MME home PLMN and the number of provisioned shared PLMNs.
- An ability to block inter radio access technology (IRAT) mobility from a different PLMN through provisioning. If IRAT mobility is blocked, the MME rejects Gn/S3 Identification Request and Context Request with cause value Request rejected.

3.13.5 LBO roamers to select S5-only S-GW (Feature m30113-03)

The *LBO roamers to select S5-only S-GW feature reduces attachment failures for a roamer with local breakout (LBO) at attach when S-GW supporting only the S5 interface is available.*

This feature includes the following S-GW selection functions for a roamer:

- Selection of an S-GW for a roamer with LBO at initial attach: the MME selects an S-GW by topological matching to the selected P-GW irrespective of the S-GW's support of S8. This ensures selection of an S-GW geographically closer to the P-GW supporting IP multimedia subsystem (IMS) access point name (APN), assuming that IMS APN is the default APN.
- Intra-MME, inter-MME, and S4-SGSN S-GW relocation: For a roamer with LBO, instead of selecting an S-GW with S5 and S8, the MME selects an S-GW using current algorithm

supported for the home subscribers, that is, the MME uses the old S-GW to find a topologically close P-GW in the UE context and then uses the P-GW to select an S-GW topologically close to the P-GW irrespective of support of S8. This method guarantees that the P-GW supporting IMS is used in the selection of a new S-GW, assuming that IMS PDN connection is the first PDN connection set up at attach.

This feature is only applicable to mode 2 selection of S-GW and P-GW. It is dependent on the *Mode 2 selection of GWs* feature.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

3.13.6 MME provisioning of default QoS profile for visiting roaming subscribers (Feature m10520-02)

The **MME provisioning of default QoS profile for visiting roaming subscribers** feature provides the benefit of limiting quality of service (QoS) for a roaming subscriber thereby giving preference to home subscribers.

This feature provides the capability to restrict roaming subscribers as to what they can request or subscribe to a QoS, irrespective of their HSS QoS parameter settings.

- The MME supports a configurable default QoS profile for roaming subscribers to allow operators to restrict roammers' QoS profiles irrespective of their QoS parameter settings in their HSS. Any values not specified in the default QoS take the HSS-provisioned values. If a roamer/subscriber was provisioned with lower settings in their HSS, those settings override the default QoS settings.
- The MME supports provisioning of QoS class indicator (QCI), Priority Level, Pre-emption capability, Pre-emption Vulnerability, Uplink APN AMBR, and Downlink APN AMBR. Any values not specified take the HSS-provisioned values.
- The MME applies the same QoS values to all the roaming UEs from a public land mobile network (PLMN). The provisioning is per PLMN.

3.13.7 Roaming QoS enhancements (Feature m10520-03)

The **Roaming QoS enhancements** feature provides enhancements to the existing base roaming quality of service (QoS) functionality.

Default roamer policy for a roamer international mobile subscriber identity (IMSI) series

For each IMSI, the MME is able to apply the local roamer QoS policy at the packet data network (PDN) connection level and at the default bearer level separately. This policy is not applicable for IP multimedia subsystem (IMS) and SOS access point names (APNs). In addition, this policy has three subsets of specific policy provisioning:

- Subset 1: Default bearer with the following QoS attributes:
 - QoS class indicator (QCI) with value range from 6-9
 - Allocation and retention priority (ARP) with value range from 1-15
 - Access point name aggregate maximum bit rate (APN-AMBR)
 - UE-AMBR
- Subset 2: Non-guaranteed bit rate (GBR) dedicated bearer policy with the following QoS attributes:
 - QCI with value range from 6-9
 - ARP priority level with value range from 1-15
- Subset 3: GBR dedicated bearer policy with the following QoS attributes:
 - QCI with value range from 2-4
 - ARP Priority Level value range from 1-15
 - GBR
 - MBR

For subset 1, the provisioning is necessary for at least one roaming QoS policy if the *Roaming QoS policy* feature is enabled.

For subset 2 and subset 3, operators can leave them empty. An empty subset 2 or 3 or both means that the operator does not support the dedicated bearer type or the dedicated bearer type is not supported for a roamer and the MME rejects the dedicated bearer establishment or rejects both types of bearers.

Default roamer policy for IMS APNs

The MME supports default roamer policy for specific IMS APNs. This policy only applies for IMS APNs. In addition, this policy has three subsets of specific policy provisioning:

- Subset 1: Default bearer policy with the following QoS attributes:
 - QCI with a value range from 5-9
 - ARP with value range from 1-15
 - APN-AMBR
 - UE-AMBR

- Subset 2: Non-GBR dedicated bearer policy with the following QoS attributes:
 - QCI with value range from 6-9
 - ARP with value range from 1-15
- Subset 3: GBR dedicated bearer policy with the following QoS attributes:
 - QCI with value range from 1-4
 - ARP Priority Level with value range from 1-15
 - GBR
 - MBR

For subset 1 of IMS APN, the provisioning is necessary if the *Roaming QoS policy* feature is enabled.

For subset 2 and subset 3, operators can leave them empty. An empty subset 2 or 3 or both means that the operator does not support the dedicated bearer type or the dedicated bearer type is not supported for a roamer and the MME rejects the dedicated bearer establishment or rejects both types of bearers.

If one of the fields in all the subsets is filled, all the fields must be filled. AMBR, GBR, and MBR cannot be zero.

For a SOS APN of E911 service, the QoS provisioning is part of the MME's local configuration for the E911 service. The MME uses the local E911 provisioning data.

Additional supported functionalities

- The MME is able to apply the local roamer QoS policy at the PDN connection level and at the default bearer and dedicated bearer levels separately.
- At the PDN connection level, operators are able to configure APN-AMBR for each requested PDN connection.
- For each default bearer, operators are able to configure
 - QCI value
 - ARP value
 - Preemption vulnerability indication (PVI)/preemption capability indication (PCI) value
 - MBR values (uplink/downlink)
- For each dedicated bearer with GBR service, operators are able to configure
 - QCI value
 - PCI/PVI value
 - GBR values (uplink/downlink)
- For each dedicated bearer with non-GBR service, operators are able to configure
 - QCI value PCI/PVI
 - MBR values (uplink/downlink)

- The MME provides an ability to turn off local roamer QoS policy control globally, so that the MME uses the QoS policies from the roamer's home HSS subscriptions and/or roamer's home policy and charging rules function (PCRF)/P-GW.
- The MME provides an ability to allow or not allow, through configuration, access to IMS APN per roaming PLMN.
- The MME validates QoS values received from the network for roaming UEs in Create Bearer Request message for dedicated bearer or non-GBR dedicated bearer setup against the provisioned QoS profile. If the provisioned QoS profile is empty, the MME rejects the dedicated bearer setup with the cause value Request Rejected Unspecified (#31).

Requirements

The *Roaming QoS enhancements* feature requires the *Base roaming QoS* feature.

Related descriptions

- [MME provisioning of default QoS profile for visiting roaming subscribers \(Feature m10520-02\)](#)

3.13.8 MME support for additional roaming QoS enhancements (Feature m10520-04)

The *MME support for additional roaming QoS enhancements* feature deals with a roamer UE requesting for a quality of service (QoS) that is higher than the provisioned default QoS profile.

This feature supports the following functionalities in relation to roamer QoS modification scenarios:

- The MME validates QoS values received from the network for a roaming UE in Create Response message for the default bearer by comparing against the provisioned default QoS profile for roamers. If the QoS values received from the S-GW are higher than the default QoS profile, the MME rejects the request by sending the non-access stratum (NAS) cause value 'EPS QoS not accepted (#37)' to the UE. However, if the QoS values received from the S-GW are lower, the MME accepts the request. This applies only for the attach procedure and does not apply for a handover or a tracking area update (TAU) with S-GW relocation.
- The MME validates QoS values received from the network for a roaming UE in Create Bearer Request message for the dedicated bearer by comparing against the provisioned

default QoS profile for roamers. If the QoS values received from the S-GW are higher than the provisioned default QoS profile, the MME rejects the request by sending a Create Bearer Response message with the cause value '#Service not supported' to the S-GW. However, if the QoS values received from the S-GW conform to the provisioned default QoS profile, the MME accepts the request.

- The MME validates QoS values for a roamer received from the network as part of a network-initiated bearer modification procedure in an Update Bearer Request message by comparing against the provisioned default QoS profile. If the QoS values received from the network are higher than the provisioned default QoS profile, the MME rejects the request by sending an Update Bearer Response message with the cause value '#Service not supported' to the S-GW. However, if the QoS values received from the S-GW conform to the provisioned default QoS profile, the MME accepts the request.
- The MME validates QoS values received from a roamer UE as part of the UE-requested bearer resource modification procedure in the Bearer Resource Modification Request message by comparing against the provisioned default QoS profile. If the QoS values received from the UE are higher than the provisioned default QoS profile, the MME rejects the request by sending a Bearer Resource Modification Reject message with the cause value '#37 EPS QoS not accepted' to the UE. However, if the QoS values received from the UE conform to the provisioned default QoS profile, the MME accepts the request.

This feature requires the base roaming QoS functionality.

Related descriptions

- [MME provisioning of default QoS profile for visiting roaming subscribers \(Feature m10520-02\)](#)
- [QoS value modifications for roamers \(Feature f10112-01\)](#)

3.13.9 Enhanced roaming restriction for IPv4v6 bearers (Feature m50051-02)

The **Enhanced roaming restriction for IPv4v6 bearers** feature supports the handling of IPv4v6 bearers in the MME when the home network of the roaming agreements does not support dual access bearer (DAB) for the IPv4v6 bearers.

Dual address bearers of a roaming UE are terminated if the MME dual access bearer support is off. Additionally, a per public land mobile network (PLMN) level DAB support is also taken into consideration before any DAB connection termination.

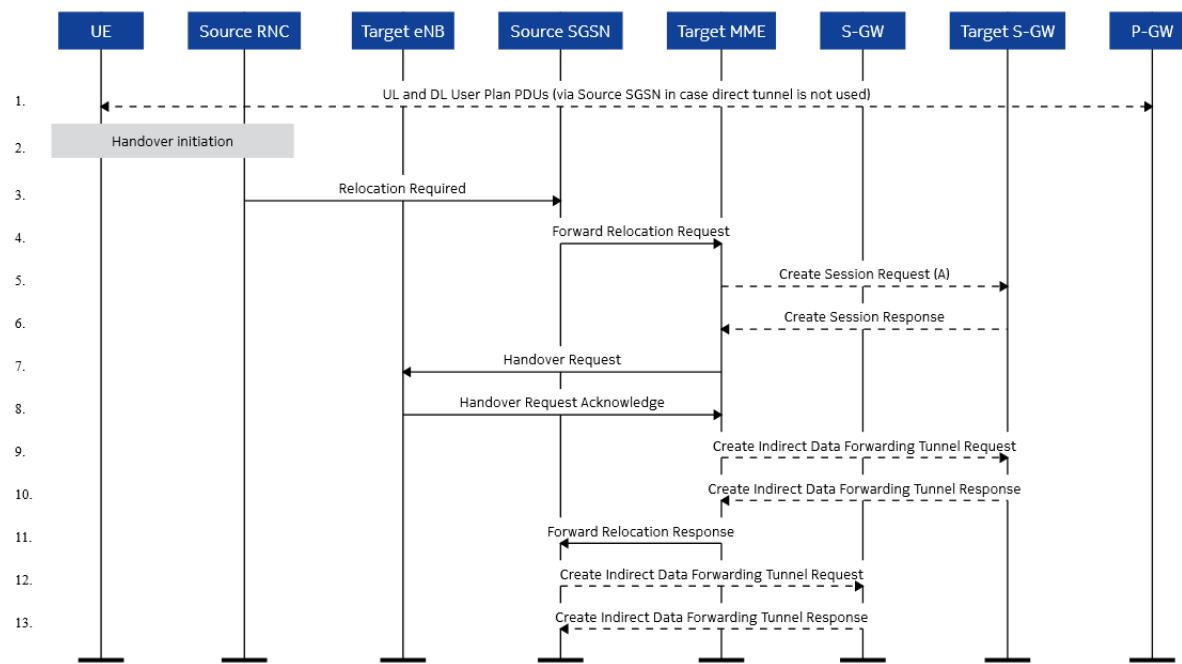
With the implementation of this feature, the existing attach, standalone packet data network (PDN) connectivity request, and inter radio access technology (IRAT) handover/tracking area update (TAU) scenarios do not significantly change. Specific packet data protocol (PDP)/PDN connections handling within the MME upon an IRAT handover/TAU changes for the list of scenarios:

1. 4G attach with ipv4 - no change
2. 4G attach with ipv6 - no change
3. 4G attach with ipv4v6 - no change
4. Standalone PDN connection with ipv4 - no change
5. Standalone PDN connection with ipv6 - no change
6. Standalone PDN connection with ipv4v6 - no change
7. Handover/TAU to 4G with v4 only - no change
8. Handover/TAU to 4G with v6 only - no change
9. Handover/TAU to 4G with v4v6 only - affected
10. Handover/TAU to 4G with v4v6 and at least one IPv4 or IPv6 - affected

For items 1 through 8, there are no anticipated scenario changes or processing changes within the MME. Admission and access controls are already in place through the existing features. Items 9 and 10 are the primary affected scenarios for this feature.

The impacts are shown in the message flow figures from 3GPP TS 23.401 v11.4.0 showing the UTRAN Iu mode to E-UTRAN inter radio access technology (inter-RAT) handover. The preparations phase, the execution phase, and a rejection case are shown. Scenarios with an S-GW relocation and without S-GW relocation are affected.

Figure 20: Inter-RAT handover preparation phase (TS 23.401)



Upon receiving the Forward Relocation Request in step 4 (A), the MME generally performs normal handover processing.

There are three primary scenarios here.

- A: None of the PDN connections to be set up have DAB.
- B: All of the PDN connections to be set up have DAB.
- C: There is a mixture of DAB and no DAB PDN connections.

Scenario A is currently supported and processes are unchanged from the current implementation.

Scenario B factors in the provisioned global DAB support and the PLMN level DAB support. If the global DAB support is not enabled, the handover is rejected.

With S-GW relocation, this rejection scenario looks like Figure *IRAT reject* (TS 23.401), except that steps 5 - 10 are skipped.

For this reject scenario, the MME rejects the handover and no handover request is sent to the target eNB.

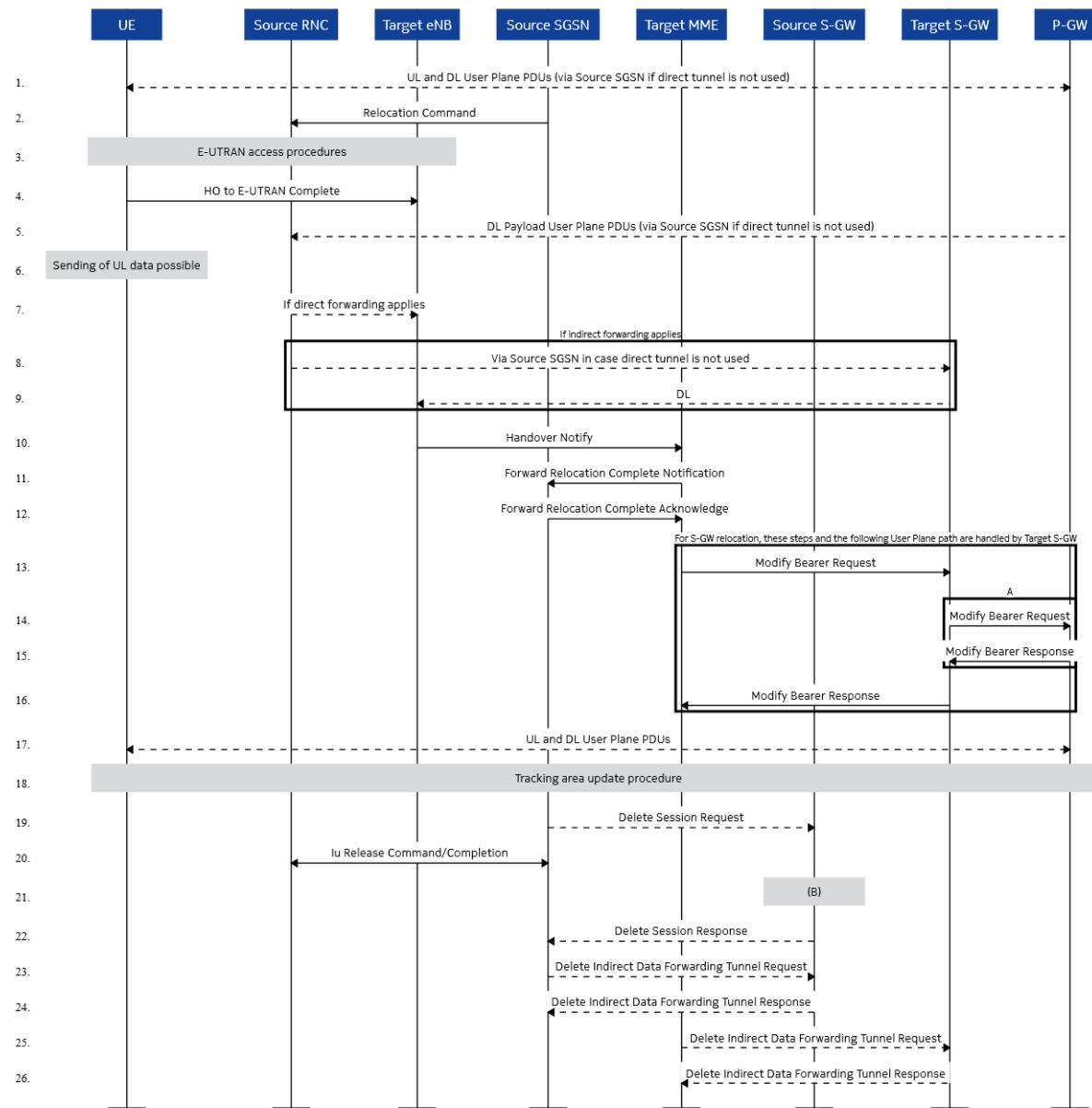
If the global DAB support is enabled, and the UE is a roamer, the PLMN level DAB support is examined by the MME. If PLMN level DAB support is not enabled, the scenario is rejected the same as if the global DAB support had been enabled. In the S-GW relocation case, no S11 Create Session Requests are sent, and in the scenario without S-GW relocation, no Handover Request is sent.

If the global DAB support is enabled and the PLMN level DAB support is enabled, the handover processing continues as normal.

Scenario C: For cases with the S-GW relocation, the MME, upon determining that there is at least one PDN connection that is not DAB, proceeds with step 4. A Create Session Request is sent for all PDN sessions (both single address and dual address sessions).

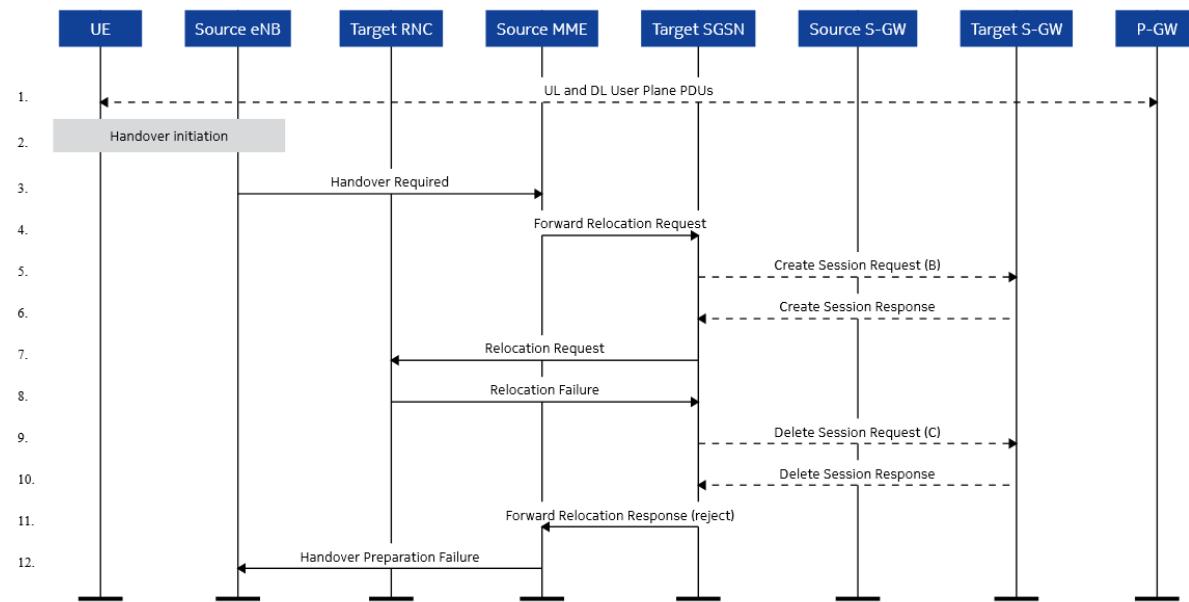
The RAB setup occurs only for PDN sessions that pass the provisioning checks. The Forward Relocation Response in step 7 contains the sessions that were successfully set up, the sessions for which setup was attempted and failed, and the sessions for which RAB setup was not attempted because of the DAB provisioning.

Figure 21: Inter-RAT handover execution phase (TS 23.401)



This enhancement feature provides no material changes within the message sequence flow for IRAT handovers. This figure is only included here for completeness.

Figure 22: IRAT reject (TS 23.401)



This feature introduces some new handling in terms of handover completion. For the scenario handover/TAU to 4G with v4v6 and at least one IPv4 or IPv6, the Create Session requests are sent to the target S-GW for all PDN connections (Step 3 (B)) in which there is an S-GW relocation. For connections that fail in RAB setup or connections for which DAB support is not allowed, the MME handoff manager (HOM) deletes the sessions (Step 7(C)). For scenarios without S-GW relocation, the MME avoids RAB setup for DAB bearers that are not accepted per provisioning, and instead treats them as failed and marked for deletion.

3.13.10 Inter-PLMN TAU and attach restrictions (Feature m10151-01)

The *Inter-PLMN TAU and attach restrictions* feature supports configuration per public land mobile network (PLMN) to enable inter-PLMN S10/S3/Gn messages to be sent to the old MME/SGSN by the new MME in case of tracking area update (TAU) Request and Attach Request with foreign globally unique temporary identity (GUTI) to get the UE context from the old MME/SGSN in a different network.

A GUTI is considered as a foreign GUTI if the PLMN ID of the GUTI does not match the PLMN ID of the serving network.

If the per PLMN option is disabled, the MME rejects a TAU Request with a provisioned cause

code instead of sending the S10/S3/Gn Context Request to the old node if PLMN ID of the old GUTI information element (IE) of the TAU Request matches a PLMN ID that is restricted for inter-PLMN TAU and attach.

In case of Attach Request with foreign GUTI, the MME does not send the S10/S3/Gn Identification Request to the old node:

- The MME sends a non-access stratum (NAS) Identification Request message to UE to get the UE international mobile subscriber identity (IMSI) to proceed with the Attach Request.
- The No form of the command is the default. The default behavior is that the inter-PLMN S10/S3/Gn Context Request and S10/S3/Gn Identification Request are not sent to the old node for TAU Request and Attach Request respectively if the PLMN ID of the GUTI matches a PLMN ID restricted for inter PLMN TAU and attach.

This feature applies to PLMNs that have roaming agreements with the serving network.

This feature can be enabled per MME basis in addition to the per PLMN option to enable inter-PLMN S10/S3/Gn messages to be sent to the old MME/SGSN.

If this feature is enabled, the MME checks the per PLMN provisioning.

By default, this feature is disabled. Also by default the per PLMN option to send inter-PLMN S10/S3/Gn messages is disabled.

When the MME receives a TAU Request, the MME derives the incoming PLMN ID from the old GUTI IE in the TAU Request message.

- If the derived incoming PLMN ID is restricted for the inter-PLMN TAU procedure, the MME rejects the TAU Request with a configured external provisioning system mobility management (EMM) cause code.
- The EMM cause code is configurable and the default is EMM cause code #9, that is, the UE identity cannot be derived by the network.

In this case, it is expected that the UE reattaches with a new MME and then IMSI number series provisioning rules are applied. This applies to both intra-LTE and inter radio access technology (IRAT) TAU Requests.

IRAT TAU is only allowed if it is enabled by this feature and also enabled by the provisioning introduced by the *Roaming enhancement* feature.

If this feature is enabled, the MME does not send the GTP Identification Request when the UE sends an Attach Request with GUTI and the GUTI PLMN ID matches the PLMN ID restricted for the inter-PLMN TAU. In this case, the MME uses the NAS Identification Request to obtain IMSI.

Related descriptions

- [Roaming enhancement \(scale, imsi-ta restriction, auth policy\) \(Feature m10109-02\)](#)

3.13.11 Forbidden PLMN using regional subscription zone codes (Feature m10135-01)

The *Forbidden PLMN using regional subscription zone codes* feature restricts a UE access to a network based on regional subscription zone codes (RSZC) in the UE subscription data.

This feature provides the ability to specify forbidden public land mobile networks (PLMNs) per UE basis, unlike roaming agreements that provide all UEs the same treatment. An RSZC is mapped to the provisioned forbidden PLMN identity (mobile country code (MCC) and mobile network code (MNC) on the MME. The MME provides provisioning of up to 4 PLMN IDs per RSZC.

The MME also provides a feature activation flag for home subscribers and also for a roaming partner.

If this feature is activated for a network, the MME checks the RSZC for the forbidden PLMNs and uses the provisioned mapping to obtain forbidden PLMNs.

Forbidden PLMNs are not included in the equivalent PLMN list (or allowed PLMN list) of the handover restriction list sent to eNB so that eNB does not allow UE's handover to the forbidden PLMNs. In addition, if the UE selects a forbidden PLMN as the serving PLMN, the MME (that is, the serving PLMN) rejects UE's mobility management requests with a provisioned non-access stratum (NAS) cause code. The default cause code is PLMN not allowed.

The MME provides local provisioning to enable/disable the forbidden PLMN using RZSC feature per MME home network (HPLMN), shared PLMN, and also for a roaming partner network of these networks.

- This feature uses the currently supported number of zone codes per network and ranges. The MME HPLMN and shared networks can each have up to 128 zone codes. Zone codes used for tracking area (TA) restrictions and forbidden PLMNs must be unique as they use the common zone codes. A zone code of the same value cannot be mapped to forbidden/allowed TAs and forbidden PLMNs.
- The MME checks for RSZC in the UE subscription data if the feature is enabled for the UE PLMN. If the RSZC that maps to a forbidden PLMN is included, the MME takes the following action:
 - If the serving PLMN (this can be the MME HPLMN or shared PLMN) is not provisioned as

forbidden, the MME proceeds with the UE's request.

- If any of the forbidden PLMNs are provisioned in the equivalent PLMN list for the UE PLMN, the MME does not include these forbidden PLMNs in the equivalent PLMN list sent to the UE in Attach Accept and TAU Accept messages
 - Forbidden PLMNs are not included in the equivalent PLMNs (EPLMNs) information element (IE) in Handover Restriction List IE of S1AP Initial Context Setup, Handover Request, or Downlink Transport messages.
 - The MME also excludes any forbidden location area identification (LAI) and tracking area identity (TAI) for these excluded equivalent networks.
 - The Handover Restriction List IE is only included in the Downlink Transport message if changes are received from the HSS or forbidden PLMN provisioning is changed.
- If the serving PLMN itself is forbidden, the MME rejects the mobility management request with the provisioned cause code for this feature.
 - A serving network can be a UE HPLMN or a visited network (VPLMN). If it is a VPLMN, the VPLMN can have roaming agreements with the UE's HPLMN.
 - If a VPLMN has no roaming agreements with the UE network, checking of these access restriction bits does not arise as none of the UEs from the network are allowed to access the VPLMN.
- The MME checks UE subscription data for the forbidden PLMN RSZC and takes action before checking the other subscription items that can cause the UE to be rejected. The forbidden PLMN checks of this feature are not applied for E911 calls. Any UE attach with emergency indication is not rejected because of forbidden PLMN checks.
- This feature does not introduce any counters. When a UE's mobility management request is rejected because of forbidden PLMN, the MME pegs an appropriate NAS cause code counter.

Use Case 1: Serving PLMN (network X) is forbidden for certain UEs of a network

MME provisioning:

- Enable the feature for the network X (this can be an MME HPLMN or a shared network).
- Provision forbidden PLMNs for RSZC 30. In this case, the network X is provisioned as a forbidden PLMN for RSZC 30.

HSS provisioning: RSZC 30 is provisioned for the UE XXXX of the network X. The national destination code (NDC) must be set to the serving network MCC and MNC.

Upon receiving a mobility management request from a UE of the network X, the MME checks for the RSZC code 30 for the subscriber of the network X.

- If the subscription data does not contain the code 30, the MME proceeds with the request.
- If the code 30 is in the subscription, the MME checks provisioned code 30 to the forbidden PLMNs mapping.
- The MME rejects the UE XYYY's request with the provisioned NAS cause code (default is Forbidden PLMN).

Use Case 2: Other PLMNs are forbidden for certain UEs of the serving network

MME provisioning:

- Enable the feature for the network X (this can be the MME HPLMN or a shared network).
- Provision forbidden PLMNs for RSZC 25. In this case, assume that networks A and B are provisioned as forbidden PLMNs for RSZC 25.

HSS provisioning: Provision RSZC 25 for the UE XYYY. The NDC must be set to the serving network MCC and MNC.

Upon receiving a mobility management request from the UE XYYY of the network X, the MME checks for RSZC 25 in the subscription data for every home subscriber.

- If the RSZC 25 is not included in the subscription data, the MME proceeds with the request.
- If the RSZC 25 is included in the subscription data, the MME checks provisioned RSZC 25 to forbidden PLMNs mapping.
 - The MME proceeds with the request as forbidden PLMN list does not contain the network X.
 - If A and B are provisioned as EPLMNs, the MME excludes these from the equivalent PLMN list sent to the UE in Attach Accept and TAU Accept messages. Additionally, the MME excludes A and B from the Equivalent PLMNs IE of Handover Restriction List IE in S1AP Initial Context Setup, Handover Request, and Downlink Transport messages.

Use Case 3: Serving PLMN (network X) is forbidden for certain UEs of a roaming partner network (network Y)

MME provisioning:

- Enable roaming for the network Y.
- Enable the feature for the network roaming partner network Y.
- Provision forbidden PLMNs for the RSZC 20. In this case, the network X is provisioned as

forbidden PLMNs for RSZC 25.

HSS provisioning: Provision the RSZC 20 for the UE YABC. The NDC must be set to the serving network MCC and MNC.

Upon receiving a mobility management request from a UE of the network Y, the MME checks the inclusion of RSZC in the subscription data of every UE of the network Y.

- If the RSZC 20 is not included in the subscription data, the MME proceeds with the request.
- If the RSZC is included in the subscription data, the MME rejects the request with the provisioned NAS cause code (default is Forbidden PLMN).

Use Case 4: Other PLMNs are forbidden for certain UEs of a roaming partner network associated with the serving network

MME provisioning:

- Enable roaming for the network Y.
- Enable the feature for the network roaming partner network Y.
- Provision forbidden PLMNs for the RSZC 35. In this case, assume that networks A and B are provisioned as forbidden PLMNs for the RSZC 35.

HSS provisioning: Provision the RSZC for a UE of the network Y. The NDC must be set to the serving network MCC and MNC.

Upon receiving a mobility management request from a UE of the network Y, the MME checks the inclusion of RSZC 35 in the subscription data for every subscriber of the network Y.

- If the RSZC 35 is not included in the subscription data, the MME proceeds with the request.
- If the RSZC 35 is included in the subscription data, the MME takes the following actions:
 - The MME proceeds with the request as forbidden PLMN list does not contain the network X.
 - If A and B are provisioned as EPLMNs, the MME excludes these from the equivalent PLMN list sent to the UE in Attach Accept and TAU Accept message. Additionally, the MME excludes A and B from the Equivalent PLMNs IE of Handover Restriction List IE in S1AP Initial Context Setup, Handover Request, and Downlink Transport messages.

3.13.12 Treating an IMSI series as home subscribers (Feature m10132-01)

The **Treating an IMSI series as home subscribers** feature is specifically intended for the operators who own multiple public land mobile network (PLMN) IDs and also when an international mobile subscriber identity (IMSI) series of a PLMN is split between operators.

Overview

With this feature, operators can provide home subscriber treatment for the other PLMN IDs that operators own. Also, when an IMSI series of a PLMN is split between operators, this feature provides a way to configure an IMSI number series for home subscriber treatment and a different IMSI series for roamer treatment.

This feature provides the ability to provision the MME:

- At the roaming agreement level, the MME treats all UEs from a PLMN either as roamers (as they are today, which is the default) or as home subscribers of the serving PLMN.
- The MME treats ranges of UE IMSIs as roamers when, at the roaming agreement level, they are to be treated as home subscribers of the serving PLMN.
- The MME treats ranges of IMSIs as home subscribers of the serving PLMN when, at the roaming agreement level, they are to be treated as roamers.

The serving PLMN can be either the home network (HPLMN) or a shared PLMN.

In addition, at the roaming agreement level and an IMSI range/tracking area identity (TAI) or location area identification (LAI) list level, this feature provides the ability to provision the MME for normal P-GW domain name server (DNS) domain derivation (as is done today, which is the default) or to override normal P-GW DNS domain derivation and use a provisioned override <mcc> and <mnc> (`epc.mnc<mnc>.mcc<mcc>.3gppnetwork.org`).

This feature does not change the S-GW DNS domain derivation.

This feature is supported for both the HPLMN and all shared PLMNs.

At the roaming agreement level

- The MME provisioning supports provisioning of another network's UEs to be treated as home subscribers of the serving PLMN.
- The MME provisioning supports override of a normal P-GW DNS domain derivation. Instead, the MME uses the provisioned override mobile country code (MCC) and mobile

network code (MNC).

Example: The provisioned override MCC and MNC is 456-789 and the access point name network identifier (APN-NI) is wap1.custx.com. The P-GW DNS APN name authority pointer (NAPTR) query uses wap1.custx.com.apn.epc.mnc789.mcc456.3gppnetwork.org.

 **Note:**

The provisioned override <mcc> and <mnc> are not used for emergency scenarios, roamer home routed scenarios, or home subscribers.

 **Note:**

The provisioned override <mcc> and <mnc> are used for roamers treated as home subscribers only when the HSS subscription data for the UE does not include an access point name operator identifier (APN-OI) replacement string.

 **Note:**

For roamers treated as home subscribers, details on the APN-OI for DNS query and GTPv2c message are described in *Local breakout enhancements (Feature m10128-02)*.

 **Note:**

The provisioned override <mcc> and <mnc> are used for roamer local breakout scenarios whether the HSS subscription data for the UE does or does not include an APN-OI replacement string.

This applies to both the gateway selection mode 1 (select a P-GW topologically close to an S-GW) and gateway selection mode 2 (select an S-GW topologically close to a P-GW).

The P-GW DNS domain derivation behavior described above only applies when the subscription PDN-GW-Allocation-Type attribute-value pair (AVP) is of the type dynamic and only applies to attach and PDN connectivity request scenarios. It does not apply to handover scenarios.

To truly provide treatment as a home subscriber of the serving PLMN, the operator must explicitly set LTE service profile and other related fields to the same values as for the actual home subscribers of the serving PLMN.

At the IMSI range/TAI list level

The MME supports provisioning of another network's UEs to be treated as home subscribers of the serving PLMN. The MME provisioning supports the override of normal P-GW DNS domain derivation. Instead, the MME uses the provisioned override MCC and MNC.

Example: The provisioned override MCC and MNC is 456-789 and the APN-NI is `wap1.custx.com`. The P-GW DNS APN NAPTR query uses `wap1.custx.com.apn.epc.mnc789.mcc456.3gppnetwork.org`.

 **Note:**

The provisioned override <mcc> and <mnc> are not used for emergency scenarios, roamer home routed scenarios, or home subscribers.

 **Note:**

The provisioned override <mcc> and <mnc> are used for roamers treated as home subscribers only when the HSS subscription data for the UE does not include an APN-OI replacement string.

 **Note:**

For roamers treated as home subscribers, details on the APN-OI for DNS query and GTPv2c message are described in *Local breakout enhancements (Feature m10128-02)*.

 **Note:**

The provisioned override <mcc> and <mnc> are used for roamer local breakout scenarios whether the HSS subscription data for the UE does or does not include an APN-OI replacement string.

This applies to both the gateway selection mode 1 (select a P-GW topologically close to an S-GW) and gateway selection mode 2 (select an S-GW topologically close to a P-GW).

The described P-GW DNS domain derivation behavior only applies when the subscription PDN-GW-Allocation-Type AVP is of the type dynamic and only applies to attach and PDN connectivity request scenarios. It does not apply to handover scenarios.

To truly provide treatment as a home subscriber of the serving PLMN, the operator must explicitly set service profile and other related fields to the same values as for actual home

subscribers of the serving PLMN.

If the UE PLMN services (`uePlmnServices`) attribute LTE roaming allowed (`lteRoamingAllowed`) is set to `false`, roaming is simply not allowed for this UE PLMN/serving PLMN pair. This cannot be overridden in any way. (It cannot be overridden by UE PLMN services attribute `lteTreatAsHomeSubscriber`. It cannot be overridden by any IMSI range services entries.)

When a UE is a roamer being treated as a home subscriber of the serving PLMN

- The roamer only attributes of the associated service agreement profile (`svcAgreementProfile`) are ignored. These attributes are:
 - `accRestGeran`
 - `accRestUtran`
 - `accRestCdma2000`
 - `accRestEutran`
 - `vplmnAllowed`
 - `networkAccessMode`
 - `vplmnLipaAllowed`
 - `vplmnCsgAllowed`
 - `s102Allowed`
- The roamer only attributes of the associated record on the UE PLMN services (`uePlmnServices`) or IMSI range services (`imsiRangeServices`) provisioning are ignored. These attributes are:
 - `imsApnQosprofileName`
 - `nonImsApnQosprofileName`
 - `custApn1QosprofileName`
 - `custApn2QosprofileName`
 - `custApn3QosprofileName`
 - `acceptDab` (in UE PLMN services only)
 - `ipV6SupportForNoDab` (in UE PLMN services only)
- The following roamer only attributes of the associated serving PLMN record on the MME PLMN form (`plmn`) are ignored (subscription data is applied). These attributes are the default quality of service (QoS) profile for visiting roaming subscribers:
 - `maxBitRateUp` (aggregate maximum bit rate (AMBR) uplink)
 - `maxBitRateDown` (AMBR downlink)
 - `qci` (QoS class identifier)
 - `arp` (allocation and retention priority)
 - `arpPciDisabled`

- `arpHiPriorityLevel`
- The destination HSS for a Treat-as-Home-Subscriber UE is based on the `imsiToHss` provisioning for the UE's IMSI.

When a UE is a roamer being treated as a home subscriber of the serving PLMN, the MME always selects the S-GW with S5 service, that is, local breakout and home routed traffic concepts do not apply. The selection of S5 only applies to attach and packet data network (PDN) connectivity request scenarios. It does not apply to handover scenarios.

The MME uses the serving PLMN EIR provisioning for the network/UEs to be treated as a home network.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

3.13.13 Local breakout enhancements (Feature m10128-02)

The *Local breakout enhancements* feature provides an ability to assign an access point name (APN) allowlist to an international mobile subscriber identity (IMSI) number series (NS).

This feature provides an ability to assign an APN allowlist to IMSI NS. The APN allowlist consists of APN network identifiers (APN-NI). The APN allowlist can only be provisioned for an IMSI series of a roaming partner of the home network or a shared network. The MME allows only local breakout (LBO) packet data network (PDN) connections to the APNs in the allowlist. This feature closes a security gap in the selection and activation of PDN activation of unauthorized APNs in the visited network when a wildcard APN is allowed for a roaming UE by allowing APNs only in the LPB APN allowlist.

The feature provides an ability to create multiple APN allowlists and assign a list to an IMSI range. Additionally, the feature supports the following capabilities if a roaming UE sends both APN operator identifier (APN-OI) and APN-NI to the MME in the Activate packet data protocol (PDP) Context/PDN Connectivity message:

- If the APN-OI from a roamer UE is the roamer UE's home network (HPLMN) OI, regardless of the LBO setting on the serving MME/SGSN, the serving MME/SGSN uses home routed architecture for this APN, unless the HSS/HLR has operator-determined barring (ODB) on the APN.

- If the APN-OI from a roamer UE is the visiting/serving network OI and if the APN is not allowed for LBO (either IMSI NS is not allowed or the IMSI NS is allowed for LBO but the APN is not in the APN allowlist for the IMSI NS), the MME/SGSN falls back to home routed architecture, that is, it selects a P-GW in the UE PLMN.
- If the APN-OI from a roamer UE is the visiting/serving network OI and if the APN is allowed for LBO (both IMSI NS is allowed for LBO and the APN-NI is in the APN allowlist for the IMSI NS), the MME/SGSN allows PDP/PDN activation based on the LBO architecture unless the roamer's HSS/HLR has ODB on the APN.
- If the APN-OI from a roamer UE is neither the roamer's HPLMN OI nor the visiting/serving network OI, the PDP/PDN session activation is rejected.

If a roaming UE does not include the APN-OI, the APN-OI setting depends on LBO or home routed traffic.

The MME takes the following actions if a roamer UE sends the APN-NI and APN-OI in the PDN Connectivity/Activate PDP Context Request messages. The following assumes that there is no ODB.

Table 20: MME actions depending on UE APN OI and APN NI

UE APN OI setting	LBO allowed	APN NI in the APN allowlist	MME actions
UE HPLMN	Yes or No	N/A	Home routed architecture
VPLMN/serving network	No	N/A	Home routed architecture
VPLMN/serving network	Yes	Yes	LBO allowed
VPLMN/serving network	Yes	No	Home routed architecture
VPLMN/serving network	No	N/A	Home routed architecture
Neither UE HPLMN or VPLMN	N/A	N/A	Reject request

The following table defines how the MME selects DNS realm for the APN fully qualified domain name (FQDN) for name authority pointer (NAPTR) query and the APN FQDN to be

sent in the GTP messages for a home subscriber:

Table 21: DNS realm selection for APN FQDN for NAPTR query, home subscriber

Home subscribers			
APN OI replacement from HSS	DNS domain override	NAPTR query APN FQDN	GTPv2C messages
		APN OI	APN OI
Yes	N/A	Use APN OI replacement	UE PLMN ID from the UE IMSI
No	N/A	UE PLMN ID from the UE	IMSI UE PLMN ID from the UE IMSI

The following table defines how the MME selects a domain name system (DNS) realm for the APN FQDN for NAPTR query and the APN FQDN to be sent in the GTP messages to treat as home subscribers. If the UE sends the APN-OI, the MME checks that the APN-OI matches the APN OI derived for the GTP messages in the following. If it does not match, the MME rejects the PDN Connectivity Request with the NAS ESM cause code #32 (Service option not allowed):

Table 22: DNS realm selection for APN FQDN for NAPTR query, treat as home subscriber

Treat as home subscribers			
APN OI replacement from HSS	DNS domain override provisioning	NAPTR query APN FQDN	GTPv2C messages
		APN OI	APN OI
Yes	Yes	Use APN OI replacement	Use provisioned DNS override
	No	Use APN OI replacement	UE PLMN ID form the UE IMSI
No	Yes	Use provisioned DNS override	Use provisioned DNS override
	No	Use VPLMN/serving network PLMN ID	UE PLMN ID form the UE IMSI

For inbound roamers with the LBO and the UE sends APN-OI matching the visited network (VPLMN) or the UE does not send APN-OI, the MME/SGSN ignores the APN-OI replacement attribute-value pair (AVP) received in the subscription data.

Table 23: DNS realm selection for APN FQDN for NAPTR query, inbound roamer

Treat as home subscribers			
APN OI replacement from HSS	DNS domain override provisioning	NAPTR query APN FQDN	GTPv2C messages
		APN OI	APN OI
Ignored	N/A	Use VPLMN/serving PLMN ID	Use VPLMN/serving PLMN ID

For inbound roamers with the LBO and the UE sends APN-OI matching the UE PLMN:

Inbound Roamers with a Home Routed APN:

If a UE sends the APN-OI, the MME checks that the APN-OI matches the APN OI derived for the GTP messages in the following. If it does not match, the MME/SGSN rejects the PDN Connectivity Request with the non-access stratum (NAS) external provisioning system session management (ESM) cause code '#32 (Service option not allowed)'.

Table 24: DNS realm selection for APN FQDN for NAPTR query, inbound roamer with home routed APN

Treat as home subscribers			
APN OI replacement from HS	DNS domain override provisioning	NAPTR query APN FQDN	GTPv2C messages
		APN OI	APN OI
Yes	Yes	Use APN OI replacement	Use provisioned DNS override
	No	Use APN OI replacement	UE PLMN ID from the UE IMSI
No	Yes	Use provisioned DNS override	Use provisioned DNS override
	No	Use UE PLMN ID from the UE IMSI	UE PLMN ID from the UE IMSI

The MME supports the provisioning as follows:

- Ability to create up to 256 LBO APN allowlists. Each list can have a maximum of 16 APNs.
- Configuration of a LBO APN allowlist to a roaming partner at the network level and also to an IMSI NS of the network.
- Ability to enable/disable the feature at the MME level and also at the UE PLMN level.
- Ability to provision the P-GW DNS realm for the roamer home routed traffic.

3.13.14 IMS/LBO related modification to HSS/P-GW override (Feature f10101-01)

The *IMS/LBO related modification to HSS/P-GW override* feature allows controlling quality of service (QoS) parameters for roamers using local breakout (LBO).

This feature adds an enhancement to existing roamer QoS-handling logic, which allows operator to skip QoS class indicator (QCI) and allocation and retention priority (ARP) values defined in operator's configurable home subscriber server (HSS) and P-GW originated QoS parameter override set in case of LBO traffic.

The enhancement gives more flexibility for operators, as they can allow voice over long-term

evolution (VoLTE) with LBO using parameters that the local network sets, but they still control visiting subscribers' roaming related to home routed scenarios.

Related descriptions

- [QoS value modifications for roammers \(Feature f10112-01\)](#)

3.13.15 IMS APN roaming control (Feature f10113-01)

The **IMS APN roaming control** feature introduces new provisioning for IMS PDN connections for roammers. This feature can be activated per roamer PLMN.

Roamer IMS PDN connection option in the service agreement profile for a PLMN indicates which IMS PDN connection is allowed for the UE. Allowed values of

`roamerImsPdnConnOption` are:

- `LBO` to allow local breakout only
- `HRT` to allow home routed traffic only
- `BOTH` to allow both LBO and HRT (default)
- `NONE` to not allow IMS PDN connection (meaning, IMS voice over PS is not supported).

The table indicates MME's behavior to determine IMS PDN connection establishment during attach and standalone PDN connectivity procedures.

Table 25: IMS PDN connection setup during attach and standalone PDN connection

Roamer IMS PDN connection option	HSS VPLMN - Dynamic - Address - Allowed AVP	MME IMS PDN connection establishment decision	Comments
LBO	Not allowed	No	MME rejects Attach Request and standalone PDN Connectivity Request for IMS PDN with provisioned ESM and EMM NAS cause code.
	Allowed	Yes	MME selects P-GW in the visited network.
HRT	Any value	Yes	MME selects P-GW in UE HPLMN.
BOTH	Allowed	Yes	MME selects P-GW in visited network.
	Not allowed	Yes	MME selects P-GW in UE HPLMN.
NONE	Any value	No	MME uses current behavior.

If MME decides to reject attach because IMS PDN connection is not allowed, it sends Attach Reject with the provisioned EMM cause code. The default value for this cause code is #19 (ESM Failure).

If MME decides to reject PDN connectivity request (both during attach and standalone PDN connectivity procedure) because IMS PDN connection is not allowed, it sends PDN Connectivity Reject with the provisioned ESM cause code. The default value for this cause code is #66 (Requested APN not supported in current RAT and PLMN combination).

The table indicates MME's behavior to determine if IMS PDN connection can stay active or not during inter-PLMN TAU:

Table 26: Roamer IMS PDN connection during inter-PLMN TAU

Roamer IMS PDN connection option	Current routing of IMS PDN connection	IMS PDN connection stays active after TAU	Comments
LBO	PDN connection is in the serving network	Yes	-
	PDN connection is in a different network	No	If all PDN connections need to be deactivated, MME rejects TAU with provisioned cause.
HRT	PDN connection is in UE PLMN	Yes	-
	PDN connection is not in UE HPLMN	No	If all PDN connections need to be deactivated, MME rejects TAU with provisioned cause.
BOTH	PDN connection is in the serving network or in UE HPLMN	Yes	-
	PDN connection is neither in the serving network nor in UE HPLMN	No	If all PDN connections need to be deactivated, MME rejects TAU with provisioned cause.
NONE	Any value	No	If all PDN connections need to be deactivated, MME rejects TAU with provisioned cause.

If MME decides to reject tracking area update procedure, it sends TAU Reject message with the provisioned EMM cause code. The default value for this cause code is #40 (No EPS bearer context activated).

This feature provides the following provisioning:

Table 27: IMS APN roaming control provisioning

Command	Parameter	Usage
uePlmnServices	imsApnRoamingControl	Enable or disable IMS APN control for roamer PLMN (by default disabled)
svcAgreementProfile	roamerImsPdnConnOption	Indicate which IMS PDN connection is allowed for the UE (by default, both LBO and HRT are allowed)
restNasMappingProfile	imsApnRoamingFailure	Provision the EMM cause code for rejecting attach (default value is #19)
restNasMappingProfile	interPlmnTauRejDueImsRoamControl	Provision the EMM cause code for rejecting TAU (default value is #40)
esmCauseCodeMapping	intErrorPdnRejectDueToNoApnsSuppEscCc	Provision the EMM cause code for rejecting PDN connectivity (default value is #66)

This feature applies to IMS PDNs only. No action is taken on non-IMS PDNs.

3.13.16 QoS value modifications for roamers (Feature f10112-01)

With this feature, the MME is able to control the QoS PCI and PVI values for roamers.

When the MME receives PCI and PVI values in the Create Bearer Request (CBR) or Update Bearer Request (UBR) message for dedicated bearers, the MME compares the PCI and PVI values with the ones in the provisioned default QoS profile, and sets the ARP-PCI and ARP-PVI values to be lower than

- values received in CBR/UBR and
- provisioned default roamer QoS profile (command `qosProfile`).

This feature is disabled by default and can be enabled using the `provPciPvi` global parameter.

Received and provisioned PCI and PVI

If the PCI value MME received in the CBR or UBR message is Enabled, and the PCI value in the provisioned default QoS profile is Disabled, the MME sets the PCI value to Disabled.

If the PVI value MME received in the CBR or UBR message is Disabled, and the PVI value in the

provisioned default QoS profile is Enabled, the MME sets the PVI value to Enabled.

Table 28: Received and provisioned PCI and PVI

QoS ARP	Higher value	Lower value
PCI	Enabled	Disabled
PVI	Disabled	Enabled

Feature interactions and dependencies

This feature has interactions with feature *IMS/LBO related modification to HSS/P-GW override (f10101-01)*.

Table 29: Feature interaction: features f10112-01 and f10101-01

f10101-01	f10112-01	MME's expected behavior
disabled	disabled	If QoS value requested by P-GW is higher than the configured value, reject Create/Update Bearer.
disabled	enabled	If priority level or QCI is higher than the configured value, reject Create/Update Bearer. If priority level and QCI comparison allows the procedure to continue, select the least value of PCI and PVI among the value requested by the P-GW and the value configured in the MME.
enabled	disabled	For LBO, allow to create or update the bearer with the QoS values given by P-GW. For HRT, if priority level or QCI is higher than the configured value, reject Create/Update Bearer. For HRT, if priority level or QCI is lower than or equal to the configured values, continue Create/Update Bearer.

Related descriptions

- [IMS/LBO related modification to HSS/P-GW override \(Feature f10101-01\)](#)
- [MME support for additional roaming QoS enhancements \(Feature m10520-04\)](#)

3.13.17 Inbound roamer QoS enhancements (Feature f10130-01)

This feature introduces enhancement to the existing roaming QoS feature by incorporating support for rejecting the received roamer GBR bearer with QCI-2 value. Received inbound roamer QCI value 2 is rejected, however, QCI-1 for voice is allowed. The feature is controlled by a global parameter.

This feature allows an operator to have greater control over roaming partners' network devices, whereby they are unable to provide specific QCI for video.

This feature is controlled by the `roamQciSuppt` global parameter. When the parameter is set to `Yes` (enabled), the MME checks the received inbound roamer GBR QCI value and if the received GBR QCI value is 2 (video), it will be rejected. This global parameter applies to the GTPv2 Create Bearer Request from the P-GW: attach and stand-alone PDN connectivity with piggyback, and TAU and handover with MME relocation.

With the default value setting of `No`, MME works as it had before the introduction of this feature.

When the feature is enabled for network-initiated bearer request scenarios, the bearer request is rejected with GTPv2 cause code #89 (Service Denied). This cause code is contained within the Create Bearer Response message. When the parameter is set to `No`, the feature is disabled, and the execution of the create dedicated bearer will proceed.

3.13.18 Autonomous local breakout for roamers (Feature f10165-01)

This feature allows MME to support local breakout for a roamer PDN connection irrespective of the setting of VPLMN Dynamic Address Allowed AVP in UE subscription data.

In order to support the feature, MME provides the following provisioning:

- autonomous local breakout on/off control at the IMSI range level
- a profile consisting of a list of APN-NI

If the locally configured APN matches the subscribed APN in the subscription profile, attach and PDN connectivity request continue even if there is no wildcard APN in the HSS subscription data.

For each APN-NI, there is a replacement APN-NI to be used for local breakout support. MME uses the APN-OI of the serving network for all DNS procedures.

Upon receiving a PDN Connectivity Request from an inbound roamer and if that APN fits a defined pattern, and comes from a defined PLMN and/or IMSI range, the MME replaces the APN-NI with a configured APN-NI and replaces the APN-OI MCC and MNC with the MCC and MNC of the MME's serving PLMN.

The VPLMN Dynamic-Address-Allowed (DAA) flag is ignored for this APN, however, the MME still honors the following settings:

- The Roamer Access to VPLMN-AP Barred bit in the Operator-Determined-Barring AVP received from the HSS.
- The VPLMN_Allowed setting provisioned on the MME in the service agreement profile.

Related descriptions

- [APN conversion and correction \(Feature f10137-04\)](#)

3.13.19 Overriding of roamer QoS (Features f10112-05 and f10112-06)

This feature enhances the existing Roaming QoS enhancements feature (m10520-03) by skipping HSS QoS values and using locally provisioned QoS values. However, the QoS values received from the GW/PCRF are accepted. The feature is UE PLMN services specific. For all other UE PLMN services combinations where this feature is not active, the old behavior applies.

The feature is controlled with command `uePlmnServices`, parameter `useLocallyProvQoS`. When parameter `useLocallyProvQoS` is set to `true`, the MME always uses the locally configured QoS profile and the HSS QoS subscription values are ignored.

3.13.20 Overriding of roamer QoS enhancements (Feature f10112-07)

This feature enhances the Overriding of roamer QoS (Features f10112-05 and f10112-06) feature by introducing the support for the homers.

This feature is controlled with command `uePlmnServices`, parameter `useLocallyProvQoSForHomers`. When parameter `useLocallyProvQoSForHomers` is

set to true, the MME always uses the locally configured QoS profile for the homers. And the HSS QoS subscription values are ignored. By default, this feature is disabled.

This feature is applicable for both homers and special roammers.

3.13.21 MME support for roammers QoS enhancements (Feature f10112-04)

This feature enhances roamer QoS by applying locally configured default QoS for roammers only towards RAN. This is not applied to gateways.

When this feature is enabled, the MME applies the lowest QoS values (QCI, ARP and AMBRs) after taking inputs from:

- locally configured roamer QoS value.
- subscribed QoS value.
- QoS values received from the gateway from inbound roamer at the PDN connection level and at the default bearer for a defined IMSI ranges.

The lowest possible QoS value is only sent to the RAN and the UE, and is not applied to the gateways. In this case, the network QoS is capped, not ignored.

The MME applies the capped QoS values upon receiving QoS values in the Create Session Response message from the S-GW and sends the lowest capped values towards the UE and the RAN.

For example, when the QCI value is 9 on the local MME, the QCI value on the HSS is 6 and the QCI value on the P-GW/PCRF is 7. The MME sends Create Session Request message with QCI=6. The P-GW/PCRF returns QCI=7. Then the MME sends QCI=9 to the UE and RAN.

Another example, when the QCI value is 6 on the local MME, the QCI value on the HSS is 7 and the QCI value on the P-GW/PCRF is 8. The MME sends Create Session Request message with QCI=7. The P-GW/PCRF returns QCI=8. Then the MME sends QCI=8 to the UE and RAN (capping).

3.13.22 MME support for enhancements to QoS values modifications for roammers (Feature f10112-09)

This feature provides the global parameter `applyLocallyProvQosValuesForHrt` to control whether the MME applies the QCI/ARP/PCI/PVI values from the locally provisioned QoS values for HRT scenarios if the received QCI/ARP/PCI/PVI values are

different. By default, this feature is disabled. This feature applies only to the dedicated bearers.

3.13.23 MME support for multiple-home PLMN - phase 1 (Feature f10193-01)

This feature supports the provisioning of the MME with PLMN IDs other than the home PLMN with type multiple-home PLMN, and treats them as home subscribers.

With this feature:

- All configurations in the home PLMN are applicable to the multiple-home PLMNs.
- The MME supports creating a multiple-home PLMN association between a UE whose PLMN is a shared-network PLMN and the MME home PLMN serving PLMN, and a UE whose home PLMN is the MME home PLMN and serving PLMN is a shared-network PLMN. The `multipleHomePlmnName` can be other network, serving network or home network (as long as it is a different PLMN name than the `servedPlmnName`).
- The MME communicates with the rest of the NFs, for example, the HSS, the S-GW and the P-GW, uses the home/serving PLMN ID for the queries or the messages. However, the IMSI of the multiple-home PLMN ID is always used.
- The RAN nodes are configured only with the home PLMN ID, and the RAN only broadcasts the home PLMN ID. The MME does not include the multiple-home PLMN IDs in the setup messages.

3.13.24 CMM support for roaming - phase 2 (Feature f20028-02)

This feature supports inter-PLMN mobility for roaming both in idle mode and connected mode.

The AMF supports the following functionalities:

- The AMF supports inter-PLMN/intra-PLMN 5GS to EPS handover via N26 interworking for roamer.
- The AMF supports inter-PLMN/intra-PLMN EPS to 5GS Handover via N26 interworking for roamer.
- The AMF supports inter-PLMN 5GS to EPS idle mode mobility via N26 interworking for roamer.
- The AMF supports inter-PLMN EPS to 5GS idle mode mobility via N26 interworking for

roamer.

- The AMF supports inter-PLMN inter-AMF idle mode mobility.
- The AMF supports inter-PLMN inter-AMF N2 Handover.
- The AMF supports V-SMF selection during inter-PLMN mobility – idle and connected mode.
- The AMF supports inter-PLMN PCF support based on provisioning.
- The AMF supports handover and session continuity for data, VoNR and EPS fallback and emergency service for roamer.
- The AMF supports reselection of H-SMF.
- The AMF and MME supports inter-PLMN mobility based on provisioning.

 **Note:**

The LBO PDUs are rejected during inter-PLMN connected mode mobility except the emergency LBO PDUs.

The feature does not support the following functionalities:

- Roaming support for Non-3GPP Access (N3IWF)
- Roaming between 5G 3GPP access and LTE/EPC non-3GPP access (ePDG)
- Slice-based roaming restriction
- I-SMF interactions for roamers

The feature does not impact the following functionalities:

- SMS (SMSF handles roaming restrictions)
- Location based call flows
- N2 and Xn handover call flows

3.14 Network sharing

Features enabling network sharing (GWCN and MOCN), equivalent PLMNs and pooling.

3.14.1 Network sharing (Feature m10902-01)

The *Network sharing* feature allows different core network operators to connect to a shared radio access network (RAN). The operators do not only share the radio network elements, but can also share the radio resources themselves.

The network sharing is a way for operators to share deployment costs for mobile networks, for example, in the rollout phase of the LTE. Support of the network sharing requires additional functionalities on the eNB and MME. Starting in Release 8, all E-UTRAN and UTRAN capable UEs are required to comply with network sharing requirements, among them the public land mobile network (PLMN) selection and reception of network sharing related system information.

The network sharing allows different core network operators to connect to a shared radio access network. The operators do not only share the radio network elements, but can also share the radio resources themselves. In addition to this shared radio access network, the operators might or might not have additional dedicated radio access networks.

3GPP TS 23.251 defines two architectures to be supported by the network sharing. In both architectures the radio access network is shared. The first architecture is referred to as Gateway Core Network (GWCN), in which core network elements such as MSCs, SGSNs and MMEs are also shared. The second architecture is referred to as the Multi-Operator Core Network (MOCN) configuration, in which only the radio access network is shared.

This feature supports both the GWCN and MOCN. For the GWCN, this feature supports a shared MME and a possibly shared S-GW/P-GW. For the MOCN, the impact to the MME is minimal; the eNB is responsible for most of the functionality.

In addition to the GWCN and MOCN as defined in 3GPP TS 23.251, this feature also supports a variant of GWCN, in which the MME and possibly the S-GW/P-GW are shared, but the radio access network is not shared. This configuration might be useful in the public safety sector, where the public safety agents can own and operate their respective E-UTRAN radio access networks, but share the evolved packet core (EPC) with a commercial LTE operator.

Figure 23: GWCN configuration

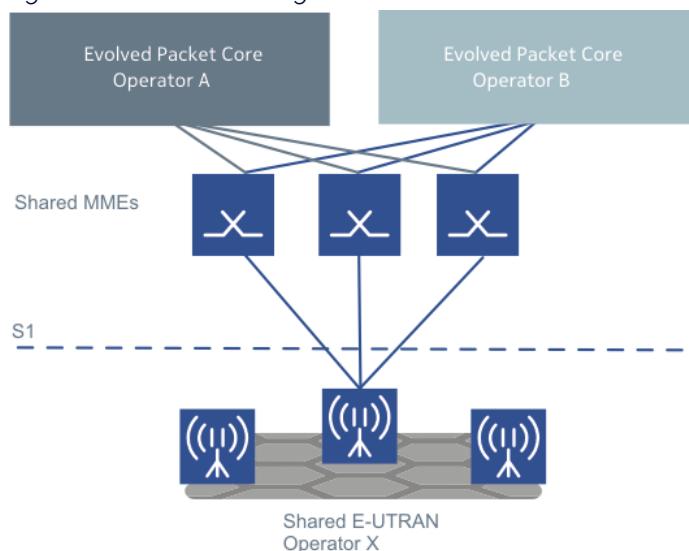
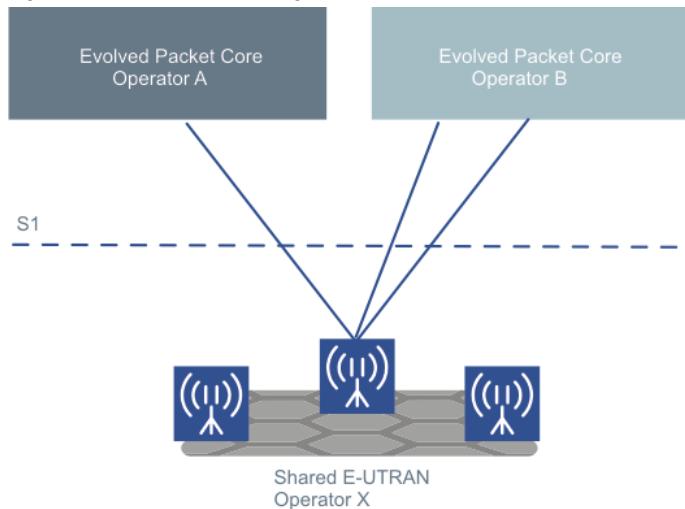


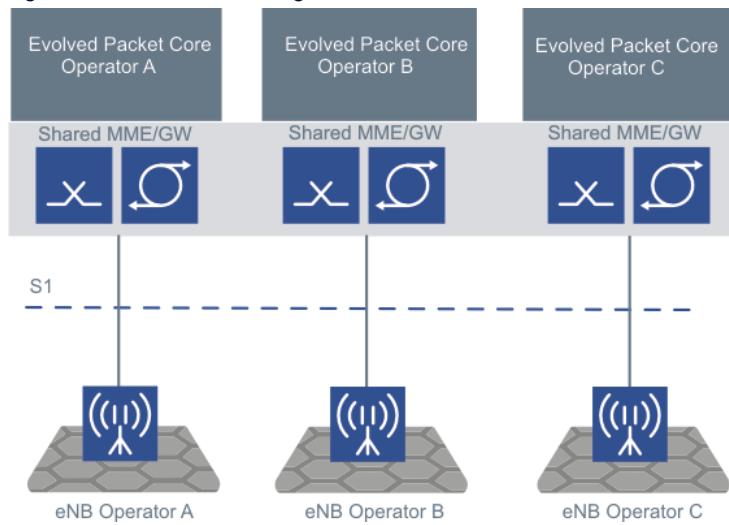
Figure 24: MOCN configuration



In the MOCN configuration, the system information broadcasted in each shared cell contains the PLMN ID of each operator and a single tracking area code (TAC) that is valid within all the PLMNs sharing the radio access network. For a shared RAN, the operators that share the RAN are the same for all cells in a tracking area.

The variant of GWCN configuration is shown in the figure.

Figure 25: GWCN configuration variant



3.14.2 15 equivalent PLMNs (Feature m10104-01)

The 15 equivalent PLMNs feature supports up to 15 equivalent PLMNs on the MME-only configuration.

The MME-only configuration also supports the provisioning of 20 forbidden tracking area

codes (TACs) and 20 location area codes (LACs) for each equivalent public land mobile network (PLMN) and home PLMN.

This feature changes only the MME scaling, not any call processing procedures.

The equivalent PLMNs list is defined in 3GPP TS 24.301 section 5.3.4.

With this feature, the network scales better because the feature provides an ability to operate with several network sharing partners.

3.14.3 MME support for dedicated core network (Feature f11601-01)

This feature enables an operator to deploy multiple dedicated core networks (DCN) within a PLMN with each DCN consisting of one or multiple CN nodes. Each DCN may be dedicated to serve specific types of subscriber. There can be several motivations for deploying DCNs, for example, to provide DCNs with specific characteristics/functions or scaling, to isolate specific UEs or subscribers (such as M2M subscribers, subscribers belonging to a specific enterprise or separate administrative domain).

A DCN comprises of one or more MME and it may comprise of one or more S-GW/P-GW/PCRF. This feature enables subscribers to be allocated to and served by a DCN based on subscription information (UE Usage Type).The specific functions are for routing and maintaining UEs in their respective DCN.

The following deployment scenarios are supported for DCN:

- DCNs may be deployed to support one RAT only (only dedicated MMEs are deployed to support E-UTRAN and dedicated SGSNs are not deployed), to support multiple RATs, or to support all RATs.
- Networks deploying DCNs may have a default DCN, which is managing UEs for which a DCN is not available or sufficient information is not available to assign a UE to a DCN. One or multiple DCNs may be deployed together with a default DCN that all share the same RAN.

The following mobility management procedures are enhanced to support DCN:

- Attach
- TAU
- Handover

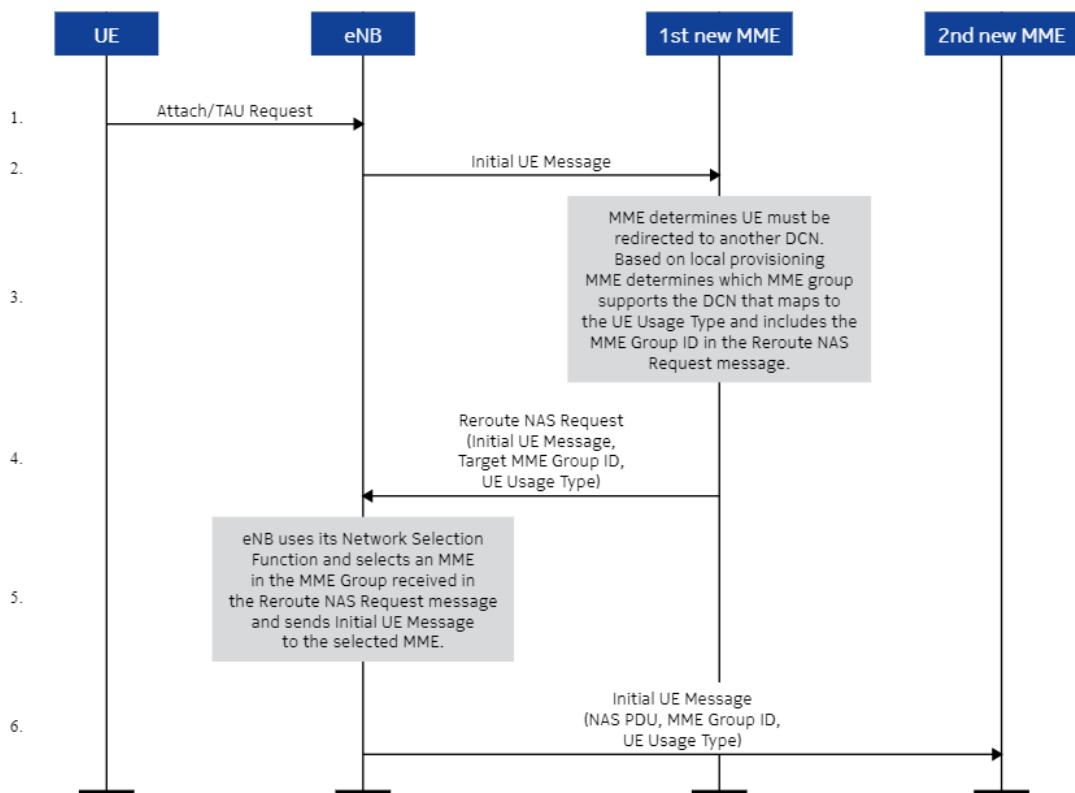
Also, the following protocols are enhanced to support DCN:

- S1-AP: The Reroute NAS Request message is introduced to enable the MME to request

for a rerouting of the Initial UE Message to the MME in the indicated DCN. The figure below shows the NAS message redirection.

- S10: The UE usage type IE is included in Forward Relocation Request, Context Response, and Identification Response.
- S6a: Authentication Information Request (AIR) and Authentication Information Answer (AIA) changes.
 - The Send UE Usage Type flag is introduced in AIR-Flags of AIR to indicate to HSS that MME supports DCN and to send the AVP UE-Usage-Type in AIA.
 - A feature bit (Feature-List-Id 2 *Table 7.3.10/2 of TS 29.272*) is introduced to indicate to HSS that MME supports Dedicated Core Network. The feature is applicable to ULR/ULA and IDR/IDA.
 - The UE-Usage-Type AVP is introduced in Subscription Data AVP.

Figure 26: NAS message redirection



Additionally, the MME is required to support selection of new MME and S-GW in a DCN supporting UE Usage Type using DNS procedures. When using DCN, the character string “+ue-<ue usage type>” is appended to the “app-protocol” name for the interfaces applicable (S10, S5, S8, S11) to DCN.

The <ue-usage-type> contains one or more UE usage type values.

Overview

A high level overview for supporting DCNs is provided below:

- An optional subscription information parameter (`ueUsageType`) is used in the selection of a DCN. The HSS provides the `ueUsageType` parameter value in the subscription information of the UE to the MME. MME selects DCN based on the operator's configured (UE Usage Type to DCN) mapping.
- If MME does not support the specific DCN, MME redirects the UE to another DCN by sending a new S1AP message Reroute NAS Request to RAN.
- If MME supports the specific DCN, MME is required to support selection of new MME, S-GW and P-GW in a DCN supporting UE Usage Type using DNS procedures.
- If the configuration shows no DCN for the specific UE Usage Type value in the subscription information, the serving MME/SGSN serves the UE by the default DCN.

3.14.4 MME support for dedicated core networks - mode 2 P-GW selection (Feature f11601-02)

This feature provides MME support for P-GW selection based on UE Usage Type in conjunction with MME support for redirection of UEs to a dedicated core network based on UE Usage Type.

The feature only applies to gateway selection mode 2. It is also applicable for home UEs and roamers treated as home UEs.

3.14.5 MME support for dedicated core networks - mode 1 (Feature f11601-03)

This feature adds support for gateway selection mode 1 for dedicated core network.

When the dedicated core networks mode 1 feature is activated, the MME selects the S-GW and P-GW for a UE that has a UE usage type with service parameters (app-protocol) appended with string `+ue<ue usage type>`.

If there is no resource record (RR) with string `+ue<ue usage type>` or the MME fails to any node with the string, the MME selects a node without the usage type string within the limits of already supported reselections. The S-GW selection applies also for the S-GW relocation due to idle mode mobility or handover, and when a UE moves from a non-DCN area to a DCN area.

3.14.6 MME support for assigning UE usage type (Decor) on IMSI range basis (Feature f11601-06)

This feature allows the CMM to define the UE usage type (UUT) based on local provisioning on a per-IMSI-range basis. With this feature, operators can provide Décor service without HSS functionality.

When this feature is activated and the UE matches an IMSI range with a valid UUT, the provisioned UUT is used for dedicated core network services. Otherwise, if the HSS includes the UUT in S6a functionality, the CMM uses UUT based on subscription data. When the UUT is added to or removed from an IMSI range record, the update can take effect at the next UE reattach or TAU or service request. All external messages, S11, S10 and N26, include the subscribed UUT regardless of whether the CMM uses IMSI-range-based UUT or subscribed UUT.

The Décor service applies only for a UE in its home PLMN, shared PLMN, or treat-as-home subscriber PLMN.

3.14.7 MME support for local provisioning of UE usage type based on 5G subscription (Feature f11601-07)

This feature extends feature *MME support for assigning UE usage type (Decor) on IMSI range basis (Feature f11601-06)* to allow local assignment of UE usage type based on 5G subscription data and/or 5G NAS capability.

The MME provisioning in `imsiRangeServices` and `uePlmnServices` defines override profiles for UUTs to be assigned to the UE. This UUT overrides any UUT that has been provided by the HSS. New flags are added to define whether the 5G subscription data and/or 5G NAS capable are used for UUT override. The use case for this feature is a network overlay. The operator wants the new MME to be able to register and provide service to 5G-capable UEs, which currently trying to access the 4G network since they are out of 5G coverage, while reassigning legacy UEs to an underlay MME network. The Décor reroute moves the legacy UEs to the underlay, with the UUT being assigned through local provisioning at the overlay MME. The network is set up that the RAN initially directs unknown UEs to the overlay MME.

3.14.8 MME support for dedicated core network enhancement (Feature f11601-08)

When this feature is enabled, the MME can obtain the UE usage type (UUT) for UEs coming from the SGSN through the Gn or S3 interface and use the UUT to select the S-GW and determine whether the UE should be rerouted.

When this feature is enabled,

- the MME retrieves the UUT from the SGSN in the Context Response, Forward Relocation Request, and Identity Response messages. For 3G to 4G Gn or S3 TAU, if the MME cannot determine whether the UE is assigned a UUT from the Gn and S3 message, the MME sends the S6a:AIR message to request the UUT from the HSS. If the MME issues an AIR as part of the procedure, the MME carries out the authentication with the UE. The MME then uses the UUT to select the S-GW and P-GW per existing functionality. The MME also uses the UUT to determine whether the UE should be rerouted to another MME per existing functionality.
- the MME sends the UUT to SGSN in the Forward Relocation Request, Context Response, and Identity Response messages.

The settings for the *MME support for assigning UE usage type (Decor) on IMSI range basis (Feature f11601-06)* feature take precedence over this feature for the S-GW and P-GW selection and MME reroute decisions.

The current Décor functionality is not supported for inbound roammers and is not supported in this feature. Gn-based IRAT handover is not supported.

3.14.9 IMSI and TAI specific EPLMN lists (Feature f10910-01)

The feature introduces the MME sending equivalent public land mobile network (EPLMN) to all users or IMSI segment or specified PLMN when UE attach in the specified TAI.

The feature makes it possible for the UE to treat a group of PLMNs, that is, PLMN codes are broadcasted by the networks, in the same manner. The feature allows the UE to treat different radio systems broadcasting different PLMN codes or networks located in different countries as belonging to the home network operator.

The EPLMN list provides a list of PLMNs which are equivalent for the currently serving PLMN. In the MME, the subscriber's IMSI analysis points to a certain PLMN, and the corresponding equivalent PLMN list is sent to the UE at the end of the attach (Attach Accept) and tracking

area update (Tracking Area Update Accept) procedures. The EPLMN list is also sent to the eNB in the Initial Context Setup Request and the Handover Request S1AP messages to avoid unnecessary network selection attempts made by the radio network.

The feature applies to serving PLMN and roamer PLMNs. A maximum of 16 EPLMNs are supported in a list.

3.14.10 MME support for customization of HRL equivalent PLMN list (Feature f10910-02)

The MME supports customization of the HRL equivalent PLMN list when the global parameter `sendEquivalentPlmnListOnlytoEnbInHandoverRestrictionList` is set to Yes.

The MME supports and allows configuration of the equivalent PLMN for homers and roamers in both the `uePlmnServices` and `imsiRangeServices` commands. However, the equivalent PLMN list is sent only to the eNB in the handover restriction list. The equivalent PLMN list is suppressed while being sent to the UE.

By default, the feature is disabled by setting the global parameter `sendEquivalentPlmnListOnlytoEnbInHandoverRestrictionList` to No. When the global parameter

`sendEquivalentPlmnListOnlytoEnbInHandoverRestrictionList` is set to Yes, the MME suppresses the equivalent PLMN list to the UE and sends the equivalent PLMN list to the eNB in the handover restriction list which is configured by setting the `ePlmnListNameEnb` parameter in the `uePlmnServices` and `imsiRangeServices` commands.

When the global parameter

`sendEquivalentPlmnListOnlytoEnbInHandoverRestrictionList` is set to No and the global parameter `ePlmnPerImsiTaiRange` is set to Yes, the MME sends the equivalent PLMN list to the UE and the eNB by setting the `ePlmnListName` parameter in the `uePlmnServices` and `imsiRangeServices` commands.

3.14.11 Enhanced triple access scenarios - delivery (Feature f14605-03)

With this feature, some MME/SGSN (serving in 2G/3G/4G) enhancements are supported.

For the SGSN part, see *Enhanced triple access scenarios - delivery (f14605-03)* in the SGSN

User Guide and the SGSN Feature Overview.

3.14.11.1 Pooling

The set of core network elements serving the same geographical area (connected to the same radio nodes) is referred to as a pool.

When core network operates in a pool, radio access nodes are connected to several CMMs. When pooling is enabled, the radio nodes try to maintain the initially chosen core network elements for the UE as long as the UE stays within the pool area. As a result, when a UE moves between different access types (2G/3G and 4G) within the same geographical area covered by the same core network pool, radio access chooses the same CMM. For example, radio access chooses the collocated SGSN or MME which previously served the UE.

When the MME/SGSN is deployed, the configuration of the collocated SGSN that the MME reads is as follows:

1. PLMN-ID (MNC + MCC)
2. LAC
3. NRI

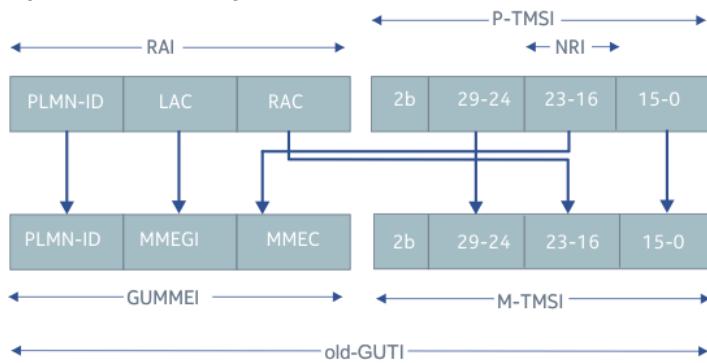
During the S1 setup procedure, the MME adds in the S1 Setup Response message the served GUMMEIs that correspond to SGSN's configuration (3GPP TS 36.413):

- one PLMN-ID for each PLMN SGSN application
- one MMEGI for each LAC SGSN application, and
- one MMEC for each NRI SGSN application

In case local SGSN's NRI length is 0, the SGSN does not belong to a pool and the MME does not encode alternative served GUMMEIs into the S1 Setup Response message.

2G/3G identifiers are mapped to 4G GUMMEI as follows:

Figure 27: Mapping of 2G/3G identifiers to LTE GUMMEI



The MME application updates the changed alternative served GUMMEI to the eNB, when the SGSN belongs to a pool (NRI length >0) and there is a change in the following SGSN configuration:

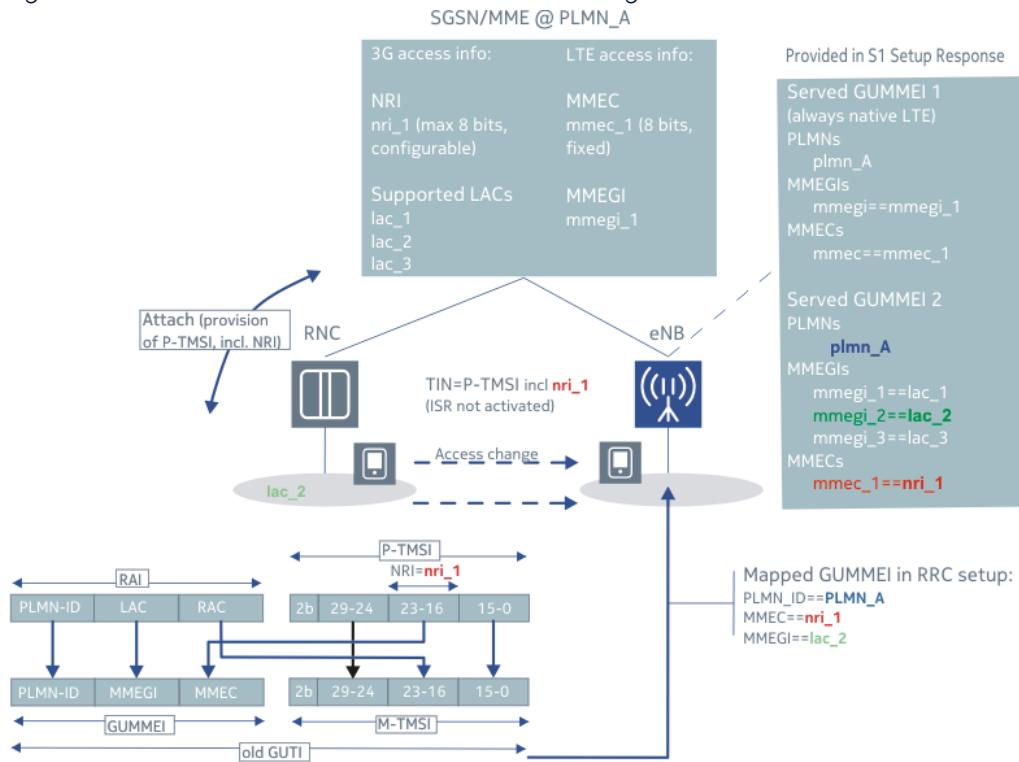
- PLMN-ID
- LAC configuration
- NRI configuration

In addition, if local SGSN's NRI length has earlier been set to 0 (for example, the SGSN is not pooled) and it is later added to the pool by configuring an NRI value, the MME updates the alternative served GUMMEIs to the eNBs, even though the alternative served GUMMEIs is not signaled to E-UTRAN during the S1 Setup procedure.

The MME encodes the new served GUMMEIs configuration to the MME Configure Update message, sends it to the eNB and starts a timer to guard the response. The eNB acknowledges with the MME Configuration Update Acknowledge message. Before this message is received, the MME does not initiate new configuration update procedure.

The MME selection in idle mode IRAT change to LTE is illustrated:

Figure 28: MME selection in idle mode IRAT change to LTE



In case local SGSN's NRI length is 0, change in local SGSN applications' PLMN-ID and/or LAI configuration does not trigger the MME configuration update procedure.

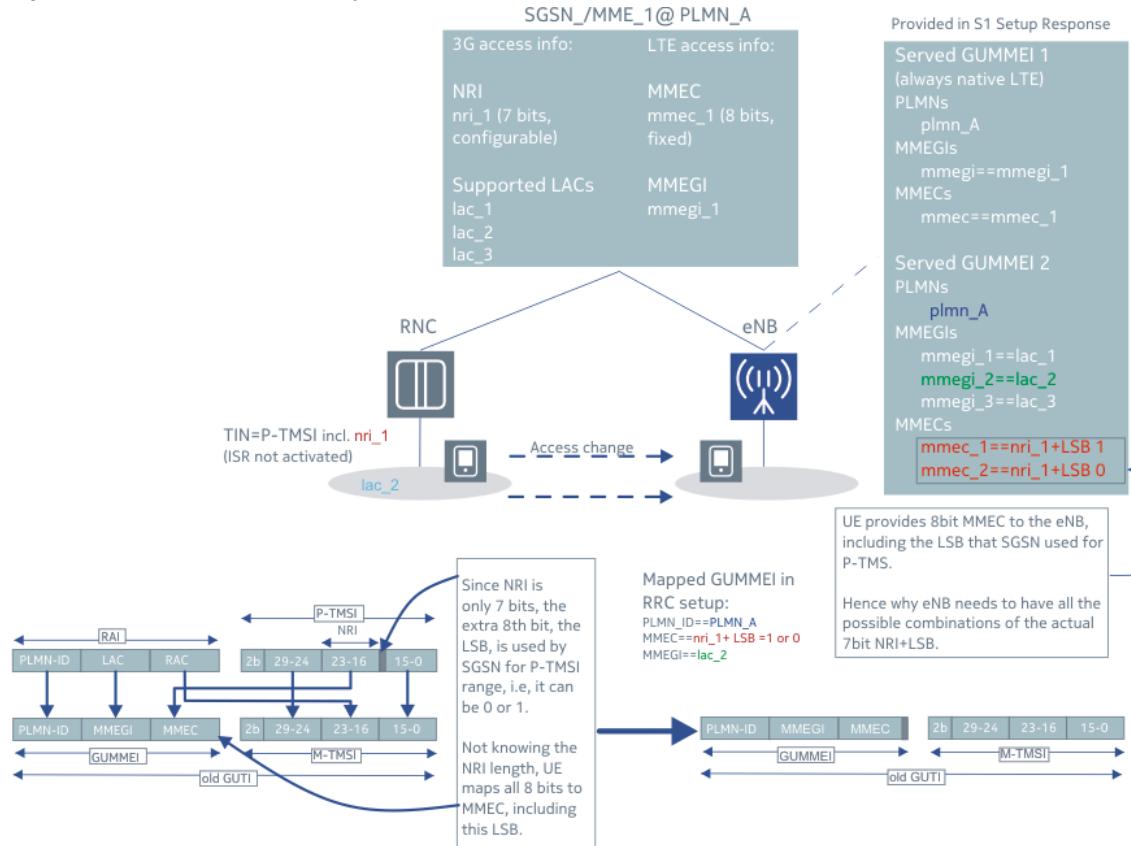
To ensure inter-operability between 2G/3G and LTE pools, the NRI does not exceed 8 bits in length. This is due to the fact that the NRI is mapped into 8-bit MMEC and if NRI value used in 2G/3G is longer than 8 bits, the excess bits get lost in the mapping process.

NRI is allowed to be shorter than MMEC. The non-NRI parts of the P-TMSI that are not used to identify the core network node which are used to identify the subscriber. If the NRI is 7 bits in length, for example, the 8th bit will be part of subscriber's P-TMSI which is randomly allocated for each subscriber. Upon access change, when NRI which is shorter than 8 bits is mapped into 8-bit MMEC, these non-NRI bits of P-TMSI are included.

The MME includes all the possible combinations of mapped MMECs in the S1 Setup Response and MME Configuration Update messages. For example, in case of 7-bit SGSN NRI, the MME actually includes two MMECs within the non-LTE served GUMMEI IE: <7-bit-nri-value> + 0 and <7-bit-nri-value> + 1. This enables the eNB to always fixedly read 8-bit MMEC and find the match from the CN configuration, no matter which value the 8th P-TMSI has.

The following figure illustrates the MME functionality via example of 7-bit-NRI:

Figure 29: MME functionality via example of 7-bit-NRI



The MME reads the configured NRI length by using the global parameter `nriLength`. Based on the read length, the MME calculates all 8-bit combinations that are possible to be received by eNB. For example, if the length difference is 1 bit, the MME indicates two alternative MMECs:

- <configured_NRI_value_of_7bits + 0>
- <configured_NRI_value_of_7bits + 1>

If the length difference is 2 bits, the MME needs to indicate four alternative MMECs:

- <configured_NRI_value_of_6bits + 00>
- <configured_NRI_value_of_6bits + 01>
- <configured_NRI_value_of_6bits + 10>
- <configured_NRI_value_of_6bits + 11>

This rule applies also to 3-bit difference, similarly.

When the global parameter `includeMappedGummei` is set to `Yes`, sending the served GUMMEIs that correspond to SGSN's configuration in S1 Setup Response message and MME Configuration Update message is enabled. Then the MME includes SGSN's mapped served GUMMEIs in any next S1 Setup Response message. Any change in SGSN's configuration

triggers a Configuration Update message that also includes the SGSN's mapped Served GUMMEIs.

In IRAT TAU or IRAT attach, the MME derives the values of NRI, MNC, MCC, LAC and RAC corresponding to UE's previous location from old-GUTI. In IRAT handover, with a target 3G RNC, the MME checks if target-RNC (RNC-id, MNC, MCC) is configured in the collocated SGSN. If the target-RNC is configured in the collocated SGSN (the MME and the SGSN belong to the same MME/SGSN in intra-CMM mobility), then no DNS query is performed to derive the source SGSN (for IRAT TAU or IRAT Attach) or target SGSN (for IRAT handover).

For handovers, find target-RNC (RNC-id, MNC, MCC) by using the `cmm rnc` command.

As part of the feature, parameters `nriLength`, `sgsnId`, `sgsnPoolId`, `nullNri`, `s4Func` and `s6dDiameter` are moved to the global parameter (gParms) group.

3.14.11.2 Target Identification IE in GTPv1 Forward Relocation Request message

When different versions of 3GPP TS 29.060 are used, different encoding/decoding is used in Target Identification IE in GTPv1 Forward Relocation Request message.

3GPP TS 29.060 supports 3 different versions in encoding/decoding of Target Identification IE in GTPv1 Forward Relocation Request message. The SGSN controls this encoding/decoding by using the `prFile` parameter `gtpTargetIdEncoding`:

Table 30: 3GPP versions and corresponding `gtpTargetIdEncoding` parameters

3GPP versions	<code>gtpTargetIdEncoding</code> value
Older than CR0668	0
Between CR0668 and CR0808	1
Newer than CR0808	2

When 3GPP versions are between CR0668 and CR0808 (and the `gtpTargetIdEncoding` parameter is set to 1), MNC+MCC is encoded/decoded as follows:

Table 31: MNC+MCC encoding/decoding for 3GPP versions between CR0668 and CR0808

octet1	MCC2	MCC1
octet2	MNC1	MCC3
octet3	MNC3	MNC2

When 3GPP versions are older than CR0668 (and the `gtpTargetIdEncoding` parameter is set to `0`), an extra controlled byte is used in the Target-Id IE.

When 3GPP versions are newer than CR0808 (and the `gtpTargetIdEncoding` parameter is set to `2`), MNC+MCC is encoded/decoded as follows:

Table 32: MNC+MCC encoding/decoding for 3GPP versions are newer than CR0808

octet1	MCC2	MCC1
octet2	MNC3	MCC3
octet3	MNC2	MNC1

To support handover scenarios between the MME and the SGSN, the encoding/decoding of Target Identification IE is configured to use the same format in both the MME (`gParms.gnTargetIdFormat`) and the SGSN (`prFile` parameter `gtpTargetIdEncoding`).

To ensure interoperability between the MME and the SGSN in 4G to 3G handovers, parameters are configured as follows:

Table 33: Gn target ID format based on GTP target ID encoding value

gtpTargetIdEncoding (for SGSN)	gnTargetIdFormat (for the MME)
0 (default)	ASN.1 With Choice/Options Octet (default)
1	GTP with RANAP-order of PLMN Digits
2	GTP with CN-order of PLMN Digits

 **Note:**

The default value of `gnTargetIdFormat` is changed from GTP with CN-order of PLMN Digits to ASN.1 With Choice/Options Octet.

3.15 Inter radio access technology (IRAT)

These features allow the UE to move between various technology networks.

3.15.1 Support for Gn HSAPA handoffs - RAU (Feature m30100-01)

The **Support for Gn HSAPA handoffs - RAU feature** enables inter radio access technology (IRAT) mobility and session continuity when the UE moves between the LTE and 2G/3G networks.

Interworking with pre-Release 8 WCDMA core feature deals with supporting Gn interface with 3GPP pre-Release 8 3G SGSN. The Gn interface is the reference point between the SGSN and MME when S3 interface is not supported. The Gn interface is the reference point between the SGSN and P-GW when S4 interface is not supported. The Gn interface enables mobility handling and inter-RAT handover when the SGSN (3G SGSN) does not implement S3/S4 interfaces.

The Gn interface between the SGSN and MME is a control plane interface and the protocol is GTPv1-C GTP tunnels are used between two nodes communicating a GTP based interface to separate traffic into different communication flows. This feature covers support for only 3GPP pre-Release 8 interworking functionality, in particular it covers the scenarios/procedures that are listed in *3GPP TS 23.401 v8.4.1 Annex D3.3, 3.5 and 3.6*.

Interworking with pre-Release 8 WCDMA core feature uses the term Old SGSN/Gn/Gp SGSN, New SGSN, and Old MME. Old SGSN/Gn/Gp SGSN refers to pre-Release 8 3G SGSN. New SGSN in routing area update procedure (*D3.5 in Annex D*) refers to pre-Release 8 3G SGSN and Old/New MME refers to the LTE MME.

3GPP pre-Release 8 SGSNs are only connected to GGSN/P-GW through the Gn/Gp interface, never connected to the S-GW. There is no S-type interface such as S4, and S12 in the pre-Release 8 3GPP architecture.

In the long term architecture, the Gn interface is replaced with the S3 interface. The SGSN is

connected through S4 to the S-GW and through S3 to the MME. For the interim period, pre-Release 8 SGSNs have to be connected to the evolved packet core (EPC) and this is done by:

- adding the GGSN functionality with Gn/Gp interface to the P-GW
- adding a Gn interface to the MME

The protocol stack of the Gn interface is shown in the figure. See *3GPP TS 29.060* for GTPcv1 specifications.

Figure 30: Gn interface protocol stack (MME – SGSN)



The Gn interface between the SGSN and P-GW is a control plane and user plane interface and the protocol is GTPv1-C and GTPv1-U. This interface enables the SGSN to control bearer management in the P-GW.

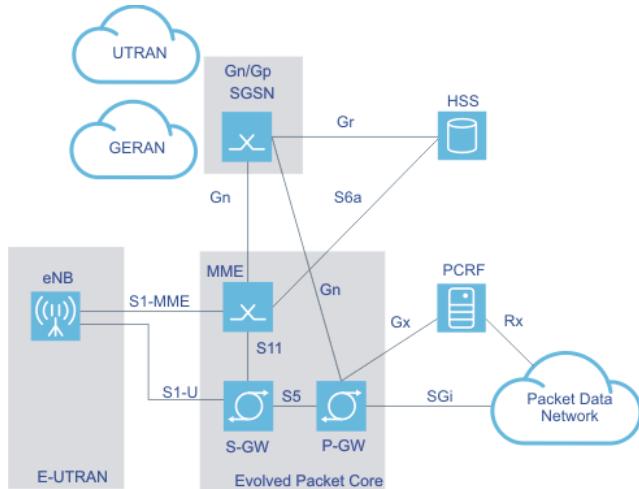
Figure 31: Gn interface protocol stack (SGSN – P-GW)



Reference architecture

When the SGSN follows the pre-Release 8 3GPP standards, the interface is the Gn interface. The Gn interface has both signaling and bearer. The signaling is directed to the MME and the bearer is directed to the P-GW. Thus, the P-GW provides the functions of the GGSN for the SGSN. In addition, the HSS supports both Gr and S6a interfaces. The MME supports Gr interface towards the HSS/HLR in a future release. The figure shows the reference architecture for pre-Release 8 SGSN.

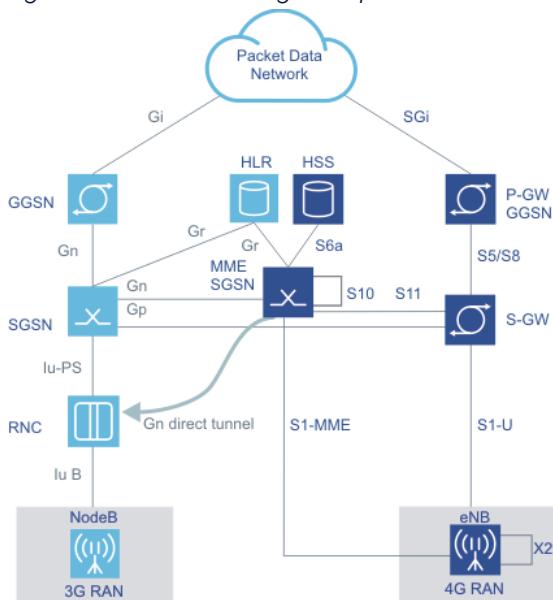
Figure 32: 3GPP Access for pre-Release 8 SGSN



Interworking with pre-Release 8 WCDMA core

If the customer has not upgraded the WCDMA core to support the Rel 8 interfaces, the EPC must interface with the WCDMA core element using the existing interfaces and must take on additional functionality. The MME interfaces with the 3G SGSN across the Gn interface to carry signaling data that uses GTPv1 protocol. The 3G SGSN interacts with the P-GW across the Gn interface that carries user data. Additionally, the MME interacts with the HLR/HSS across the Gr interface that is based on MAP protocol (this functionality is supported in a future MME release). The reference diagram shows 3G and 4G networks and depicts interworking with pre-Release 8 WCDMA core.

Figure 33: Interworking with pre-Release 8 WDCMA core



Direct tunnel functionality

Direct tunnel, also known as SGSN bypass, was introduced in 3GPP Release 7 architecture. Direct tunnel is an optional function in lu mode that allows the SGSN to establish a direct user plane tunnel between the RAN and GGSN (for connectivity with GGSN through Gn/Gp) or the S-GW (for connectivity through S4) within the packet switching (PS) domain. In 3GPP pre-Release 8 architecture, if a direct tunnel is used, then user traffic goes directly from the RNC to GGSN/P-GW and in Release 8 architecture the user traffic goes directly from the RNC to S-GW across the S12 interface.

A direct tunnel capable SGSN has the capability to be configured on a per RNC and per GGSN or S-GW basis whether or not it can use a direct user plane connection. The SGSN handles the control plane signaling and makes the decision when to establish a direct tunnel.

Requirements

This feature requires a 4G/3G/2G capable UE and the MME support of Gn/S3.

 **Note:**

For more information on the PS handover scenarios that are supported and not supported in CMM, see *SGSN Feature Overview*, section *S3-based packet switch handover (Feature SG01242)*.

3.15.2 RIM procedure between E-UTRAN and UTRAN (Feature m30030-01)

The RAN information management (RIM) procedure between E-UTRAN and UTRAN feature allows for faster radio setup by exchanging RAN parameters through the core ahead of the inter-RAT handover.

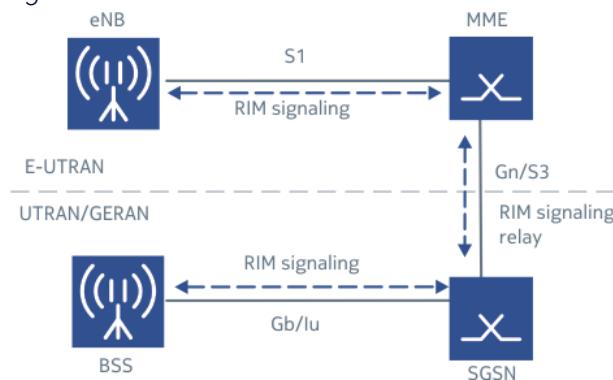
The *Network assisted cell change (NACC)* feature was originally introduced in Release 4 as a tool to minimize the service outage time for all quality of service (QoS) classes when a GPRS mobile subscriber (MS) in packet transfer mode moves between GSM cells belonging to the same BSC.

The NACC enables better performance for packet data services upon inter-cell change for those networks that do not support the packet switching (PS) handover. It reduces the service interruption time for UEs in active mode upon cell change by providing in the source

cell, before the cell change, system information of a target cell allowing the packet access. The NACC for this function is applicable for inter-RAT cell changes from a source E-UTRAN cell towards a target GERAN cell. Support for the RAN information management (RIM) procedure (used by the NACC) for inter-RAT cell change from a source E-UTRAN cell to a target UTRAN cell was introduced by 3GPP in Release 9.

The NACC from the E-UTRAN to GERAN follows the principles of the network assisted cell change between the UTRAN and GERAN as described in 3GPP TS 25.413 and 3GPP TS 23.060. It specifies the RIM procedures as shown in the figure.

Figure 34: RIM



The support for the NACC from the E-UTRAN to GERAN and the support of the RIM procedure between the E-UTRAN and UTRAN has the following impacts on the E-UTRAN/GERAN/UTRAN architecture:

- Affected nodes: BSC, eNB, RNC, MME, SGSN
- Affected network interfaces: Gb, Iu, Gn, S3, S1
- Affected radio interfaces: Um and Uu

Note:

This feature is applicable to Gn, S3, and S1 interfaces.

RIM procedures

The RIM procedures provide a generic mechanism for the exchange of arbitrary information between applications belonging to the RAN nodes. The RAN information is transferred through the MME and SGSN core network nodes. To make the RAN information transparent for the core network, the RAN information is included in a RIM container that is not interpreted by the core network nodes.

The RAN information is transferred in RIM containers from the source RAN node to the

destination RAN node by use of messages. Each message carrying the RIM container is routed and relayed independently by the core network nodes. Any relation between messages is transparent for the MME/SGSN, that is, a request/response exchange between RIM applications, for example, is routed and relayed as two independent messages by the MME/SGSN.

The interfaces that are used are the Gb, Iu, S1, Gn, and S3 interfaces. The RAN information in the RIM container is transparent for the core network. The MME or SGSN supporting the RIM procedures provides addressing, routing, and relaying functions.

Addressing

All the messages used for the exchange of RAN information contain the addresses of the source and destination RAN nodes. The eNB is addressed by the Target eNodeB Identifier.

Routing

The following description applies to all the messages used for the exchange of RAN information. The source RAN node sends a message to its MME or SGSN including the source and destination addresses. The MME/SGSN uses the destination address to route the message encapsulated in a GTP message to the correct MME/SGSN through Gn or S3 interface. The MME/SGSN connected to the destination RAN node decides which RAN node to send the message to based on the destination address.

Relying

The MME does relaying between S1 and Gn and/or S3 messages as described in 3GPP TS 36.413 and 3GPP TS 29.274/TS 29.060.

Requirements

This feature requires support of the inter-RAT handover.

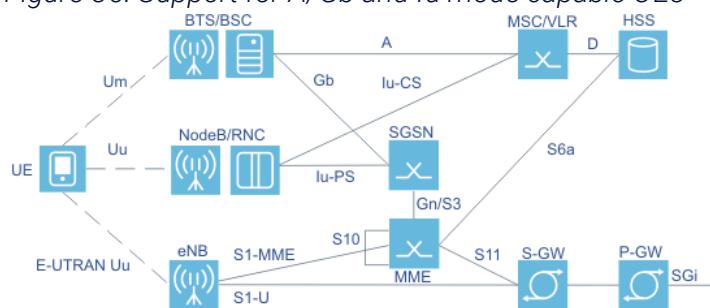
3.15.3 A/Gb and Iu mode capable UEs (Feature m30100-06)

The MME provides A/Gb or Iu mode capable UEs or both with necessary A/Gb and Iu mode related parameters that the UEs store and use later when the UE moves to the

UTRAN/GERAN.

The MME can also receive these parameters over the Gn/S3/S10 interface when the UE moves from the UTRAN/GERAN to the E-UTRAN or moves between MMEs. During the routing area update (RAU), tracking area update (TAU), S1 handover, and inter radio access technology (IRAT) handover procedures over the S10/Gn/S3 interface, the MME exchanges these parameters with the peer MME or SGSN. The MME stores these parameters in the VLR. The figure shows the A and Gb interfaces between the BTS/BSC and MSC/VLR, and the Iu interfaces between the NodeB/RNC and MSC/SGSN.

Figure 35: Support for A/Gb and Iu mode capable UEs



This feature enables inter-RAT mobility and session continuity when UE moves between the LTE and 2G/3G networks.

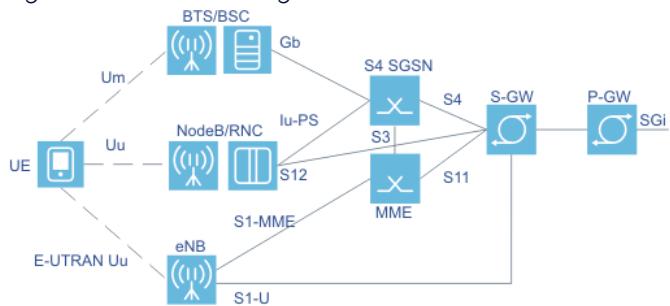
This feature requires 4G/3G/2G capable UE and MME support of Gn/S3.

3.15.4 Interworking between E-UTRAN and UTRAN/GERAN over S3 interface (Feature m30200-01)

The *Interworking between E-UTRAN and UTRAN/GERAN over S3 interface* feature enables inter radio access technology (inter-RAT) mobility and session continuity when UE moves between LTE and 2G/3G S4-SGSN.

This feature supports the interworking between the E-UTRAN and UTRAN/GERAN, where the MME interworks with an S4-SGSN over the S3 interface. An S4-SGSN is a Release 8 SGSN that supports the S4 interface to the S-GW and the S3 interface to the MME. A S4-SGSN is capable of handling evolved packet system (EPS) Bearer Contexts. Therefore, when the MME interworks with an S4 SGSN, the MME does not need to do the mapping between the EPS Bearer Contexts and packet data protocol (PDP) Contexts. The interworking architecture is shown in the figure. Note that even though this figure shows only one S-GW, the S-GW serving a specific UE can change when the UE moves from the E-UTRAN to UTRA/GERAN or vice versa.

Figure 36: Interworking between E-UTRAN and UTRAN/GERAN over S3



When a UE moves between the E-UTRAN and UTRAN/GERAN, if the S-GW does not change, then the MME and the SGSN interact with the same S-GW for a specific UE over the respective S11 and S4 interfaces. From the S-GW point of view, there is only one S-GW TEID-C per UE on the S11 and the S4 interfaces. The same S-GW tunnel is shared for the incoming control messages related to the operations on the same UE. At any specified time, for the same UE, the S-GW stores only one TEID-C from either the MME or the SGSN. The S-GW uses this TEID-C to send S11 or S4 messages to the respective MME or SGSN.

This feature includes the support of the S3 interface to the S4-SGSN and the following interworking procedures between the E-UTRAN and UTRAN/GERAN. Note that ISR and user location update reporting are not supported in this feature.

- Attach procedure
- Tracking area update (TAU) with or without S-GW change, when UE moves from UTRAN/GERAN to E-UTRAN
- Routing area update (RAU) with or without S-GW change, when UE moves from E-UTRAN to UTRAN/GERAN
- Inter-RAT handover
 - E-UTRAN to UTRAN handover
 - UTRAN to E-UTRAN handover
 - E-UTRAN to GERAN handover
 - GERAN to E-UTRAN handover
 - Inter-RAT handover cancel

During inter RAT handover when the UE disconnects from the source RAT but not yet connects to the target RAT, the downlink data packets received in the source RAT for the UE must be forwarded to the target RAT. Depending on the configuration in a service provider's network, the data forwarding can either be direct forwarding or indirect forwarding. When direct forwarding is supported, the downlink data is forwarded directly to the target without looping the downlink packets back to an uplink. In other words, the data forwarding path for direct forwarding is:

- Inter-RAT between E-UTRAN and UTRAN: source eNB → target RNC, or source RNC → target eNB
- Inter-RAT between E-UTRAN and GERAN: source eNB → target SGSN → target BSS, or source BSS → source SGSN → target eNB

The UTRAN network has the capability to support a direct tunnel between the RNC and S-GW. This is the S12 interface shown in the figure. When the S12 interface is supported, data packets are delivered directly between the RNC and S-GW without going through the intermediate SGSN. Direct tunnel is not supported in the GERAN network. The data forwarding path for indirect forwarding in the UTRAN makes use of the direct tunnel when it is supported by the network.

This feature requires S3 interface.

3.15.5 E-UTRAN to GERAN/UTRAN cell reselection and redirection (Feature m10906-01)

The *E-UTRAN to GERAN/UTRAN cell reselection and redirection* feature enables inter radio access technology (inter-RAT) mobility and session continuity when a UE moves between the LTE and 2G/3G SGSN.

This feature provides standards support for the E-UTRAN to GERAN/UTRAN cell reselection and redirection using S1 UE Context Release Command for both the connected and idle mode UE. The MME must handle cause inter-RAT redirection in the S1 Release message sent from an eNB whenever a UE does a cell re-selection.

This feature requires S3/Gn interface.

3.15.6 LAC values greater than 32 767 (Feature m30105-01)

The *LAC values greater than 32 767* feature enables operators to overcome an interworking issue when the UE moves from the 2G/3G network to the LTE network and the 2G/3G network sets the location area code (LAC) most significant bit (MSB) to 1.

This feature resolves an issue that arose because of a change in use of the MSBit in LAC and MME Group ID.

In the development of the Rel 8 standard a solution was worked out to address different temporary IDs in the GERAN/UTRAN and E-UTRAN and how to handle mobility between the

radio access technologies (RATs) without modifying Gn SGSNs. One result of this work was the specification to use the MSBit in LAC and MME Group ID to indicate whether the temporary ID was mapped or not, that is, MSBit = 1 indicates an MME Group ID (temporary ID allocated by MME) and MSBit = 0 indicates LAC (temporary ID allocated by SGSN).

In the pre-Rel 8 standard there is no restriction on using the MSBit or any value range of the 16-bit LAC value.

Some major operators have already configured LACs using the full value range of the LAC value (that is, there already are LAC values with MSBit = 1 in deployed networks), and it is not practicable for those operators to reconfigure their networks.

In Release 8:

- MSB of <LAC> is set to 0 (a change from pre-Release 8 where a MSB of 1 is possible)
- MSB of <MME group Id> set to 1

The UE maps <LAC> to <MME group Id> when mapping packet temporary mobile subscriber identity (P-TMSI)+routing area identity (RAI) to globally unique temporary identity (GUTI) during the UE move from the SGSN coverage to the MME coverage.

The MME uses the MSB of <MME group Id> in received OLD GUTI to determine old node type that is, the SGSN or MME:

- MSB of 1: Node Type = MME
- MSB of 0: Node Type = SGSN
- MME then chooses the name authority pointer (NAPTR) query format for the MME or SGSN based on the MSB value.

This Release 8 change creates the following problem:

- When the UE moves from the SGSN coverage, the MSB can be set to 1 when LAC values supported in the network are greater than 32 768.
 - With LAC MSB = 1, the MME cannot decide on the old node type because it cannot tell if the received OLD GUTI in TAU/Attach Request is a native GUTI or a GUTI mapped from P-TMSI + RAI.
 - The MME cannot decide on NAPTR query format for the MME or SGSN.

An option for workaround of this problem is to use GPRS Ciphering Key Sequence Number information element (IE) in the TAU Request message as an indicator that the UE has come from the SGSN coverage. 3GPP TS 24.301 8.2.29.3: *"The UE shall include this IE if the UE performs an A/Gb mode or Iu mode to S1 mode inter-system change in EMM-IDLE mode and the TIN indicates "PTMSI".*

Note:

If P-TMSI Signature or Additional GUTI or both are present then the GPRS Ciphering Key Sequence Number must be present. Otherwise TAU message must be treated as an invalid formatted message.

Based on the receipt of the GPRS Ciphering Key Sequence Number IE in TAU Request message, the MME formulates a NAPTR query for SGSN for to retrieve SGSN IP address.

If the TAU Request does not include the GPRS Ciphering Key Sequence Number IE, the MME formulates a NAPTR query for the MME to retrieve the MME address.

It is possible for the Attach Request be sent without the GPRS Ciphering Key Sequence Number IE. If it does not, then:

- The MME cannot determine if GUTI received is native GUTI or GUTI mapped from PTMSI + RAI.
- The MME tries NAPTR query for the MME first to get the MME IP address. If a record is returned, the received GUTI is native GUTI and no further action is required. The MME proceeds with the Attach Request.
- If no record is returned in the response, the received GUTI is GUTI mapped from PTMSI + RAI. The MME tries NAPTR query for the SGSN to get the SGSN IP address. If a record is returned, the MME proceeds with Attach Request. If no record is returned, the MME proceeds per current behavior.

This feature requires that the UE includes GPRS Ciphering Key Sequence Number IE in TAU request message when moving from the 2G/3G. The MME does double domain name system (DNS) query if this IE is not included in the Attach Request message when the UE moves from the 2G/3G to LTE.

3.15.7 Inter-RAT handover procedure from E-UTRAN to GERAN (Feature m30104-01)

The **Inter-RAT handover procedure from E-UTRAN to GERAN feature enables inter radio access technology (inter-RAT) interworking between the LTE and 2G.**

This feature supports inter-RAT handover procedure from the E-UTRAN to GERAN A/Gb preparation and execution phase as defined in 3GPP TS 23.401 Annex D3.7 and inter-RAT handover procedure preparation and execution phase from the GERAN A/Gb mode to EUTRAN as defined in 3GPP TS 23.401 Annex D3.8.

This feature requires support of G3/Gn interface.

3.15.8 Gn/S3 enhancements (Feature m30111-01)

The *Gn/S3 enhancements* feature avoids exhaustion of Gn/S3 managed object instances by deleting S3/Gn interface managed objects or instances when they become inactive for a period of time.

This feature introduces the following enhancements to the Gn/S3interface:

- A major alarm is raised when the last available managed object slot has been consumed.
- Enhanced aging algorithm that eliminates SGSNs that have not been contacted for any UE procedure for a long time.

The current procedure to send GTP Echo Requests and keep the Gn link up as long as replies are received and only delete the object when the remote far end point stops responding for an hour (or more) is not effective and as a result this feature provides a scheme that never exhausts the Gn interfaces and removes stale GSNs (the ones that have the longest interval of not handling a UE procedure).

This feature requires the inactivity-based setting.

3.15.9 IRAT mobility QoS parameter updates (Feature m30106-02)

The *IRAT mobility QoS parameter updates* feature enhances user experience by updating the bearer quality of service (QoS) to match the UE LTE subscription upon the UE move from the 2G/3G to LTE.

This feature provides a configurable option of the MME update of bearer QoS parameters to the P-GW (by sending S11 Modify Bearer Command) when the UE moves from the 2G/3G radio access technology (RAT) to LTE and old node is the S4-SGSN or Gn-SGSN. If the option is enabled, the S11 Modify Bearer Command is only sent if bearer QoS parameters received from the S4-SGSN or Gn-SGSN and the QoS parameters in the subscription data received from the HSS do not match.

In addition, this feature also supports a collision scenario handling whereby the MME can receive multiple Update Bearer Requests from the network at the same time.

3.15.10 Indirect data forwarding during pre-Rel 8 PS handover (Feature m30103-02)

With the *Indirect data forwarding during pre-Rel 8 PS handover* feature, the MME provides a method for creating GTPv2 based indirect data forwarding tunnel request towards the S-GW across S11 interface for the MME to the 3G SGSN combined hard handover and the serving radio network subsystem (SRNS) relocation procedure as described in 3GPP TS 23.401 Annex D.3.3.

This procedure covers both direct and indirect forwarding. The MME has configuration data that specifies for inter radio access technology (inter-RAT) handovers whether indirect forwarding does not apply or always applies. Indirect data forwarding can be with and without the S-GW relocation, however, for the 3GPP TS 23.401 Annex D3.3 procedure the S-GW relocation does not apply, this procedure purely deals with indirect data forwarding without the S-GW relocation.

3.15.11 Enhanced eHRPD to LTE idle mode handover (Feature m20100-03)

The *Enhanced eHRPD to LTE idle mode handover* feature supports the MME selection of the same P-GW when a UE has already activated bearers on a P-GW in a non-3GPP network enhanced High Rate Packet Data (eHRPD) in the case of subscriber data indicating dynamic allocation of the P-GW.

The UE indicates to the MME that it already has bearers on the P-GW by setting the Request Type information element (IE) to handover in the packet data network (PDN) Connectivity Request message. If the Request Type is set to handover, the MME does not use straightforward name authority pointer (S-NAPTR) procedures to discover the P-GW but uses the fully qualified domain name (FQDN) provided by the HSS. This selection applies to both UE Attach Request and Standalone PDN Connectivity Request. The MME also indicates to the S-GW/P-GW that the UE is handed over a non-3GPP network to a 3GPP network by setting the Handover Indication bit in Indication IE of S11 Create Session Request and Modify Bearer Request messages.

3.15.12 Cell redirection from LTE to 1xRT (Feature m20103-06)

The *Cell redirection from LTE to 1xRT* feature allows a connected mode and idle mode UE

to move from the LTE to the 1xRTT radio access network (RAN).

The UE provides LTE and optional 1xRTT radio measurements to the eNB based on the LTE and 1xRTT neighbor information configured by the eNB through dedicated radio resource controller (RRC) messages and redirects the UE to the desirable 1xRTT band class and frequency.

In the 1xRTT packet-switched (PS) redirection scenario, a LTE data suspension is required when the connected UE is transferred to the 1xRTT system for 1XRTT PD service. The MME must support the cause value Redirection towards 1xRTT.

- The MME, upon receiving UE Context Release request with a cause value Redirection towards 1xRTT from eNB, requests the S-GW for non-GBR evolved packet system (EPS) bearers release by sending S11 Release Access Bearer Request message.
- After deactivating/releasing of EPS bearers, the MME sends S11 Suspend Notification message to the S-GW.
- The S-GW, upon receiving this message, should discard packets it receives for the suspended UE.
- The S-GW sends a suspend notification to the P-GW and the P-GW should discard packets it receives for the suspended UE and send the S-GW a Suspend Acknowledge message with a cause value.
- The S-GW sends a Suspend Acknowledge message with a cause value to the MME, and upon receiving the Suspend Acknowledge from the S-GW, the MME sends a UE Context Release Command with cause value Redirection towards 1xRTT to the eNB.

3.15.13 Cell S3 Forward Relocation Response from different IP (Feature m30112-01)

The *Cell S3 Forward Relocation Response from different IP* feature addresses deployments where the target peer node can support multiple control plane IP addresses and requires subsequent communications for this procedure to use the IP address provided in the Forward Relocation Response.

This feature supports reception of S3 Forward Relocation Response from an IP address that is different from the destination IP address of the S3 Forward Relocation Request. The MME, in this case, accepts the S3 Forward Relocation Response and proceeds with inter radio access technology (IRAT) handover. This feature, in addition to S3 Forward Relocation Request, also allows any response message type to come back from a different IP address.

3.15.14 WiFi handoff with mode 2 (Feature m10130-01)

The **WiFi handoff with mode 2** feature supports preserving the same P-GW in both the LTE and WiFi networks so that a packet data network (PDN) connection is preserved when the UE moves between LTE and WiFi.

The MME updates the HSS with the fully qualified domain name (FQDN) of the selected P-GW for a PDN connection if the UE subscription data allows handover to a non-3GPP access.

When the UE moves to the WiFi access, the P-GW FDQN stored in the HSS is used by the WiFi network to keep the same P-GW.

When the UE moves from the WiFi to LTE, the UE indicates to the MME that it is moving from non-3GPP access by setting the Request Type information element (IE) of the Standalone PDN Connectivity Request or PDN Connectivity Request sent in Attach Request to handover. This triggers the MME to use the P-GW FDQN stored in the UE access point name (APN) subscription data so that the same P-GW is maintained to preserve the PDN connection.

3.15.15 MME support for forming APN FQDN on non-3GPP handover scenarios (Feature f10560-01)

With this feature, the MME selects which PLMN ID to indicate for the APN operator identifier (APN-OI) on the S11 Create Session Request message.

The feature is applied when the MME receives a PDN connectivity request message with request type "Handover" and finds the P-GW information from the HSS (MIP6-Agent-Info AVP) based on the requested APN.

This functionality is controlled through the global parameter `pdnHoS11ApnFormulation`.

3.15.16 Unconditionally set up radio bearers for inter-RAT TAU (Feature f10128-01)

The **Unconditionally set up radio bearers for inter-RAT TAU** feature provides the global parameter `treatIratTauActiveTau`.

When the `treatIratTauActiveTau` global parameter is enabled, the MME sets up radio bearers during ECM-IDLE inter-RAT TAU request regardless of the active flag setting received in the TAU Request message. By default, `treatIratTauActiveTau` is disabled.

3.15.17 Emergency calls WLAN handover (Feature f10509-01)

This feature supports emergency calls handover of authenticated UE between the E-UTRAN/EPC and the WLAN by utilizing the HSS to store the selected P-GW identity and to forward the selected P-GW identity to the other access.

This capability is not supported for SIMless UEs or unauthenticated UEs. The MME provides provisioning capability to enable the feature.

3.15.18 CMM support for ARD provisioned in HSS and pass it with service-based HO to radio accordingly (Feature f11343-01)

This feature supports HSS access restriction data (ARD) provisioning and passing with service-based handover to radio accordingly in the CMM.

This feature supports:

- SGSN receiving and storing 'WB-E-UTRAN Not Allowed' Access-Restriction-Data from the HSS.
- SGSN informing radio network controller (RNC) with E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request messages.
- MME updating the 'WB-E-UTRAN Not Allowed' in SGSN's subscriber data in DBS.
- CMM avoiding unnecessary ping pong between 3G and 4G changes when 'WB-E-UTRAN Not Allowed' is set in HSS ARD (3G attach) or when no ARD is set in HLR but DIAMETER_ERROR_USER_UNKNOWN and DIAMETER_ERROR_RAT_NOT_ALLOWED is received by HSS (4G attach, TAU).

Enabling new functionality

With this feature, the SGSN supports ARD from S6d and pass it to the RAN and the MME in combined node during attach or TAU can store 'WB-E-UTRAN Not Allowed' in the DB if DIAMETER_ERROR_USER_UNKNOWN is received during location update. If the subscriber is still in the database and, for example, the subscriber was attached in the SGSN before, the purge is not done, the MME sends #15 No suitable cells in TA.

This global parameter is disabled by default.

S6d changes

With this feature, the S4-SGSN decodes and stores 'WB-E-UTRAN Not Allowed' when received from S6d interface.

RANAP changes

With this feature, the S4-SGSN encodes the E-UTRAN service handover IE and includes it in the following RANAP messages for 3G subscribers:

- RAB Assignment Request
- Relocation Request

If the S4-SGSN does not receive the Access-Restriction-Data parameter from the HSS during location update, SGSN assumes that such restrictions do not exist, therefore handover to E-UTRAN is allowed.

In case the ARD value is 'E-UTRAN not allowed' and this feature is enabled, the S4-SGSN will include the E-UTRAN service handover IE with value 'Handover to E-UTRAN shall not be performed' in the listed RANAP messages. When the ARD value is not 'E-UTRAN not allowed', E-UTRAN service handover IE will not be included in the RANAP signaling.

The ARD value 'E-UTRAN not allowed' will only be used in order to decide whether to send the E-UTRAN service handover IE with value 'Handover to E-UTRAN shall not be performed' in RANAP messages signaling. The S4-SGSN will not refuse outgoing mobility to MME if E-UTRAN not allowed is set.

In case the ARD value is modified, the new information will be used in order to decide whether the IEs are sent in the next applicable RANAP message.

The SGSN will not distinguish among home subscribers and roamers. If the HSS of a roamer sends ARD with E-UTRAN not allowed, the E-UTRAN service handover IE is sent to RNC same way as homers.

MME mobility management changes, IRAT changes

With this feature, the MME differentiates its default functionality for the following cases:

1. Home subscribers who are using S6d and subscribers who have ARD provisioned in HSS.
2. Home subscribers who are using Gr (certain IMSI ranges) and subscribers who have no ARD provisioned in HLR
3. Inbound roamers who are using Gr and subscribers who have no ARD provisioned in HLR.

The MME in the combined node supports:

- If DIAMETER_ERROR_RAT_NOT_ALLOWED (5421) (case 1) is received from the HSS during location updating (ULA), the MME sets the ARD field to 'WB-E-UTRAN Not Allowed' in DB and sends #15 No suitable cells in TA.
- If DIAMETER_ERROR_USER_UNKNOWN (case 2 and 3) is received from the HSS during location updating (ULA), the MME checks subscriber database to see whether the subscriber exists (the subscriber attached in the SGSN earlier and the purge is not done). If the subscriber exists, the MME sets ARD field to 'WB-E-UTRAN Not Allowed' in DB and sends #15 No suitable cells in TA (normally, #8 Reactivation requested is used). If the subscriber does not exist, the change will not be implemented.
- If a VPLMN has no roaming agreements with the UE network in 4G, but in 2G/3G, the MME does not query the HSS. The MME sets the ARD in the same way as if the HSS returns with DIAMETER_ERROR_USER_UNKNOWN.

For the SGSN, if the subscriber moves back, for example, during the RAU or HO procedure, the SGSN applies the service-based HO IE based on the ARD properly set in the database if the feature is enabled.

The SGSN does not support Gr ARD with the same value.

3.15.19 MME support for inter-system RAU enhancements (Feature f11821-01)

In this feature, the global parameter `sendDeleteSessionReqForIntersystemRau` is used to control whether the MME can send Delete Session Request to the S-GW upon receiving Cancel Location Request from the HSS with cancellation Type = MME update procedure during Gn-based inter-system RAU and S3-based inter-system RAU with S-GW relocation.

When the feature is enabled by setting the parameter

`sendDeleteSessionReqForIntersystemRau` to Yes, the MME sends Delete Session Request to the S-GW upon receiving Cancel Location Request from the HSS with cancellation Type = MME update procedure during Gn-based inter-system RAU and S3-based inter-system RAU with S-GW relocation. When the feature is disabled by setting the parameter `sendDeleteSessionReqForIntersystemRau` to No, the MME does not send Delete Session Request to the S-GW upon receiving Cancel Location Request from the HSS with cancellation Type=MME update procedure during Gn-based inter-system RAU and S3-based inter-system RAU with S-GW relocation.

3.16 CSFB

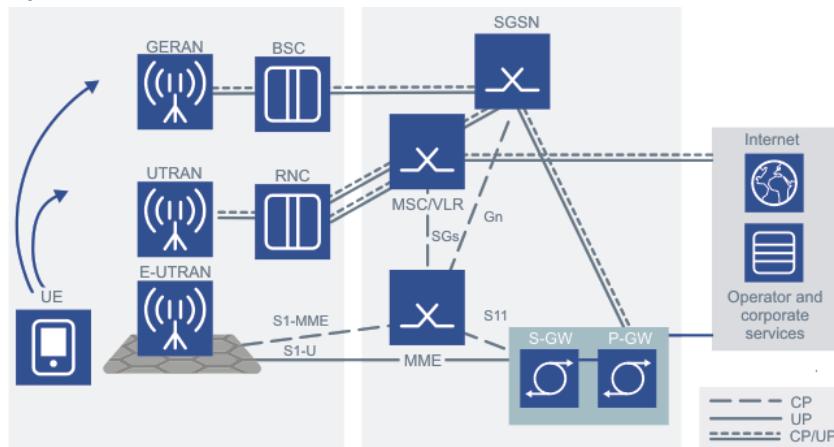
Features enabling support for circuit switched fallback (CSFB) to GERAN/UTRAN.

3.16.1 SGs based CS fallback and SMS interworking with GSM/UMTS (Feature m30101-03)

The SGs based CS fallback and SMS interworking with GSM/UMTS feature enables operators to offer circuit switching (CS) domain services such as CS voice and SMS.

The Circuit SwitchedFallback (CSFB) in evolved packet system (EPS) enables the provisioning of voice and other CS-domain services (for example, SMS) by reusing the CS infrastructure when the UE is served by the E-UTRAN. A CSFB enabled terminal connected to the E-UTRAN can use GERAN or UTRAN to establish one or more CS domain services. This function is only available when the E-UTRAN coverage is overlapped by either GERAN coverage or UTRAN coverage. The CSFB in EPS function is realized by using the SGs interface mechanism between the MSC Server/VLR and the MME. The reference architecture for CSFB in EPS for GERAN/UTRAN is shown in the figure. Note that in 3GPP TS 23.272, the interface between the SGSN and MME is S3. In the figure, Gn interface is used between the SGSN and MME (interface to a pre-Release 8 SGSN).

Figure 37: CSFB architecture



The SGs interface is used for the mobility management and paging procedures between EPS and the CS domain. This interface is also used for the delivery of both mobile originating and mobile terminating SMS.

The SGs interface uses SCTP as the transport layer. The MME is responsible for establishing

SCTP associations with the MSC Servers/VLRs.

The CSFB capable UE supports access to EPS as well as access to the CS domain over the GERAN/UTRAN. It supports the following additional functions:

- combined EPS/international mobile subscriber identity (IMSI) attach, tracking area update (TAU), and detach procedures
- CSFB and SMS procedures by reusing the CS domain services

The MME identifies a UE as CSFB-capable when the UE sets the EPS attach type information element (IE) to combined EPS/IMSI attach in the non-access stratum (NAS) Attach Request message, or sets the EPS update type IE to combined TA/LA updating or combined tracking area (TA)/location area (LA) updating with IMSI attach in the NAS Tracking Area Update Request message.

The CSFB-enabled MME:

- supports the combined EPS/IMSI attach and TAU
- derives an MSC Server/VLR number from a location area identification (LAI) that is mapped from the tracking area identity (TAI) in which the UE is located. The TAI to LAI mapping is provisioned on the MME. When multiple MSC Servers/VLRs serve the same LAI, the MME uses a round-robin scheme to determine the MSC Server/VLR.
- maintains SGs association toward MSC Server/VLR for EPS/IMSI attached UE
- initiates IMSI detach at EPS detach
- initiates paging procedure towards eNB when MSC Server/VLR pages the UE for CS services
- supports CS fallback procedures with or without concurrent PS handover to the GERAN/UTRAN
- supports SMS procedures
- rejects CSFB call request (for example, because of Operations, Administrations and Maintenance (OAM) reasons)

After the UE is EPS/IMSI combined attached to the EPS and the CS network, the UE can initiate a CSFB call with or without concurrent handover of packet switching (PS) bearers. It can also send SMS to the CS domain. Likewise, if there is a terminating CS call or SMS message for the UE, the CS domain pages the UE regardless if the UE is in the ECM-IDLE or ECM-CONNECTED mode. The EPS handles the CS paging message properly based on the ECM state.

There is a difference between the handling of CS fallback calls and SMS by the UE and EPS. For CS fallback calls, at the moment when a CS fallback call is requested (either originating or terminating), the UE falls back to the GERAN/UTRAN access network that supports the traditional voice services. The UE uses the standard CS voice call setup procedures to

establish the voice call in the CS domain. For SMS (either originating or terminating), the UE stays in the LTE access network and sends/receives the SMS over EPS.

The CS fallback and SMS features support the following scenarios:

- Mobile-originating CS fallback call in ECM-CONNECTED mode – PS handover supported
- Mobile-originating CS fallback call in ECM-CONNECTED mode – PS handover not supported
- Mobile-originating CS fallback call in ECM-IDLE mode
- Mobile-terminating CS fallback call in ECM-CONNECTED mode – PS handover supported
- Mobile-terminating CS fallback call in ECM-CONNECTED mode – PS handover not supported
- Mobile-terminating CS fallback call in ECM-IDLE mode
- Mobile-originating SMS in ECM-CONNECTED mode
- Mobile-originating SMS in ECM-IDLE mode
- Mobile-terminating SMS in ECM-CONNECTED mode
- Mobile-terminating SMS in ECM-IDLE mode

This feature requires support of SGs interface to the MSC along with overlay GERAN/UTRAN access network.

3.16.2 SMS-only over SGs interface (Feature m11004-02)

The *SMS-only over SGs interface* feature enables operators to deploy circuit-switched fallback (CSFB) solution for SMS only. This simplifies network deployment as there is no need to deploy an overlay GERAN/UTRAN access network to support circuit switching (CS) voice.

The CSFB solution over the SGs interface supports originating/terminating voice calls, in which the UE accesses voice services through the existing CS domain by falling back to the 2G/3G CS network. In addition, the CSFB solution supports SMS delivery through the 2G/3G CS network, in which the UE sends/receives SMS over the SGs interface while staying in the LTE network.

However, some operators have expressed interest in offering SMS service over the SGs interface but not the CSFB voice calls. This has the following advantages:

- The CSFB solution requires the operator to upgrade all MSCs to support the SGs interface in the areas where the legacy 2G/3G network overlaps with the LTE network. With the SMS-only over SGs interface, the operator can designate a few MSCs for SMS and upgrade only those MSCs.
- The CSFB solution requires fallback to the GERAN/UTRAN radio access technologies

(RATs) and hence requires the overlapped GERAN/UTRAN coverage. The SMS-only over SGs does not require the overlapped GERAN/UTRAN coverage.

- The CSFB solution requires operators to provision the MME with the identity of the MSC to be reached at a combined Attach/tracking area update (TAU) Request. With the SMS-only solution, the MME can use a simple algorithm or provision a single MSC for the SGs interface.
- SMS-only over SGs is less restrictive than CSFB in tracking area (TA) boundary planning and the use of TA list. Unlike CSFB, the SMS-only solution does not require the operator to carefully plan the geographic correlation between the TAs and the location areas (LAs)/MSCs in the legacy 2G/3G network (for example, the coverage of a TA must be wholly contained in the area covered by only one LA, that is, a TA cannot span across multiple LAs). Nor does the SMS-only solution require that the list of TAs delivered to a UE in the Attach/TAU Accept message only contain TAs within a single LA.

The feature also allows the operators to specify their preference for CS fallback support per public land mobile network (PLMN) basis. Before this feature the operator could specify per PLMN basis if the network provides CSFB for voice and SMS to UEs with the corresponding home network (HPLMN). With the implementation of this feature the operator can additionally specify SMS-only or CS fallback not preferred per PLMN basis. The operator can specify no CSFB support or CSFB for voice and SMS or CSFB for SMS or CSFB not preferred per PLMN basis. The operator may specify CS fallback not preferred if the MME supports CSFB for voice but prefers that the UE from a specific PLMN not to use it.

The CS fallback support provided to a UE is a function of what the UE requested, what the MME is capable of offering, what can be offered to the UE HPLMN and what the subscriber profile specifies. The UE is offered the most restrictive CS fallback support of them all.

Upon receipt of SMS-only or CS fallback not preferred, the UE takes that into account while selecting the RAT and IMS voice or CSFB voice. If neither SMS-only nor CS fallback not preferred is received by the UE, it ends up using CSFB for voice calls when needed in accordance with 3GPP TS 23.221 Annex A.

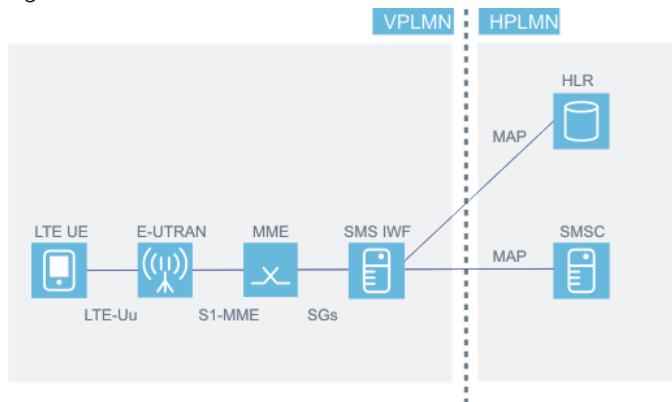
3.16.3 Additional SMS enhancements (Feature m30101-09)

The *Additional SMS enhancements* feature allows operators to deploy an **SMS interworking function (IWF) instead of a regular **MSC** to provide **SMS only service** for **inbound roammers**.**

This feature supports session management (SM)-only feature for inbound roammers for

operators that deploy a dedicated IWF instead of a 3GPP MSC/VLR. For all practical purposes the IWF appears to the MME as a 3GPP MSC/VLR. The figure shows architecture with IWF. The IWF in the figure acts as a limited MSC/VLR.

Figure 38: Architecture with IWF



This feature enhances the currently supported SMS only capability on the MME to include certain optional information elements (IEs) in SGsAP messages from the MME to the MSC/VLR.

- The MME supports MSC/VLR (IWF) selection based on hash value from the international mobile subscriber identity (IMSI) to determine the MSC/VLR number when multiple MSC/VLRs serve the same location area identification (LAI).

Note:

In case of SMS only, there is only one LAI that maps to all the MSC/VLRs.

- The MME supports up to four MSC/VLRs. Each MSC/VLR can have up to four single-homed or multi-homed SCTP associations.
- The MME complies with the following table in including the optional IE in SGsAP messages to the MSC/VLR

Table 34: Optional IE in SGsAP messages

Message	IE
SGsAP-UPDATE-LOCATION-REQUEST	IMEI
	TAI
	E-CGI
SGsAP-UPLINK-UNITDATA	IMEISV
	UE Time Zone
	TAI
	E-CGI
SGsAP-SERVICE-REQUEST	IMSISV
	UE Time Zone
	TAI
	E-CGI

- The SGs interface is IPv4/v6 capable

This feature requires that SMS only service is enabled.

3.16.4 CSFB enhancements (Feature m30102-03)

The CSFB enhancements feature allows LTE-only operators to provide circuit-switched (CS) voice and SMS services for roammers from a 2G/3G only network. Additional paging and release 9 enhancements are included.

This feature enhances circuit-switched fallback (CSFB)/SMS features already supported on the MME:

- SGs paging enhancement

If the MME registers a UE with a MSC/VLR over the SGs interface, the MSC/VLR can page the UE over the SGs interface. If the UE fails to respond to the paging, the MSC/VLR can retry for multiple times. The MME is provisioned with additional data to control the paging method and the paging guard timer for each paging attempt from the MSC/VLR.

- Release 9 compliance

The S3 Suspend Notification and Suspend Acknowledge messages are supported. In addition, the Release 9 behavior on handling the UE not available for PS service cause in the S1 UE Context Release Request message is supported.

- Support CSFB across different 4G and 2G/3G operators

This applies when an LTE-only operator has an overlay network with a 2G/3G operator, and there is a roaming agreement between the LTE-only operator and the 2G/3G operator. Subscribers of the 2G/3G operator get high-speed data services from the LTE-only operator and voice services from the home 2G/3G operator. To support CSFB from the LTE network to the 2G/3G network, the MMEs in the LTE-only operator's network have SGs interfaces to the MSC/VLRs in the 2G/3G operator's network. Coordination on the allocation of tracking areas (TAs) in the LTE-only network and the allocation of location areas (LAs) in the 2G/3G network is needed to reduce unnecessary voice call setup delay during the CSFB procedure.

There are other CSFB enhancements defined in the Release 9 standards, which affect the eNB and RNC but are transparent to the MME. This feature does not cover those enhancements.

This feature requires support of SGs interface between roaming partners' networks.

3.16.5 S102-based CS fallback to 3G1X voice (Feature m20103-01)

The *S102-based CS fallback to 3G1X voice* feature provides support for **S102 interface on the MME for circuit-switched fallback (CSFB) from LTE data to 3G1X circuit voice for 3G1X voice call origination and termination. It also supports SMS over S102 in evolved packet system (EPS).**

When CDMA operators migrate to the LTE and voice-capable terminals are available, operators still must support voice and SMS services until IP multimedia subsystem (IMS)-based voice over IP (VoIP) over LTE is available everywhere. Thus, 1xRTT circuit switching (CS) can still provide CS services and SMS. The CDMA CSFB to CDMA CS access (1xRTT) for voice and SMS services is then needed to transfer UE to 1xRTT for SMS or data calls.

If the UE is operating in a dual receiver configuration, it is able to do 1xRTT registration and other signaling without any network support between accesses. For voice calls, the UE is moved to 1xRTT access. In addition, the UE might have to leave the LTE network to be able to do 1xRTT-related signaling.

As the UE is not available when it leaves the E-UTRAN, the MME needs to apply special

handling to bearers on the EPC side: it suspends non-guaranteed bit rate (GBR) bearers and deactivates GBR bearers so that resources are not left hanging.

This feature provides S102 interface support on the MME for CSFB from LTE data to 3G1X circuit voice for 3G1X voice call origination and termination. In addition, this feature also supports SMS over S102 in EPS. The mobile-originating (MO) SMS and mobile-terminating (MT) SMS are tunneled in EPS and over S102 and do not cause any CSFB to CDMA 1xRTT, and consequently does not require any overlapped CDMA 1xRTT coverage.

The S102 reference point between the MME and 3GPP2 1xCS IWS to relay 3GPP2 1xCS signaling messages to support single radio voice call continuity (SRVCC) as specified in 3GPP TS 23.216 and CSFB to 1x CS network as specified in 3GPP TS 23.272. 1x CS signaling messages are those messages that are defined for the A21 interface as described in 3GPP2 A.S0008-C and 3GPP2 A.S0009-C. The S102 interface messages are based on A21 messages.

The S102 interface is used to support UEs that do not transmit and receive on both the LTE and 1x radio interfaces simultaneously. S102 protocol aspects for SRVCC from E-UTRAN access to 3GPP2 1xCS.

The S102 application is based on User Datagram Protocol (UDP)/IP transport medium, UDP 23272 is the registered S102 (MME-to-destination UDP port number to be used for signaling interconnection between the MME and an IWS for the S102 application).

The S102 interface allows CSFB to 1xRTT to establish voice call in the CS domain through support of registration over EPS procedures as specified in 3GPP TS 23.272.

With this feature data terminal ready (DTR) is preserved when an Extended Service Request is received when VLR CSFB indicator is not set.

The MME enabled for CSFB to 1xRTT supports the following additional functions:

- It serves as a signaling tunneling end point towards the 3GPP2 1xCS IWS through the S102 interface for sending/receiving encapsulated 3GPP2 1xCS signaling messages to and from the UE, which are encapsulated in S1-MME S1 Information Transfer messages, as defined in TR 36.938.
- 1xCS-IWS (terminating S102 reference point) selection for CSFB procedures
- handling of S102 tunnel redirection in case of MME relocation

If the network supports CSFB priority call handling, the MME supports the following additional functions:

- For page message received on the S102 interface with priority indication, the MME provides preferential treatment to this message and also the subsequent CSFB procedure compared to other normal transactions. If the UE needs to be paged, the MME

sets priority indication on the paging request to the eNB. The MME also sets priority indication, that is, CSFB High Priority, in S1AP message to the eNB, so that eNB can initiate the CSFB procedure with priority, as specified in 3GPP TS 36.413.

- For a CSFB request from a service user, the MME determines that the CSFB request needs priority handling based on the UE's EPS subscription information. The MME in congestion situation provides preferential treatment to this request and also sets priority indication, that is, CSFB High Priority, in S1AP message to the eNB to initiate CSFB procedure, as specified in 3GPP TS 36.413.

This feature requires IWS.

3.16.6 Provisioning control whether ESR for MO call is accepted (Feature f10111-02)

With this feature, the operator can decide whether to reject the Extended Service Request message for dual transceiver receiver (DTR) UEs.

By default, the flag is disabled. When the flag is enabled by using the global parameter `rejDtrExtendedServiceRequest`, the MME sends cause code #18 "CS Domain not available" in service reject to the UE.

3.16.7 3G1x voice on dual transceiver handset (Features m20103-04, m20103-05)

The 3G1x voice on dual transceiver handset feature provides support for 3G1x voice call origination and termination on dual transmitter and dual receiver LTE handsets without the use of S102 interface to 3G1x infoware system (IWS).

This feature is used by the UEs that have dual transmitter and dual receiver. These UEs use the LTE for data and the 3G1x circuit-switched (CS) domain for the voice and SMS. The UE is configured to acquire and register on 3G1x using the 3G1x transmitter before the LTE. The UE acquires and attaches to the LTE over the LTE transmitter after 3G1x registration.

This feature requires changes to the 3G1x Overhead Parameter message to inform the UE that the 3G1x has an LTE overlay. Upon receipt of the LTE capable information in the 3G1x Overhead Parameter message, a dual transmitter and dual receiver UE searches for an LTE system. If the LTE capable information is not received, the UE does not search for an LTE system in the interest of reducing power consumption.

At any specified time, the UE operates either in an LTE data or circuit voice mode but not both. When a 3G1x call is originated or terminated, the UE requests the MME to suspend the LTE data session. Upon the completion of the 3G1x call, the UE requests the MME to resume the LTE data session.

The dual transmitter and dual transceiver UEs are expected to do the 3G1x registration (for example, location based, based on SID/NID, or timer based) and LTE tracking area update (TAU) independently of the dual transmitter and receiver. Similarly, the dual transmitter and dual transceiver UEs are expected to do the 3G1x and LTE handover independently. The dual transmitter and dual transceiver UEs are expected to monitor 3G1x page while in the LTE mode but not to monitor the LTE page while in the 3G1x voice call.

For a dual transmitter and dual transceiver UEs no 3G1x radio measurements are done by the LTE system. In the absence of these, the UE decides which system is selected.

Where the circuit-switched fallback (CSFB) is supported, the network supports both the dual transmitter-dual transceiver UE and the CSFB UE. However, a single UE operates in only one mode.

This feature requires IWS.

3.16.8 Modify Bearer Request during CSFB (Feature f10111-01)

The *Modify Bearer Request during CSFB* feature provides a provisioning ability to send the S11 Modify Bearer Request during an idle UE initiated extended service request procedure with SGs interface.

If the feature is activated, the MME sends the S11 Modify Bearer Request (MBR) to the S-GW. If the feature is deactivated, the MME does not send the S11 MBR. By default, the feature is activated.

The current MME behavior of sending MBR in an idle UE initiated extended service request procedure is supported to handle the S-GW behavior of not being able to set up indirect tunnels without the MBR. However, 3GPP circuit-switched fallback (CSFB) specifications (3GPP TS 23.272) do not require sending of the MBR. Hence, this feature is created to make the MME's behavior consistent with 3GPP specifications, at the same time preserving the current behavior. The feature assumes that all S-GWs in a core network have the same behavior.

3.16.9 Suppress registered LAI in Context Setup Requests to eNB (Feature f10412-01)

This feature provides provisioning controlled support for suppression of the registered LAI IE in messages Initial Context Setup request and UE Context Modification request for certain CSFB deployments.

When this IE is included in these messages, it allows the eNB to take this registered LAI into account when selecting the target cell or frequency for CSFB. When this IE is present in the CMM implementation for CSFB, this limits the network to which the UE can fall back to either the 4G serving network or the UE's home network. When this IE is suppressed, the UE can fall back to a network different from either the 4G serving network or the UE's home network.

This feature is controlled by the global parameter `suppressRegisteredLai` (disabled by default).

3.16.10 Maintain UE SGs-Association state to MSC after SGs link failure (Feature f11812-01)

This feature provides an option to specify whether the CMM should accept and process an SGs page request from an MSC other than the currently registered MSC.

The global parameter `acceptSgsPageFromNonRegMsc` controls this feature. When the feature is disabled (the default), the MME CSFB declares a link failure to an MSC after the SCTP connection stays down for a period (for example, 10 seconds). As part of the failure handling, the MME sets `mscReliable` to false and also sets the SGs-Association state for each registered UE to SGs-NULL (essentially treating the condition as having received a SGs-Reset message from the MSC/VLR). If the MSC pool subsequently attempts to reach the UE with paging, the MME rejects the pages with SGs cause 'IMSI detached for non-EPS services' until the next UE activity forces the UE to reattach to the circuit core.

If the feature is enabled, the MME does not change the UE SGs-Association state after such a link failure. This means that the UE will be accessible in the window between start of SGs link failure and UE activity (for UEs registered to the failed MSC).

4. Session management

The EPS session management (ESM) procedures support bearer activation, modification, deactivation, and preservation of data sessions.

4.1 Idle-active change (Feature m10001-01)

The *Idle-active change* feature is a basic requirement for the MME. The UE uses the idle-active change to save the battery; the network uses it to save radio capacity.

With this feature, the UE or the network can initiate data path activation requests. The UE has previously entered the idle state as a result of an S1 release procedure initiated by the eNB. If the UE wants to send data, it sends a service request to return to the active state.

In the network-initiated service request, the MME uses paging to activate the UE.

4.2 Piggyback functionality for default bearer activation (Feature m11006-01)

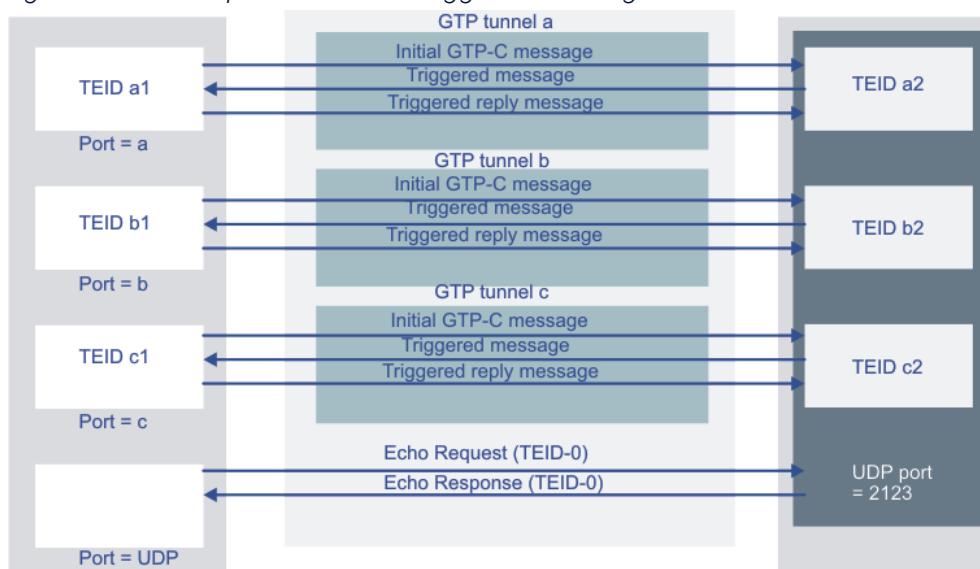
The *Piggyback functionality for default bearer activation* feature provides the benefit of combining both attach and UE-requested public data network (PDN) connectivity procedures for default and dedicated bearer activation into a single message.

The MME supports piggyback functionality whereby the messages for the default bearer activation at attach and UE requested PDN connectivity procedures and for the dedicated bearer activation procedure are combined into a single message.

Piggybacking is only applicable if all nodes in the chain (MME, S-GW, and P-GW) support piggybacking.

The figure shows the GTP-C path initial and triggered message concept.

Figure 39: GTP-C path initial and triggered messages



The expected reply to a request message is a triggered message and the reply has the same message name as the request but with Response replacing Request. If a request message is a reply to a command message, then the request message is a triggered message; otherwise the request message is an initial message. Responses do not have replies except when a Context Acknowledge is required as a reply to Context Response message as specified in relevant Stage 2 procedures. Context Acknowledge is always a triggered message and does not have a reply.

A message whose name ends in Command is always an initial message. If a command message fails, the name of the reply message is constructed by replacing Command with Failure Indication. Apart from Downlink Data Notification Failure Indication message, a failure indication is a triggered message. The Failure Indication message does not have a reply. A message whose name ends in Notification is always an initial message. The expected triggered message in reply has the same message name but with Acknowledge replacing Notification, except for Downlink Data Notification that has the reply Downlink Data Notification Acknowledge. An acknowledge message does not have a reply. CS Paging Indication, Stop Paging Indication, RAN Information Relay, Configuration Transfer Tunnel, Trace Session Activation, Trace Session Deactivation, and Downlink Data Notification Failure Indication messages are initial messages that do not have a reply. A Version Not Supported Indication message is a triggered message.

4.3 Scenario-based actions on move VLR (Feature m10714-03)

The **Scenario-based actions on move VLR** feature ensures UE session continuity. When the identity of a UE in a procedure-triggering message is unknown to the MME, a control plane processing services (CPPS) is selected and a temporary visitor location register (VLR) record is created.

In the MME relocating procedure, the MME requests information about the UE from the source MME and typically learns the UE's international mobile subscriber identity (IMSI) in that exchange. The MME uses the IMSI to determine whether a VLR record for the UE already exists with the UE with the EMM state of EMM-REGISTERED. If such a record exists, the MME must clean up the previously established sessions and then merge whatever information is appropriate from the old record into the new record. This cleanup and information merging process is called 'move VLR'.

In the current implementation of the move VLR action, cleanup of the previously established sessions is done without regard to the current triggering procedure. This can lead to inappropriate cleanup actions which cause the triggering procedure to fail. Specifically, the Delete Session Request is typically sent during the move VLR action when the triggering procedure is an S-GW relocating event.

The Delete Session Request message includes the Indications Flag IE and the Operation Indication and Scope Indication flag settings determine how the message is treated with regard to the P-GW:

- If the triggering procedure is attach, it is appropriate to delete old session data on both the old S-GW and P-GW.
- If the triggering procedure is an inter-MME tracking area update (TAU), it is appropriate to delete old session data on the old S-GW but not on the P-GW.
- Currently the Delete Session Request is sent during move VLR old session cleanup with the Operation Indication flag set, indicating to the S-GW that the Delete Session Request should be forwarded to the P-GW for deletion of session data there.

For an inter-MME TAU treated this way, further processing of the procedure includes sending Create Session Request to the new S-GW with the Operation Indication flag set to 1 in the Indication Flags IE of that message.

This is intended to indicate to the P-GW that the existing session should be maintained and that an S-GW relocation has occurred. Having just deleted the session data on the P-GW during the move VLR action, the P-GW rejects the request with cause No context found and the triggering procedure fails.

The existing treatment of the Delete Session Request during the session cleanup of the move VLR action is appropriate when the triggering procedure is the Attach Request.

4.4 P-GW pause of charging (Feature m10219-01)

The *P-GW pause of charging* feature provides more accurate information for gateway charging.

This feature supports P-GW pause of charging that is used to solve the mismatched charging in the S-GW and the P-GW. When there is a downlink data and the UE is in ECM-IDLE state, the S-GW is not charging for data while the P-GW is charging for data. No data is being sent over the radio link; hence the CDRs in the S-GW and P-GW can be different.

- The MME upon receiving the UE Context Release Request with the cause value set to Radio Connection with UE lost, sets Abnormal release of radio link flag in Indication Flag information element (IE) to value 1 in the Release Access Bearers Request message to the S-GW across the S11 interface.
- Setting of the bit to 1 by the MME indicates to the S-GW that the access bearers are released because of abnormal release of the radio link.

This capability is always on.

Note:

GTPv2 standards require that a receiving entity silently/gracefully ignores unexpected and unknown IEs. CR1406 introduces capabilities into the MME from 3GPP TS 29.274 v12.2.0 that might not be supported by other vendor S-GWs. A global parameter can be used to shield such an S-GW from the IEs. Decision was made that S-GW should follow standards and ignore unexpected IEs as required.

4.5 Selection of action on no response to Modify Bearer (Feature m10804-02)

With the *Selection of action on no response to Modify Bearer* feature operators can select their preferred solution when no response is received from the S-GW with the Modify Bearer Request.

This feature supports a provisioning parameter to determine the action to take when there is no response to a Modify Bearer Request. Based on provisioning the MME either:

- treats the situation as a permanent failure and detaches the UE.
- treats the situation as a transient failure. This means that instead of detaching the UE, the MME simply releases the S1. That means that if the UE attempts a service request again, the MME again attempts to set up the bearer path by processing the service request. This setting should be used in association with the S-GW *inter-chassis redundancy* feature, because that feature causes silence on the S11 for several tens of seconds.

4.6 Piggyback option for dedicated bearer setup (Feature m11006-03)

With the *Piggyback option for dedicated bearer setup* feature, the operator can offer real time service for an application that requires an instant availability of a voice bearer.

This feature provides a provisioning option for S11 piggyback support for a dedicated bearer setup.

The option is a Yes/No flag that indicates whether the MME should send piggyback support for dedicated bearer setup to the S-GW in the Create Session message. If the parameter is set to `Yes`, the message indicates the MME support. If it is set to `No`, the message indicates no support.

By default, the MME always supports the piggyback option for the dedicated bearer setup. In some cases, this causes a problem in the P-GW; this parameter allows the MME to set support for piggyback to `No` in the S11 Create Session message.

4.7 Modify Access Bearer Request (Feature m20105-01)

With the *Modify Access Bearer Request* feature multiple bearers can be modified or deleted with one message.

This feature provides support for 3GPP-specified Modify Access Bearer Request (MABR) message on the S11 interface between the MME and S-GW.

The feature can be enabled on the MME using global parameter `supportModifyAccessBearerRequest`. By default, the capability is disabled.

If the feature is enabled, the MME indicates the support for the message in Sending Node Features information element (IE) of the Echo Request message to the S-GW, which indicates its support in the Sending Node Features IE of the Echo Response message.

If both the S-GW and the MME support the feature, the MME can send a Modify Access Bearer Request message on the S11 interface to the S-GW as part of the following procedures as specified in 3GPP TS 29.274:

- UE-triggered service request if there is no suspended bearer for that UE
- S1-based handover without S-GW relocation
- X2-based handover without S-GW relocation
- inter-MME E-UTRAN tracking area update without S-GW change
- intra-MME E-UTRAN tracking area update without S-GW change with active flag

MABR can be sent when all the following conditions are fulfilled:

- RAT type has not changed.
- Serving network has not changed.
- The MME does not have to send the UE's location and/or user CSG information and/or the UE time zone to the P-GW.

The following summarizes the call processing software changes for this feature:

- If the feature is enabled, S11 Echo Request and Echo Response messages contain Node Feature IE and indicate the support of the MABR.
- If the MME also receives support of MABR indication in the Node Feature IE of the Echo Request or Response message from the S-GW, the MME starts to use MABR in the following scenarios when User Location Information (ULI), CSG, and UE time zone are not reported to the P-GW:
 - In service request procedure, including SRS-triggered service request, if the UE is not suspended, the MME replaces the current multiple Modify Bearer Requests with one Modify Access Bearer Request. The MABR includes S1-U eNodeB F-TEID for all successful bearers.
 - In inter-MME tracking area update (TAU) without S-GW relocation procedure, the MME replaces the current multiple Modify Bearer Requests with one Modify Access Bearer Request before update location exchange with the HSS. The MABR includes the MME's sender F-TEID. If the TAU Request has active flag, the MME also replaces the second set of Modify Bearer Requests with a second Modify Access Bearer Request after initial context setup exchange with the eNB. The second MABR includes S1-U eNodeB F-TEID for all successful bearers.
 - In intra-MME TAU without S-GW relocation procedure, the MME replaces the current multiple Modify Bearer Requests with one Modify Access Bearer Request. The MABR includes S1-U eNodeB F-TEID for all successful bearers.
 - In X2-based handover without the S-GW relocation procedure, the MME replaces the current multiple Modify Bearer Requests with one Modify Access Bearer Request. The MABR includes S1-U eNodeB F-TEID for all successful bearers.

- In S1-based handover without S-GW relocation procedure, the MME replaces the current multiple Modify Bearer Requests with one Modify Access Bearer Request. The MABR includes S1-U eNodeB F-TEID for all successful bearers.
- In each scenario, the MABR might contain a list of bearers to be removed.

4.8 Private Extension IE enhancements (Feature m10154-01)

The *Private Extension IE enhancements* feature provides control over the use of non-access stratum (NAS) cause in Private Extension information element (IE).

This feature changes the implementation in relation to handling 3GPP standard-based solution and Private Extension IE.

Before the implementation of this feature, a single flag controls NAS cause in Private Extension along with standard-specified inclusion of NAS Release Cause IE in the Delete Bearer Command. More precisely, the flag is controlled by a global parameter and it does not switch between the standard method and Proprietary Extension IE in a straight-forward way:

- If the parameter is set to `No`, neither the standard method nor the proprietary IEs are included.
- If the parameter is set to `Yes`, both the 3GPP standard-defined NAS Release Cause IE and the proprietary NAS cause in the Private Extension are included.

Details for specific procedures when the global parameter is set to `Yes`:

- Delete Session Request: both the standard method and the proprietary extension IEs are sent.
- Delete Bearer Command: radio access network (RAN) cause and NAS cause are included within the Bearer Context list.
- Delete Bearer Command: the proprietary IE within message level IE is sent.
- Release Access Bearer: the proprietary IE is included.
- Update Bearer Response: the proprietary IE is included.
- Delete Bearer Response: the proprietary IE is included.
- Create Bearer Response: the proprietary IE is included.

This feature adds the flexibility to switch between standard IE and private extension through a global parameter. Two different global parameters are used to independently control either use of NAS cause in private extension or 3GPP-specified NAS failure indication cause code:

- NAS cause in private extension: `sendNasRanCauseOnS11`
- 3GPP specified NAS or RAN failure indication cause code: `sendSgw3gppNasRanCause`

With implementation of this feature, use of NAS cause in private extension is based on the provisioning of these parameters as follows:

- If the parameter is set to `No`, the proprietary IE is not included
- If the parameter is set to `Yes`, proprietary NAS cause in the private extension is included and applies to the following procedures:
 - Delete Session Request
 - Delete Bearer Command
 - Release Access Bearer
 - Update Bearer Response
 - Create Bearer Response

4.9 Controlling the Delay Downlink Packet Notification IE is S11 (Feature f10127-01)

Controlling the Delay Downlink Packet Notification IE in S11 feature provisions the MME to exclude or include the IE in S11 Modify Bearer Request (MBR) and Modify Access Bearer Request (MABR) message for the service request scenario.

The MME supports a global parameter `exclDelayDlPktNotifReq` to enable/disable the ability to exclude the Delay Downlink Packet Notification IE within the following S11 messages:

- Modify Bearer Request
- Modify Access Bearer Request

The allowed values of this parameter are `Yes` and `No` (default). If the parameter is set to `Yes` indicates that the IE is excluded from S11 MBR and MABR messages. If it is set to `No` indicates that the IE is included in the S11 MBR and MABR messages.

When a delay value is received at the S-GW from a particular MME, the S-GW delays sending data notification requests for all idle calls belonging to that particular MME. Once the timer expires, requests can be sent. The delay value at the S-GW is determined by the factor received in the delay value IE.

4.10 Setting up radio bearers during TAU request with GBR bearer present regardless of Active Flag value (Feature f10702-05)

This feature helps in quickly re-establishing voice calls in cases such as UE load balancing.

When the MME receives a TAU Request message (both in MME relocating and non-relocating cases), a check is made to see if the UE has any GBR bearers. If any is found, the TAU Request message is treated as if the active flag in the request was set regardless of whether the UE sets the flag or not. This treatment will result in activating the radio bearers so that a service, such as IMS voice call, is established quickly.

The feature can be enabled via provisioning. The feature provides PM counts for TAU Request Messages of UE with GBR bearers treated as a TAU Request Message with active flag.

4.11 MME relocation for multiple bearers with the same APN and PDN type (Feature f10107-03)

This feature supports maintaining all bearers for MME relocation scenarios.

When the feature is enabled and the UE has multiple default bearers with the same APN and PDN type, all bearers with the same APN and PDN type are maintained for an MME relocation.

When the feature is disabled and the UE has multiple default bearers with the same APN and PDN type, only one of the multiple bearers is maintained for an MME relocation.

This feature only applies to gateway selection mode 2.

4.12 Duplicate PDN connections during 2G/3G to 4G IRAT TAU (Feature f10137-06)

This feature supports the correct treatment of 4G bearers during inter-RAT TAU or handover when the Context Response/Forward Relocation Request message from the SGSN indicates that two or more PDP contexts share the same APN and PDN type values. By default, this feature is enabled.

4.13 NAS non-delivery indication for session management procedures (Feature f10117-06)

This feature covers queuing of NAS Session Management messages to a UE when the MME receives S1-AP NAS Non-Delivery Indication message (for a bearer activation, modification and deactivation request) with cause indicating 'x2 handover triggered' or 'S1 intra-system handover triggered'. The MME aborts the procedure when the cause is neither 'x2 handover triggered' nor 'S1 intra-system handover triggered'. The MME processes the queued message after the completion of the handover.

This feature covers the following UE-initiated session management procedures:

- Standalone PDN connectivity request
- PDN disconnect request
- Bearer resource allocation
- Bearer resource modification

This feature covers the following network-initiated procedures:

- Create bearer request
- Update bearer request
- Delete bearer request

For the successful handovers:

The MME retransmits the ESM message in DL NAS or restarts the procedure for the new eNB. This depends on the time the NAS Non-Delivery Indication message is received by the MME. When the NAS Non-Delivery Indication message is received prior to the handover initiating message (for example, the Path Switch Request message in the X2 handover case) the MME retransmits DL NAS after the handover is completed. Otherwise, current collision handling is done and the ESM procedure is restarted, for example, by sending appropriate E-RAB message depending on the procedure.

Note:

This feature does not change the current MME handling of timeouts or E-RAB failures, even if the E-RAB failure was caused by handover in progress.

MME handles the TAU interaction as it is specified in feature *MME collision handling of HO/TAU and ESM procedures (m10117-05)*. When the MME determines that the TAU request is expected, the MME starts timer `hoTauRequestWait`. The MME restarts the procedure or retransmits the request after the completion of the TAU request or upon the expiration

of the timer.

An internal hard-coded 1-second guard timer is also set. The MME retransmits the queued ESM messages upon the expiration of this timer.

In case that additional requests are sent by the GW while the handover is in progress, the MME queues additional requests as in feature *m10117-05* or rejects the request with cause 110 'Temporarily rejected due to handover/TAU/RAU procedure in progress' as supported by feature *MME support for provisioning control for GTPv2 cause code 110 (f11505-01)* with global parameter `sendSgw3gppS11cc`. After the handover or the TAU procedure is completed, the MME resumes or restarts the SM procedure which was in progress when the handover started, and for which the NAS Non-Delivery Indication message was sent by the eNB. Then the MME proceeds with the additional queued GW requests.

If the handover triggers S-GW relocation, colliding ESM procedure is rejected with cause 110 'Temporarily rejected due to handover/TAU/RAU procedure in progress'.

Inter-system handovers are not in the scope of this feature. Counter `VS.NASDownlinkNAstransportRejected_S1InterHO` is added to count the Non-Delivered NAS messages due to this reason.

In case of failed handovers, the MME retransmits the NAS message or restarts the SM procedure when UE S1 connection still exists.

4.14 MME support for differentiating LTE-M traffic (Feature f11734-01)

This feature enables the MME to handle UE LTE-M indication (CAT-M1 or CAT-M2) from the eNB and provide this information to gateways.

The RAN informs the MME that the UE is an LTE-M UE and the MME stores this information until the detach procedure is performed. During the PDN creation or modification procedure, the MME sends the LTE-M indication through the S-GW to the P-GW, which takes care of the charging. The indications are also transferred between the MMEs in the inter-MME mobility procedure.

4.15 User Location Information (ULI) handling

Features related to sending and contents of User Location Information (ULI) IE.

4.15.1 Extended procedures where ULI message is sent over S11 (Feature m10120-01)

The **Extended procedures where ULI message is sent over S11 feature provides the benefit of including User Location Information (ULI) in all the S11 messages regardless of ULI setting by the P-GW. As a result, appropriate billing can occur.**

With this feature, the MME incorporates the ULI information element (IE) in the following S11 messages irrespective of an ULI flag setting by the P-GW:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response

In addition, this feature also supports Radio Access Technology (RAT) IE and Serving Network IE to be sent in the Create Session Request and Modify Bearer Request messages.

The feature also incorporates UE Time Zone IE in the following S11 messages sent towards the S-GW:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response

This feature also provides support for reporting intra-eNB cell change using Change Notification Request message.

4.15.2 ULI enhancements (Feature m10120-05)

The **ULI enhancements feature provides capability through provisioning not to include User Location Information (ULI) information element (IE) for inbound roamers.**

With this feature, the MME does not send the ULI IE when enabled by provisioning in the following cases:

- Inbound roamer
- On the S8 interface where the home P-GW is used

The functionality is not applicable for local breakout (LBO) without S8.

The following S11 messages do not include the ULI IE when the feature is enabled by provisioning:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response

The MME supports a global parameter, `retrieveUeLocation`, to enable/disable the ability to retrieve the UE location information from the eNB. The supported values are Yes and No (default). The value Yes indicates that the MME operator policy is to use the location reporting procedure (3GPP TS 23.401 section 5.9.1) to retrieve the E-UTRAN cell global identifier (ECGI) from the eNB. The value No indicates that the operator policy is to use the last known user location information.

The MME supports provisioning of a timer, `s1ueLocationReport`, to be used in the location reporting procedure to time for the receipt of the Location Report from the eNB. The supported range is 100 ms to 8000 ms. The default value is 2000 ms (2 seconds), with an increment granularity of 100 ms.

The S1UELocationReport timer is used only in case that the request type event within the S1AP Location Reporting Control message is S1AP_DIRECT.

The MME supports provisioning of a global parameter, `uliHomeRoutedUe`, to enable/disable the ability to include the ULI IE within the following S11 messages:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response

The supported values are Yes and No (default). The value Yes indicates that the ULI IE is included in S11 messaging per 3GPP TS 29.274. The value No indicates that the ULI is not included for home routed UEs (inbound roamer UEs using S8).

The `uliEnhancement` and the `uliHomeRoutedUe` global parameters can be enabled and disabled independently of each other. The `uliHomeRoutedUe` global parameter has precedence over the `uliEnhancement` parameter.

The `uliEnhancement` parameter indicates that the ULI IE is always included in spite of the Change Reporting Action IE from the P-GW. The `uliHomeRoutedUe` parameter indicates whether the ULI is included in S11 messaging for home routed UEs using an S8 connection to the P-GW.

4.15.3 ULI enhancement for dedicated bearer activation procedure (Feature m10120-04)

This feature supports customer-specific inclusion of both E-UTRAN cell global identifier (ECGI) and tracking area identity (TAI) in Create Bearer Response message towards the S-GW.

This feature incorporates inclusion of both ECGI and TAI in Create Bearer Response message that is sent towards the S-GW across the S11 interface.

The 3GPP TS 29.274 specifically calls for inclusion of only ECGI within User Location Information (ULI) information element (IE) in Create Bearer Response message by the MME, however, this feature can be activated to deviate from standards by incorporating both ECGI and TAI in Create Bearer Response message.

4.15.4 MME/ULI to include ECGI and TAI in Update/Delete Bearer Response messages (Feature m10120-09)

This feature supports customer-specific inclusion of both E-UTRAN cell global identifier (ECGI) and tracking area identity (TAI) in Update and Delete Bearer Response messages towards the S-GW.

When this feature is enabled, the MME includes both the ECGI and TAI in User Location Information (ULI) information element (IE) across the S11 interface in the Update and Delete Bearer Response message that is sent towards the S-GW. The S-GW forwards accordingly the IE on the S5/S8 interface.

4.15.5 Provisionable control of ULI for SGW IE in Create Session Request and Modify Bearer Request (Feature f10105-02)

This feature introduces a global parameter to control inclusion of ULI for SGW IE in Create Session Request and Modify Bearer Request messages that are sent to S-GW across the S11 interface.

The global parameter `includeUliCrSessModBrr` controls the inclusion of ULI for SGW IE in Create Session Request and Modify Bearer Request messages sent to S-GW. By default, the parameter is set to `Yes`. When the parameter is set to `No`, the MME will not include the IE in Create Session Request and Modify Bearer Request messages that are sent to S-GW.

4.15.6 MME support for PSCell IE to determine UE location (Feature f10935-01)

This feature introduces MME support for the PSCell IE, which is included in either the ULI or as a standalone IE in S1 messages by the eNB.

When the location reporting control procedure is used in the MME, if the `requestPsCellInLrc` global parameter is set to `Yes`, then the MME includes additional location information. If the Additional Location Information IE is included in the Location Reporting Control message and if EN-DC is activated, the eNB includes the current PSCell in the report. Refer to the *Lawful Interception* guide for more information.

4.16 PDN type selection

Features enabling selection of PDN type (IPv4, IPv6 or IPv4v6).

4.16.1 Separate UE PDN connection per PDN type (Feature m10121-01)

The **Separate UE PDN connection per PDN type** feature supports access to IPv4 and IPv6 services for non-dual stack capable UE or non-dual stack support gateway.

The MME supports a UE connection per packet data network (PDN) type (IPv4, IPv6) to a single PDN. Before implementation of this feature, the MME only supports a single UE connection to a PDN. With this feature, the UE can have separate IPv4 and IPv6 connections

to the same PDN.

4.16.2 IPv4/IPv6 selection enhancements (Feature m10129-01)

The *IPv4/IPv6 selection enhancements* feature provides configurable IPv4/IPv6 selection conditions according to customer need.

This feature provides the following enhancements:

- Exclusion of IPv4/IPv6 S-GW address from the selection under certain conditions. The MME excludes A (IPv4)/AAAA (IPv6) S-GW records from the selection if IPv4/IPv6 address is not provisioned locally on the MME.
- Change to the current MME selection of IP version when both IPv4 and IPv6 addresses are in the sender's F-TEID in the Create Session Response message. Instead of selecting IPv6 as a preferred address for a subsequent message, the MME uses the IP version on which the Create Session Response is received. For example, if Create Session Response is received on IPv4 path, the MME uses IPv4 S11 path, if available, and the destination IP address in the IP header is set to IPv4 address in the sender's F-TEID received in the Create Session Response message. If the S11 path is not available, the session fails.

 **Note:**

The MME continues to support the IPv6 S-GW address as the preferred S-GW address if it is available.

4.16.3 Provisioning for emergency PDN type (Feature f11006-01)

With this feature, the operator is able to provision which PDN type the MME uses when the UE requests IPv4v6 type on emergency PDN establishment.

An IPv4v6 capable UE always requests IPv4v6 type, but the MME may only have had fixed selection of which type to use (IPv4, IPv6 or IPv4v6) when IPv4v6 is requested. This feature provides provisioning option to select the type.

4.16.4 MME support for configurable PDN type IPv4v6 (Feature f10174-01)

MME support for configurable PDN type IPv4v6 feature allows the operator to select the PDN type to IPv4 or IPv6 when the PDN type received from HSS is IPv4OrIpv6 and UE requested IPv4v6.

UE requests PDN connectivity with PDN type IPv4v6 for an APN. However, PDN type in the APN configuration of UE subscription data from HSS is IPv4Orv6. MME determines PDN type based on the provision.

The feature is controlled by `defaultIpv4ForPdnTypeIpv4OrIpv6` global parameter. The allowed values are `Yes` (default) and `No`. If the parameter is set to `Yes`, the selected PDN type is IPv4. If it is set to `No`, the selected PDN type is IPv6.

4.17 QoS

Features supporting quality of service handling and provisioning.

4.17.1 MME custom QoS parameter mapping from EPS to Release 99 (Feature m30107-02)

The MME custom QoS parameter mapping from EPS to Release 99 feature supports switching between two options of mapping quality of service (QoS) from evolved packet system (EPS) to R99.

This feature supports provisioning capability to select two options of how the QoS parameter values of an EPS bearer are mapped to and from Release 99 QoS parameter values of a packet data protocol (PDP) context in the MME.

- Option 1 supports the mapping specified in 3GPP TS 23.401 Annex E.
- Option 2 is provided to force use of LLC unacknowledged mode for bearers with QCI value of 4, 5, 6, 8, and 9. Option 2 achieves this by setting the SDU error ratio to 1E-4 instead of 1E-6. In this option, all other QoS parameters are set as specified in 3GPP TS 23.401 Annex E.

4.17.2 Additional extended QoS fields (Feature m30109-01)

The *Additional extended QoS fields* feature supports inclusion of extended QoS attributes upon transitioning from the LTE to 2G/3G networks.

When a UE transitions from the LTE network to the UTRAN/GERAN network, the following extended quality of service (QoS) parameters/fields are included and sent by the MME:

- Signaling Indication
- Source Statistics Descriptor
- Maximum Bit Rate for Downlink (Extended)
- Maximum Bit Rate for Uplink (Extended)
- Guaranteed Bit Rate for Downlink (Extended)
- Guaranteed Bit Rate for Uplink (Extended).

4.17.3 Flexible QoS mapping (Feature m30107-03)

Flexible QoS mapping is provided for interworking between the LTE and 2G/3G networks.

This feature provides flexible mapping between the LTE and R99 quality of service (QoS) provisioning to allow operators to select QoS mapping to provide the same user experience as when a subscriber moves between the LTE and 2G/3G networks.

- In inter radio access technology (inter-RAT) procedures where a UE moves from the LTE to UMTS/GERAN, the MME must map the evolved packet system (EPS) QoS parameters for each bearer into the set of QoS parameters used in the GPRS core network (generally referred to as R99 QoS or pre-Rel 8 QoS).
- The MME must also map R99 QoS parameters into EPS QoS parameters for each bearer when a UE moves from the UMTS/GERAN to LTE.

The MME implements this mapping as specified in *3GPP TS 23.401 Annex E*. This feature provides additional provisioning flexibility to override the fixed mapping.

QoS class indicator (QCI) to 2G/3G QoS parameters

This table maps an EPS QCI value into a set of R99 QoS parameters. The mapping is as specified in *3GPP TS 23.401*.

Key: qci {1-9}

Attributes:

- traffic_class {Conversational, Streaming, Interactive, Background}
- sdu_error_ratio { 1x10E-2, 7x10E-3, 1x10E-3, 1x10E-4, 1x10E-5, 1x10E-6, 1x10E-1 }
- transfer_delay (10-400 ms)
- traffic_handling_priority {1,2,3,blank }

Table 35: QCI to 2G/3G QoS parameters (TS 23.401)

QCI	traffic_class	sdu_error_ratio	transfer_delay	traffic_handling_priority
1	Conversational	1x10E-2	100	blank
2	Conversational	1x10E-3	150	blank
3	Conversational	1x10E-3	80	blank
4	Streaming	1x10E-6	300	blank
5	Interactive	1x10E-6	100	1
6	Interactive	1x10E-6	300	1
7	Interactive	1x10E-3	100	2
8	Interactive	1x10E-6	300	3
9	Background	1x10E-6	300	blank

Cross-checks:

- traffic_handling_priority must be blank if traffic_class is not Interactive
- traffic_handling_priority cannot be blank if traffic_class is Interactive.

2G/3G QoS parameters to QCI

Table 2G/3G QoS parameters to QCI maps each possible set of R99 QoS parameters into an EPS QCI number. In the R99 QoS, there are some seemingly independent parameters, however, upon analyzing the mappings specified in 3GPP TS 23.401 Annex E, it is clear that there are only a few discrete combinations that make sense and that must be considered in any mapping to QCI. To limit the complexity of the table, these discrete combinations are captured in a small set of enumerated values.

Key: qos_class enum {

- Conversational_Speech
- Conversational_Unknown_HighDelay
- Conversational_Unknown_LowDelay

- Streaming_Speech
- Streaming_Unknown
- Interactive_ThP1_Signaling
- Interactive_ThP1_NonSignaling
- Interactive_ThP2
- Interactive_ThP3 Background }

Attributes: qci {1..9}

Table 36: 2G/3G QoS parameters to QCI

qos_class	qci
Conversational_Speech	1
Conversational_Unknown_HighDelay	2
Conversational_Unknown_LowDelay	3
Streaming_Speech	4
Streaming_Unknown	4
Interactive_ThP1_Signaling	5
Interactive_ThP1_NonSignaling	6
Interactive_ThP2	7
Interactive_ThP3	8
Background	9

The operator has the responsibility to make the mappings in each direction (QCI to 2G/3G QoS and 2G/3G QoS to QCI) consistent.

Mapping of GPRS QoS to EPS QoS

Mapping of GPRS QoS to EPS QoS is done for incoming Gn messages (SGSN Context Response and Forward Relocation Request). There is no other case where this mapping is needed.

Classification of R99 QoS specifications into the 10 possible keys of the 2G/3G QoS Parameters to QCI table is as follows (where TC means Traffic Class, SSD means Source

Statistics Descriptor, TD means Transfer Delay, THP means Traffic Handling Priority, and SI means Signaling Indication):

- TC = Conversational
 - SSD = Speech -> Conversational_Speech
 - SSD = Unknown (or SSD not present)
 - TD >= High_Delay_Threshold -> Conversational_Unknown_HighDelay
 - TD < High_Delay_Threshold -> Conversational_Unknown_LowDelay
- TC = Streaming
 - SSD = Speech -> Streaming_Speech
 - SSD = Unknown (or SSD not present) -> Streaming_Unknown
- TC = Interactive
 - THP = 1
 - SI = Signaling -> Interactive_THP1_Signaling
 - SI ≠ Signaling (or SI not present) -> Interactive_THP1_NonSignaling
 - THP = 2 -> Interactive_THP2
 - THP = 3 -> Interactive_THP3
- TC = Background -> Background

4.17.4 UE AMBR update at the completion of TAU or handover (Feature m11333-01)

The UE AMBR update at the completion of TAU or handover feature supports a standard feature. The feature controls UE aggregate maximum bit rate (AMBR) based on calculation of a non-guaranteed bit rate (non-GBR) bearers' access point name's (APN's) AMBR.

This feature supports the scenario where the MME identifies a change in UE AMBR at the end of the tracking area update (TAU) or handover procedure. In this case, the MME validates whether UE AMBR has changed, and if it has, then MME initiates S1-AP UE context modification procedure to signal a modified UE AMBR towards the eNB.

4.17.5 Extension of maximum bit rates in QoS IE (Feature f11903-01)

The Extension of maximum bit rates in QoS IE feature enables the MME to comply with Rel11 3GPP standard which increased the range of maximum and guaranteed bit rate in QoS IE from 256 Mbps up to 10 Gbps. This feature also supports 5G early trials by

providing the capability to MME allow UE bearer setup with bit rates up to 10 Gbps, when requested by P-GW/S-GW.

This feature provides the following capabilities:

- This feature enables the MME to comply with Rel11 3GPP standard which increased the range of maximum and guaranteed bit rate in QoS IE from 256 Mbps up to 10 Gbps. The increase in bit rate was accomplished by adding extended-2 octets into the QoS IE, as shown in the following figure.

Figure 40: EPS quality of service information element

8	7	6	5	4	3	2	1	
								octet 1
								octet 2
								octet 3
								octet 4*
								octet 5*
								octet 6*
								octet 7*
								octet 8*
								octet 9*
								octet 10*
								octet 11*
								octet 12*
								octet 13*
								octet 14*
								octet 15*

Operators can control, via the global parameters `includeExtended2inEpsQosIes` and `includeExtended2inNegotiatedIes`, the inclusion of extended-2 octets in QoS IE to the UE. These two global parameter settings can be independently set and are disabled by default.

The global parameter `includeExtended2inEpsQosIes` controls the setting of the EPS QoS IE in the Activate Default/Dedicated EPS Bearer Context Request message and of New EPS QoS IE in the Modify EPS Bearer Context Request message.

The global parameter `includeExtended2inNegotiatedIes` controls the setting of Negotiated QoS IE in Activate Default/Dedicated EPS Bearer Context Request message and of the New QoS IE in the Modify EPS Bearer Context Request message.

Operators can control, via the option `includeR11QosExtensionsOnGn` of the `lteTo2G3GQosMapping` command, the inclusion of the extended-2 octets in mapped R99 QoS IE over Gn interface to the SGSN. The parameter setting is disabled by default.

- This feature extends maximum guaranteed bit rate provisioning, up to 10 Gbps, for the following QoS profiles (profile types provisionable through the `qosProfile` command):
 - custom 1 APN QoS profile
 - custom 2 APN QoS profile
 - custom 3 APN QoS profile
 - IMS APN QoS profile
 - non-IMS APN QoS profile
- When the global parameter `skipSubscribedAmbrMaxBitrate` is enabled, the MME skips the UE-subscribed APN-AMBR and UE-AMBR to allow the bearer setup with bit rates

even higher than the 4.2 Gbps maximum bit rate limit allowed by subscription in the HSS.

4.17.6 Operator defined QCI provisioning control (Feature f10167-02)

This feature introduces provisioning control for the inclusion of standard QCI value in the message that is sent back to the UE.

This feature introduces global parameter `includeMapped3gppQciToUe` to control the inclusion of standard QCI value in the message that is sent back to the UE.

If the parameter is set to `No`, the requested QCI value will be included in the NAS message that is sent back to the UE.

When the parameter is set to `Yes`, the 3GPP QCI value mapped from the operator defined QCI value will be included in the Activate Default Bearer Context Request, Activate Dedicated Bearer Context Request, and Modify Bearer Context Request messages sent to the UE. This applies to both default and dedicated bearers. This only applies to NAS messages to UE. It does not impact the QCI in S1AP or S11 messages.

Related descriptions

- [Operator defined QCI \(Feature m10202-02\)](#)
- [Enhanced operator defined QCI \(Feature f10167-01\)](#)

4.17.7 HSS/P-GW QoS parameter override for home subscribers (Feature f10112-03)

If enabled, the MME applies the local home QoS override values at the PDN connection level, at the default bearer, and dedicated bearer levels separately for a defined IMSI series. At the PDN connection level, operators can configure APN-AMBR for each requested PDN connection.

By default, the feature is disabled. The global parameter `supportQoSOverride` enables this feature.

This feature applies to:

- Initial attach
- Standalone PDN connectivity request
- TAU
- Network-initiated bearer activation (dedicated bearer) and modification

- HSS-initiated subscribed QoS modification (insert subscriber data)

i Note:

MME support for additional roaming QoS enhancements (m10520-04) does not support TAU with S-GW relocation.

The existing `qosProfile` CLI commands are used for roammers and homers. At the `imsiRangeServices` and `uePlmnServices` command levels, `qosProfile` configuration for roammers is also applicable to homers.

Note the following exceptions:

- Home subscriber QoS override is not applicable to IMS-APN.
- In `imsiRangeServices` and `qosProfile` commands, the `ueAmbrUseHssValue` and `apnAmbrUseHssValue` parameters, respectively, are not applicable for home subscribers.

4.18 MME support for behavior change for Resource Not Available in Modify Bearer and Modify Access Bearer Response (Feature f10184-01)

In this feature, the global parameter `s11CauseRsrcUnavailPdnDelInSr` is used to control the CMM behavior upon receiving "Resource Not Available" in Modify Bearer Response and Modify Access Bearer Response from the S-GW in the service request procedure.

When the feature is enabled by setting the global parameter

`s11CauseRsrcUnavailPdnDelInSr` to Yes, "Resource Not Available" is treated as a non-temporary error and Delete Session Request is sent to the S-GW. When the feature is disabled by setting the global parameter `s11CauseRsrcUnavailPdnDelInSr` to No, "Resource Not Available" is treated as a temporary error and Delete Session Request is not sent to the S-GW.

4.19 MME support for CS Service Notification Repeat after UE re-establishment (Feature f10936-01)

This feature enables the MME to retransmit the CS Service Notification message for a NAS Non-Delivery Indication with cause code "Radio Connection with UE Lost", in the

event that a subscriber loses coverage but the connection is re-established via a different eNB within a configurable time frame.

When a circuit switched fallback (CSFB) attempt occurs while a subscriber in a connected mode loses coverage, the eNB sends to the MME a NAS Non-Delivery Indication with cause code "Radio Connection with UE Lost". It is possible that the UE manages to re-establish the connection via a different eNB within a few milliseconds. This feature enables the MME to retransmit the CS Service Notification message for a NAS Non-Delivery Indication, as a response to the SGs downlink service operation, using the configurable timer

`hoRcvCsSvcNotifyNasNonDeliveryRadioConnLost`, and when the `hoRcvCsSvcNotifyNasNonDeliveryRadioConnLost` timer expires eNB will re-attempt to send a downlink message. This feature is enabled by setting the `retransCsSvcNotifyOnNasNonDeliveryRadioConnLost` global parameter to `Yes`.

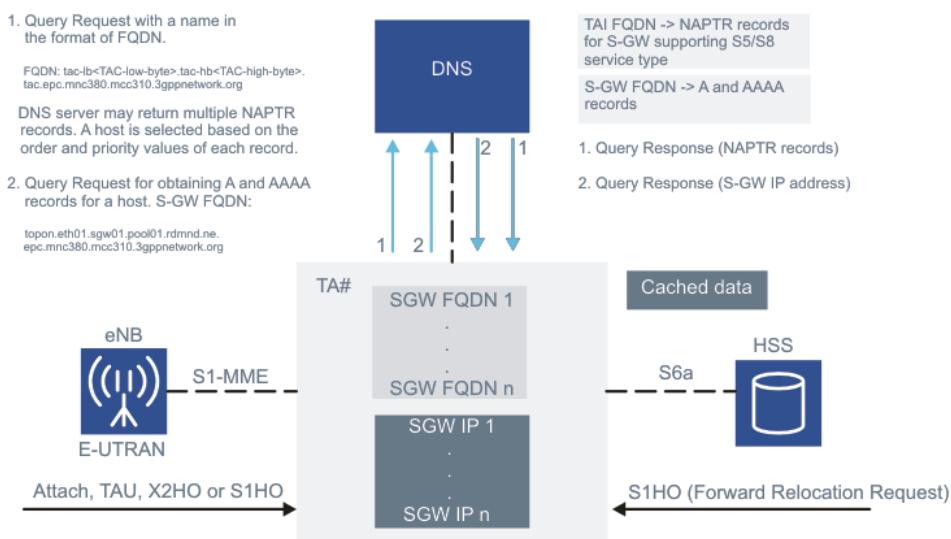
5. Node selection

Network element selections to find an appropriate S-GW and P-GW, old or new MME, and old or new SGSN are made with the help of domain name system (DNS).

Selection of S-GW, P-GW, MME, and SGSN complies with the following 3GPP specifications:

- 3GPP TS 29.303: name authority pointer (NAPTR) procedures and selection criterion
- 3GPP TS 23.003: fully qualified domain name (FQDN) specifications for various nodes and definition of services supported.

Figure 41: NAPTR procedures



S-NAPTR procedure – NAPTR records

Table 37: S-NAPTR record fields

Order	Preference	Flags	Services	Replacement
400	999	"a"	x-3gpp-sgw:x-s5-gtp	topon.Eth-0.gw32.region.operator.com
400	999	"a"	x-3gpp-sgw:x-s11	topon.Eth-1.gw32.region.operator.com
100	999	"a"	x-3gpp-sgw:x-s5-gtp	topon.Eth-0.gw33.region.operator.com
100	999	"a"	x-3gpp-sgw:x-s11	topon.Eth-1.gw33.region.operator.com

MME supports the top on and top off prefixes for topologically close node selection.

MME supports hostnames in the following form:

```
<"topon" | "topoff"> . <single-label-interface-name> . <canonical-
node-name>
```

For example: `topon.Eth-0.SGW32.region.operator.com`

Canonical node name is `region.operator.com`. A node must have a single canonical node name.

Table 38: Definitions of NAPTR record fields

Field name	Description
Order	A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed. The list of NAPTR records returned must be ordered from the lowest to the highest and the lowest order number is tried first.
Preferences	A 16-bit unsigned integer specifying the order in which NAPTR records with an equal order value should be processed. The lower preference value is processed first.
Flags	A character string. S-NAPTR procedure allows only three values: “a”, “s” and “”. The flags indicate further actions that must be taken on the records. The “” flag indicates that further query should be launched to obtain additional NAPTR records. The “a” and “s” flags are called terminal flags indicating end of the NAPTR processing. In the case of an “s” flag, DNS query is launched with the replacement field target to obtain service (SRV) records. In the case of an “a” flag, an IP address is sought for the replacement field target.
Services	A character string that identifies a service and its associated protocol that is supported by the host. The service names (app-service) and protocol names (app-protocol) used by the evolved packet core (EPC) are specified in 3GPP TS 23.003 section 19.4.3.
Regular Expression	A character string. Not used by the EPC discovery procedures.
Replacement	A domain name in label format. This is the next domain name to query to obtain A, AAA, or SRV records.

At attach, MME first selects S-GWs that service the tracking area identity (TAI) and support S5 interface using the S-NAPTR procedure.

- For a roamer, MME selects an S-GW supporting both S5 and S8 interfaces.
- From the list of select S-GWs, an S-GW host with lowest order value is selected.
- If there are more than one host with the same order value, the MME assigns UE sessions in proportion to the preference value. Hosts with low preference value are considered to have higher capacity.
- S-GW hosts with high order value are considered as backup S-GWs and are used if S-GW with low order values cannot be used.
- The MME uses the canonical node name of the S-GW selected to select a NAPTR record supporting S11 service on the same S-GW node. If two or more records are selected, the MME uses the order and priority value of each record to distribute the traffic.
- The MME launches a DNS query to obtain A and AAAA records for the selected S5 and S11

interface.

- All the sessions of UE are assigned to the same S-GW host.

For tracking area update (TAU) request, X2 handover, S1 handover and IRAT handover, if a different S-GW provides services for the new (target) TAI, the MME discovers the S-GW or S-GWs serving the new TAI using S-NAPTR procedures. Selection of S-GW based on TAI enables selection of S-GW geographically close to the serving eNB.

- For X2 handover, S1 handover and TAU, the MME continues to use the current S11 interface if the S-GW supporting the interface exists in the NAPTR records irrespective of the order value of the other S-GW NAPTR records.
- If a new S-GW needs to be selected, the MME simply uses the order and preference values to select it.

A name in the format of FQDN is used for NAPTR query:

```
tac-lb<TAC-low-byte>.tac-hb<TAC-
highbyte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

In the FQDN, tracking area code (TAC), mobile network code (MNC), and mobile country code (MCC) are obtained from TAI received in the S1-AP message (that is, current TAI of UE).

MME selection of P-GW

The MME discovers and selects a P-GW for

- Attach Request for the selection of a P-GW of default APN.
- any UE PDN Connectivity Request.

The MME uses the following access point name (APN) configuration fields obtained from the HSS for the selection of P-GW:

- APN network identifier (APN-NI) (Service-Selection attribute-value pair (AVP))
- visited network (VPLMN) dynamic address allowed – used to allow local breakout or not (VPLMN-Dynamic-Address-Allowed AVP)
- P-GW IP address (MIP-Home-Agent-Address AVP)
- P-GW fully qualified domain name (FDQN) (MIP-Home-Agent-Host AVP)
- P-GW allocation type (PGW-Allocation-Type AVP):
 - Static: Use P-GW IP address if received or use FQDN if received to obtain A and AAAA records.
 - Dynamic: S-NAPTR procedure uses a FQDN derived using APN-OI and APN-NI.

For a non-roamer, the MME constructs a name in the form of FQDN for S-NAPTR procedure

as follows:

- APN-NI.mnc<MNC>.mcc<MCC>.3gppnetwork.org
 - This format is only used for DNS query.
 - APN sent to S-GW, MME, or SGSN is of the APN-NI.APN-OI format, where APN-NI can consist of three or more labels and APN-OI consists of mnc<MNC>.mcc<MCC>.gprs.
 - MCC and MNC used are UE's HPLMN.
- MME selects P-GWs supporting 'app-protocol' x-s5.

For a roamer, the MME sets the MNC and MCC as follows:

- If VPLMN dynamic address is not allowed either by the HSS or local roaming provisioning, the MME considers this as home routed traffic:
 - MCC and MNC obtained from the UE's international mobile subscriber identity (IMSI) are used.
 - the MME selects P-GWs supporting 'app-protocol' x-s8.
- If VPLMN dynamic address is allowed by both the subscriber data and local provisioning, the MME selection of P-GW in the VPLMN is allowed: MCC and MNC of the visited PLMN (MME's home PLMN) is used.
- The MME selects P-GWs supporting 'app-protocol' x-s5.
- The MME can receive multiple NAPTR records for an APN FQDN query.
- The MME selects P-GWs topologically close to the selected S-GW by suffix label matching.
- The MME assigns UE session based on the order and priority values if multiple P-GWs are selected.
- The MME supports APN-OI replacement string for the home routed traffic.

MME re-selection of S-GW and P-GW

Re-selection of S-GW and P-GW is done for Create Session Request failures or if the MME timed out waiting for Create Session Request.

Scenarios that require S-GW and P-GW re-selection:

- Attach procedure
 - Request Type information element (IE) of PDN Connectivity Request message is set to value Handover.
 - Request Type IE of PDN Connectivity Request message is set to values other than Handover.
- Standalone PDN connectivity request procedure
 - Request Type IE of PDN Connectivity Request message is set to value Handover.
 - Request Type IE of PDN Connectivity Request message is set to values other than Handover.

- S-GW relocation because of TAU, X2 handover, or S1 handover.

Table 39: Attach procedure: Cause values and MME actions

Attach							
Cause value	MME actions						
	Request Type IE value in PDN Connectivity Request and selection mode						
	Handover + Selection Mode 1	Handover + Selection Mode 2	Other than Handover + Selection Mode 1	Other than Handover + Selection Mode 2			
Timed out waiting for Create Session Response	Select another S-GW	P-GW and S-GW pair	Select another S-GW	P-GW and S-GW pair			
64 - Context not found and cause source is S-GW	Reject	Reject	Reject	Reject			
72 - System failure and cause source is S-GW	Reject	P-GW and S-GW pair	Reject	P-GW and S-GW pair			
73 - No resources available and cause source is S-GW	Select another S-GW	P-GW and S-GW pair	Select another S-GW	P-GW and S-GW pair			
78 - Missing or unknown APN and cause source is S-GW	Reject	P-GW and S-GW pair	Reject	P-GW and S-GW pair			
94 - Request rejected and cause source is S-GW	Select another S-GW	P-GW and S-GW pair	Select another S-GW	P-GW and S-GW pair			
100 - Remote peer is not responding	Select another S-GW	P-GW and S-GW pair	Select another S-GW	P-GW and S-GW pair			
64 - Context not found and cause source is P-GW	Select another P-GW	Select another P-GW	Reject	Reject			
72 - System failure and cause source is P-GW	Reject	Select another P-GW	Reject	P-GW and S-GW pair			

Attach							
Cause value	MME actions						
	Request Type IE value in PDN Connectivity Request and selection mode						
	Handover + Selection Mode 1	Handover + Selection Mode 2	Other than Handover + Selection Mode 1	Other than Handover + Selection Mode 2			
73 – No resources available and cause source is P-GW	Select another P-GW	Select another P-GW	Select another P-GW	P-GW and S-GW pair			
78 – Missing or unknown APN and cause source is P-GW	Reject	Select another P-GW	Reject	P-GW and S-GW pair			
94 – Request rejected and cause source is P-GW	Reject	Select another P-GW	Select another P-GW	P-GW and S-GW pair			

Note:

Re-selection is done from the S-GW and P-GW candidate list obtained from S-NAPTR procedure using appropriate FQDN.

Note:

When UE moves between E-UTRAN and enhanced High Rate Packet Data (eHRPD), the same P-GW is maintained so that UE and P-GW maintain the same session context.

Note:

Request is rejected for all other cause values.

MME re-selection of S-GW and P-GW - Standalone PDN Connectivity Request

Table 40: Standalone PDN connectivity request procedure: Cause value and MME actions

Standalone PDN connectivity request				
Cause value	MME actions			
	Request Type IE value in PDN Connectivity Request and selection mode			
	Handover + Selection Mode 1	Handover + Selection Mode 2	Other than Handover + Selection Mode 1	Other than Handover + Selection Mode 1
Timed out waiting for Create Session Response	Reject	Reject	Reject	Reject
64 – Context not found and cause source is S-GW	Reject	Reject	Reject	Reject
72 – System failure and cause source is S-GW	Reject	Reject	Reject	Reject
73 – No resources available and cause source is S-GW	Reject	Reject	Reject	Reject
78 – Missing or unknown APN and cause source is S-GW	Reject	Reject	Reject	Reject
94 – Request rejected and cause source is S-GW	Reject	Reject	Reject	Reject
100 – Remote peer is not responding	Reject	Select another P-GW	Select another P-GW	Select another P-GW
64 – Context not found and cause source is P-GW	Select another P-GW	Select another P-GW	Reject	Reject

Standalone PDN connectivity request				
Cause value	MME actions			
	Request Type IE value in PDN Connectivity Request and selection mode			
	Handover + Selection Mode 1	Handover + Selection Mode 2	Other than Handover + Selection Mode 1	Other than Handover + Selection Mode 1
72 – System failure and cause source is P-GW	Reject	Select another P-GW	Select another P-GW	Select another P-GW
73 – No resources available and cause source is P-GW	Select another P-GW	Select another P-GW	Select another P-GW	Select another P-GW
78 – Missing or unknown APN and cause source is P-GW	Reject	Select another P-GW	Select another P-GW	Select another P-GW
94 – Request rejected and cause source is P-GW	Reject	Select another P-GW	Select another P-GW	Select another P-GW

Note:

Re-selection is done from the S-GW and P-GW candidate list obtained from S-NAPTR procedure using appropriate FQDN.

Note:

When UE moves between E-UTRAN and eHRPD, the same P-GW is maintained so that UE and P-GW maintain the same session context.

Note:

No S-GW re-selection is done as the S-GW selected in the attach procedure cannot be changed.

Note:

Request is rejected for all other cause values.

MME re-selection of S-GW and P-GW – S-GW relocation

Table 41: S-GW relocation: cause values and MME actions

S-GW relocation for TAU, X2 handover and S1 handover	
Cause	MME actions
Timed out waiting for Create Session Request	If the first default bearer, select another SGW; otherwise reject
64 – Context not found and cause source is S-GW	Reject
72 – System failure and cause source is S-GW	If the first default bearer, select another SGW; otherwise reject
73 – No resources available and cause source is S-GW	If the first default bearer, select another SGW; otherwise reject
78 – Missing or unknown APN and cause source is S-GW	Reject
94 – Request rejected and cause source is S-GW	If the first default bearer, select another SGW; otherwise reject
100 – Remote peer is not responding	If the first default bearer, select another SGW; otherwise reject
64 – Context not found and cause source is P-GW	Reject
72 – System failure and cause source is P-GW	Reject
73 – No resources available and cause source is P-GW	Reject
78 – Missing or unknown APN and cause source is P-GW	Reject
94 – Request rejected and cause source is P-GW	Reject

Note:

Re-selection is done from the S-GW and P-GW candidate list obtained from S-NAPTR procedure using appropriate FQDN.

Note:

TAU Request is rejected for all other cause values.

Note:

Handover is aborted for all other cause values.

5.1 DNS

DNS-based node selection features.

5.1.1 Enhancements to MME DNS support to discover MME/P-GW/S-GW/SGSN (Feature m10103-06)

The **Enhancements to MME DNS support to discover MME/P-GW/S-GW/SGSN feature increases the number of S-GWs that can be handled and enhances domain name system (DNS) troubleshooting.**

This feature supports the following capabilities:

- Handling up to 80 name authority pointer (NAPTR) records per query to support increased number of S-GWs and MMEs serving an area.
- Purging one or more entries from the DNS cache. This facilitates updates of DNS cache before time to live (TTL) expires by forcing the MME to launch DNS queries for the missing NAPTR entries.
- A CLI command to output DNA cache. Options to output are:
 - Entire cache
 - Entries matching a single label (for example, pgw, tac-lb01)
 - Multiple labels (for example, pgw, northwest)
 - Entries matching patterns such as <label1>.<label2> (for example, tac-lb-1.tac-hb02)
 - All entries for a service type (for example, s5, s11, s10, s3)

- All entries matching an order, a priority, or order and priority

5.1.2 MME support for increased S-GW FQDNs limit in DNS response (Feature f12201-01)

The *MME support for increased S-GW FQDNs limit in DNS response* feature increases the supported total number of S-GW DNS query responses to 256.

For S-GW DNS queries, the MME supports a total of NAPTR “a” flag records plus NAPTR “s” flag records plus SRV records of at least 256. MME supports up to 254 SRV records.

5.1.3 SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN (Feature m10103-07)

The *SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN* feature enhances current name authority pointer (NAPTR) procedures to support service records (SRV RR) for better management of nodes.

This feature supports SRV RRs for the MME domain name server (DNS) discovery of MME, P-GW, S-GW, or SGSN.

DNS SRV is defined in *RFC 2782* and it allows a use of multiple servers for load balancing and fail-over. Support of SRV RR requires the MME to support NAPTR resource record flag “s” in addition to the “a” flag. The “s” flag causes the straightforward name authority pointer (S-NAPTR) procedure to query for intermediary SRV records that point to A and AAAA records.

A SRV RR consists of the fields described in the table. The *3GPP TS 29.303* has not defined Service and Proto values to be used. However, service names and protocol names defined in *3GPP TS 23.003 section 19.4.3* can be used to construct `srvc.prot.name`. The MME ignores the Proto and Port fields as the MME uses the specified protocol (UDP or TCP) and port numbers as specified for an interface by the 3GPP standards.

Table 42: RData field of the RR record

Field Name	Description
Service	The symbolic name of the desired service, as defined in Assigned Numbers [RFC 1700] or locally. An underscore (_) is prepended to the service identifier to avoid collisions with DNS labels that occur in nature.
Proto	The symbolic name of the desired protocol, with an underscore (_) prepended to prevent collisions.
Priority	A 16-bit unsigned integer specifying the priority of the target host. A client must attempt to contact the target host with the lowest numbered priority it can reach.
Weight	A 16-bit unsigned integer used for the server selection. The weight field specifies a relative weight for the records with the same priority. A server with a higher relative capacity is assigned proportionately higher weight. A client should select a server proportionate to its weight.
Port	Port number in the range of 0-65535. The 3GPP TS 29.303 does not specify what port numbers should be used for different services. These ports may conflict with the ports specified in 3GPP TS 29.274.
Target	This is the domain name of the target host and might require a query to obtain A and AAAA records for IP addresses. A DNS server can return A and AAAA records in the additional section of DNS query reply.

The MME uses the priority and weight fields in the S-GW, P-GW, MME, or SGSN selection as follows:

- The MME first selects a host with the lowest priority value.
- If there are multiple hosts with the same priority value, the MME assigns the UE sessions to a host in proportion to the weight. Hosts with high weight value are considered to have higher capacity.
- Hosts with high priority values are considered as backup, and they are selected if hosts with low priority values are not available.

The MME supports the following service types for the SRV RR:

- x-3gpp-sgw:x-s5-gtp, x-3gpp-sgw:x-s8-gtp, x-3gpp-sgw:-x-s5-pmip, x-3gpp-sgw:x-s8-pmip, x-3gpp-sgw:x-s11
- x-3gpp-pgw:x-s5-gtp, x-3gpp-pgw:x-s8-gtp, x-3gpp-pgw:x-s5-pmip, x-3gpp-pgw:x-s8-pmip, x-3gpp-pgw:x-gn, x-3gpp-pgw:x-gp
- x-3gpp-sgsn:x-gn, x-3gpp-sgsn:x-s3

- x-3gpp-mme:s10

S-GW and P-GW selection

This feature does not change the existing requirements or introduce any new requirements to the selection of S-GW and P-GW supporting a service type (s5, s8, s5+s8, and s11) for a UE that is a home subscriber, or a roaming subscriber, or a roaming subscriber treated as a home subscriber during the attach procedure, idle mobility, and handovers, other than expanding the S-GW and P-GW candidate list to include SRV RR.

- Mode 1

For the mode 1 selection, the MME first selects a NAPTR record, based on the order and preference fields of the S-GW NAPTR records. If the selected record has “s” flag, another DNS query is launched using the replacement string to obtain SRV records. The MME selects an S-GW based on the priority and weight fields of the SRV records. These records are sorted from the lowest numbered priority to the highest number priority and then the highest numbered weight to the lowest numbered weight of the RR. The MME selects the first S-GW from the list. If the MME has to reselect an S-GW, it selects an S-GW that is next in the list to the previously selected S-GW. In case of S-GW reselection, the MME makes one additional attempt to select an S-GW. If there are not enough SRV records for reselection, the MME uses other NAPTR records for the remaining attempts. This selection procedure applies to S-GW selection at attach and also whenever a new S-GW is selected because of S-GW relocation.

For P-GW selection, after obtaining the access point name (APN) NAPTR RR, the MME launches further queries to resolve NAPTR records with “s” and “a” flags to build a complete P-GW candidate list. This list is used to find a P-GW topologically close to the selected S-GW by label matching among the P-GW and S-GW names that start with topn. If there are multiple SRV RRs of a NAPTR RR with equal label matches, the MME uses the preference and weight fields of the SRV record to select a P-GW. If there are records with equal label matching across two or more NAPTR records, the MME uses the NAPTR record’s preference and order attributes to select a NAPTR record. If the NAPTR record is associated with SRV records, the MME uses the SRV records for the selection of P-GW from the set of SRV records with the label matching. Reselection of P-GW, in this case, remains the same.

- Mode 2

In the mode 2 selection, topologically close P-GW and S-GW are selected irrespective of the values of the order and preference fields of the S-GW at attach from the candidate list of P-GWs and S-GWs. If there are multiple P-GW and S-GW pairs with equal topological closeness, the MME uses the S-GW order and preference fields to select a S-GW and P-GW pair. The same algorithm is continued to be used with SRV records to find S-GW and P-GW

pair. The SRV records require the MME to launch queries to resolve NAPTR records with “s” flag to build a complete P-GW and S-GW candidate list. These candidate lists are used in finding a S-GW and P-GW pair with the most number of label matches. If there are S-GW and P-GW pairs with equal label matching, S-GWs are used for the selection. If there are multiple SRV RRs of a NAPTR RR with equal matching labels, the MME uses the preference and weight fields of the SRV record of an S-GW in selecting an S-GW. If there are records with equal matching labels across two or more NAPTR records, the MME uses the NAPTR record’s preference and order attributes to select NAPTR record. If the NAPTR record is associated with SRV records, the MME uses the SRV records for the selection of S-GW from the set of SRV records with the matching labels.

This feature does not change the current selection of S-GW selection algorithm during inter radio access technology (IRAT) and intra-LTE mobility other than extending the S-GW candidate list. The procedure consists of selecting a P-GW from the active list of packet data network (PDN) connections and using the P-GW fully qualified domain name (FQDN) to find an S-GW that is topologically close to the selected P-GW by label matching. After obtaining the S-GW NAPTR RR, the MME launches further queries to resolve NAPTR records with “s” and “a” flags to build a complete S-GW candidate list. An S-GW that is topologically close to the selected P-GW is selected by label matching. If there are multiple SRV RRs of a NAPTR RR with equal matching labels, the MME uses the preference and weight fields of the SRV record of a S-GW in selecting a S-GW. If there are records with equal matching labels across two or more NAPTR records, the MME uses the NAPTR record’s preference and order attributes to select an NAPTR record. If the NAPTR record is associated with SRV records, the MME uses the SRV records for the selection of P-GW from the set of SRV records with the matching labels.

This feature does not change the reselection of S-GW and P-GW other than using the SRV records for the selection of an alternate S-GW and P-GW pair.

MME and SGSN selection

The MME and SGSN selection is enhanced to handle NAPTR records with “s” flag. The MME first selects a NAPTR record based on the order and preference fields of the NAPTR RR received. If the selected NAPTR RR has “s” flag, the MME launches a query to obtain SRV RR and selects an MME/SGSN based on the priority and weight fields.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

5.1.4 NAPTR records with empty flag (Feature m10103-16)

The **NAPTR records with empty flag** feature enhances current name authority pointer (NAPTR) procedures to support empty resource record (RR) for better management of nodes.

This feature supports NAPTR RR with “” for the selection of a P-GW for both mode 1 and mode 2 selection. The MME supports this NAPTR RR with the following service types:

- x-3gpp-pgw:x-s5-gtp
- x-3gpp-pgw:x-s8-gtp
- x-3gpp-pgw:x-gn
- x-3gpp-pgw:x-gp

The MME supports load balancing across NAPTR RR with “”, “a” and/or “s” flag.

The MME drops NAPTR RR with “” flag (that is, does not use these) in any query using the replacement string of a NAPTR RR with “” flag, that is, the MME only uses NAPTR RR with “s” and “a” flags.

For a home subscriber or for a local breakout case, the MME prefers a P-GW supporting both x-s5-gtp and x-gn. If there are no P-GWs supporting both, the MME selects a P-GW supporting x-s5-gtp only, if available.

For a home routed roamer traffic, the MME prefers a P-GW supporting both x-s8-gtp and x-gp. If there are no P-GWs supporting both the service types, the SGSN selects a P-GW supporting x-s8-gtp only, if available.

This feature is dependent on the S-GW and P-GW selection mode 1 and mode 2 of the SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN feature.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)
- [SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN \(Feature m10103-07\)](#)

5.1.5 Fallback to default APN-OI on DNS failures (Feature m10121-04)

The **Fallback to default APN-OI on DNS failures** feature increases a chance of a successful PDN connectivity if name authority pointer (NAPTR) query for an access point name (APN)

using APN OI replacement fails (that is, the MME timed out waiting for domain name system (DNS) server response or DNS query response has not returned any valid resource record (RR)).

This feature is applicable to home subscriber UEs, UEs that are treated as home subscribers, and inbound roammers.

- Home subscriber UE:

The MME launches the APN NAPTR query with APN OI of the APN fully qualified domain name (FQDN) set to the UE home network (HPLMN) ID (that is, public land mobile network (PLMN) ID in the UE international mobile subscriber identity (IMSI)).

- Treat as home subscriber UE:

The MME launches a second APN NAPTR query with APN OI of the APN FQDN set to the provisioned P-GW DNS domain override. If this NAPTR query fails to return any valid RR or times out, the MME launches a third APN NAPTR query with APN OI set to the serving PLMN ID.

- Roamer UE:

The MME launches a second APN NAPTR query with APN OI of the APN FQDN set to the provisioned home routed APN OI override for the roamer UE. If this NAPTR query fails to return any valid RR or times out, the MME launches a third APN NAPTR query with APN OI of APN FQDN set to the UE HPLMN ID (that is, PLMN ID in UE IMSI).

5.1.6 Removing setting of MSB of MME Group ID provisioning restriction (Feature m10533-02)

The *Removing setting of MSB of MME Group ID provisioning restriction* feature supports provisioning of the MME group ID range from x0000 to xFFFF. It provides smooth inter-access mobility between 2G/3G and LTE.

Additionally, this feature supports double dipping of domain name system (DNS) to obtain old node's IP address if the MME must obtain the UE context from the old node.

For attach/tracking area update (TAU) procedures, the MME uses the non-access stratum (NAS) message markers to first determine the serving node, such as Old Guti Type IE, Old P-TMSI Signature, and Additional GUTI. If any of the markers are present, the MME only relies on those markers to determine the serving node type (that is, the SGSN or MME). If the NAS message does not contain previous serving node information element (IE) markers, the MME may perform a double DNS dip to determine the serving node.

- The first attempt is based on the most significant bit (MSB) of the Group ID in the globally unique temporary identity (GUTI).

- If the MSB of the group ID is set to 0, the MME first uses name authority pointer (NAPTR) query to obtain SGSN IP address.
- If no records are returned, the MME tries the NAPTR query for MME IP address whenever MSB bit of the Group ID in GUTI received from the UE is not set.

5.1.7 S-GW NAPTR records with empty flag (Feature f10175-01)

This feature enhances the current S-GW selection method by supporting NAPTR RR with empty flag.

The MME supports NAPTR RR with the "" flag for the S-GW queries for both mode 1 and mode 2 S-GW selections. The MME supports service types x-s5-gtp, x-s8-gtp, and x-s11-gtp.

The MME supports load balancing across NAPTR RR with the "", "a" and "s" flags.

The MME drops S-GW NAPTR RR with the "" flag in any query using the replacement string of a NAPTR RR with the "" flag. The MME only uses S-GW NAPTR RR with the "s" and "a" flags.

If the MME receives more than 16 S-GW NAPTR RR "" flag records, only the first 16 of the NAPTR queries are performed.

This feature can be enabled and disabled using global parameter `mmeSgwQueryEmptyflagRr`. By default, the feature is disabled.

This feature can only be enabled when the MME support for NAPTR RR with "s" flag feature is enabled using global parameter `supportDnsSrv`.

5.1.8 Increased number of SRV queries (Feature m10103-13)

The *Increased number of SRV queries* feature supports a large number of SRV records.

Before implementation of this feature, the MME S-GW and P-GW SRV scaling rules were:

- If the MME receives more than 32 P-GW name authority pointer (NAPTR) "s" flag records, it is acceptable for the MME to do SRV queries for only the first 32.
- If the MME receives more than eight S-GW NAPTR "s" flag records, it is acceptable for the MME to do SRV queries for only the first eight.

With the implementation of this feature, the MME does up to 64 SRV queries for P-GW

NAPTR “s” flag records and up to 16 SRV queries for S-GW NAPTR “s” flag records.

This feature is dependent on the *SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN* feature.

Related descriptions

- [SRV records for MME DNS discovery for MME/P-GW/S-GW/SGSN \(Feature m10103-07\)](#)

5.1.9 DNS enhancement (Feature f12205-01)

This feature optimizes CPPS aDNS and IPDS unbound cache sizes and provides IPDS unbound to external DNS server communication monitoring.

The CMM domain name lookup is used by CMM call processing to resolve FQDN/hostname on S-GW/P-GW selection and mobility tracking area inquiry.

This feature provides real-time DNS query route selection, optimized CPPS aDNS and IPDS unbound cache sizes. In addition, CMM to external DNS server communication monitoring is provided.

The feature functions as follows:

- Provides CPPS DNS query request to IPDS unbound path selection.
- Provides CPPS aDNS cache usage monitoring and information alarm.
- Adds DNS query guard timers to avoid CxnMgr “stuck” object when encounter event such as CPPS session distributor messaging abnormality.
- Adds new IPDS unbound to external DNS server(s) connectivity monitoring. It monitors unbound real time calculated round trip timeout value (RTO) to gauge the usability of each IPDS unbound to external server endpoints. A major or critical communication degradation alarm is raised on per IPDS pool ID 0 members to external DNS server endpoint basis.

5.1.10 MME support for steering option 3x subs to combo nodes for capacity offload (Feature f10004-01)

With this feature, a provider can control the use of the 4G core or the 5G core (via combined P-GW-C+SMF) for specific PDN connections and type of UEs by provisioning UE subscription at the HSS.

The feature enables support for using a combination of P-GW-C+SMF for 3x UEs by

manipulating the HSS subscriber profile and leveraging the existing 4G DNS-based node selection mechanism. As part of this feature, an operator can configure the level of 5G core penetration to active PDN connections of 3x subscribers who are eligible to use P-GW-C+SMF.

When the *MME support for steering option 3x subs to combo nodes for capacity offload* feature is enabled, the MME evaluates the received “Access to 5GC not allowed” bit of the Core-Network-Restrictions and the Interworking-5GS-Indicator AVPs of the APN Configuration AVP to decide the selection of the SMF+P-GW-C (combination P-GW).

 **Note:**

“Access-Restriction-Data” AVP is not considered for combination P-GW selection.

DNS network/service capabilities and node selection

The MME searches DNS records for service capabilities for different subscribers as shown in the following table:

Table 43: Search order for service capabilities

Subscriber type	Provisioning	Specified UE usage-type (UUT)	Search order of service capabilities
5G-enabled (N1 mode and/or DCNR capable)	5GC operation	Yes	1. +nc-nr.smf+ue-<uut> 2. +nc-smf+ue-<uut> 3. +nc-nr+ue-<uut> 4. +ue-<uut> 5. +nc-nr.smf 6. +nc-smf 7. +nc-nr 8. No modifiers
5G-enabled	5GC operation	No	1. +nc-nr.smf 2. +nc-smf 3. +nc-nr 4. No modifiers
5G-enabled	EPC operation (not allowed using combination PGW-C+SMF)	Yes	1. +nc-nr+ue-<uut> 2. +ue-<uut> 3. +nc-nr 4. No modifiers
5G-enabled	EPC operation	No	1. +nc-nr 2. No modifiers
4G-only	Not applicable	Yes	1. +ue-<uut> 2. No modifiers
4G-only	Not applicable	No	No modifiers

Configuration options

The global parameter `smfPgwcSelSupport` enables selection of combined P-GW-C using only HSS subscription information as criteria, without considering UE N1 mode support. By default, it is disabled.

This feature also provides the following configuration options:

- The ability for the MME to prioritize NC-NR capable gateway over combined P-GW-C capable gateway. If enabled, the MME gives priority to an NC-NR capable gateway over a combined P-GW-C capable gateway when DNS query retrieves multiple candidates (each

serving only one of these service parameters).

- The selection of DC-NR-capable P-GW-C for LTE-only UEs.
- The limit to the number of SMF+P-GW-C nodes that the MME tries before falling back to standalone P-GW, which is set independently for 3x-capable and N1-capable UEs.

 **Note:**

Pure 4G-only subscribers do not have a configurable limit.

- Tunable parameters to control the percentage of traffic (0% - 100%) that is sent to the SMF+P-GW-C. If this percentage is set to 0%, the MME does not send any traffic to the SMF+P-GW-C. If parameter is set to 100%, the MME sends all 5GC-eligible traffic to the SMF+P-GW-C. Separate parameters are available for UEs that do not support N1 (NSA/option 3x UEs that have been specifically configured to use the 5G core) and for UEs that do support N1 (future SA/option 2 UEs).

When the associated `standalone` service parameter is requested and the respective fallback parameter is enabled, fallback is supported. If fallback is not possible, the call is rejected.

Service selection for multiple service parameter scenarios

The table shows the search order for service capabilities when multiple service parameters are requested.

Table 44: Service selection for multiple service parameters

	Search order for service capabilities
SMF over DCNR priority (default)	<ol style="list-style-type: none"> 1. +nc-nr.smf+ue-<uut> 2. +nc-smf+ue-<uut> 3. +nc-nr+ue-<uut> 4. +ue-<uut> 5. check DCN fallback; if fallback is disabled, reject 6. +nc-nr.smf 7. +nc-smf 8. +nc-nr 9. check DCNR fallback; if fallback is disabled, reject 10. No modifiers
DCNR over SMF priority	<ol style="list-style-type: none"> 1. +nc-nr.smf+ue-<uut> 2. +nc-nr+ue-<uut> 3. +nc-smf+ue-<uut> 4. +ue-<uut> 5. check DCN fallback; reject if fallback disabled 6. +nc-nr.smf 7. +nc-nr 8. check DCNR fallback; if fallback is disabled, reject 9. +nc-smf 10. No modifiers

5.1.11 MME support for steering option 3x subs to combo nodes for capacity offload - phase 2 (Feature f10004-02)

This feature supports the ripcord bypass functionality, which is determined based on the DNS entries received by the MME during DNS resolution.

Ripcord basically means traffic offload during failover. If pre-5GC core is unable to correctly process PDU session requests, the MME fails over to use the P-GW instead of SMF+P-GW-C automatically.

Ripcord controls are applied only if the DNS returns a mix of SMF+P-GW-C and P-GWs for a specific DNS resolution. This applies to both the retry limit and the tunable dial as follows:

- If the DNS returns a mix of SMF+P-GW-C and P-GW FQDNs for the resolved APN, then the MME uses the ripcord features as originally designed:
 - The MME attempts to use x SMF+PGW-C nodes before switching to P-GWs, where x is

the configured limit based on the ripcord feature.

- The MME only sends y percent of eligible 5GC subscribers to an SMF+P-GW-C, where y is the configured ripcord dial value.
- If the DNS returns only SMF+P-GW-C FQDNs for the resolved APN, the MME ignores the ripcord functionality.

The MME performs retry attempts either for N1-mode UEs or 3x UEs, as configured in *MME support for steering option 3x subs to combo nodes for capacity offload (Feature f10004-01)*, if there is an additional combo SMF+PGW-C node available to select based on the DNS response.

Additionally, new PM counters are introduced for reporting the number of matching FQDN labels between S-GW and P-GW FQDNs. Counters are pegged whenever the MME attempts bearer setup towards the selected S/P-GW pair.

The following table shows the search order for service capabilities when multiple service parameters are requested, and all present DNS entries include the smf service (combo SMF+P-GW-C nodes).

Table 45: Search order for service capabilities

Subscriber type	Provisioning	Specified UE usage-type (UUT)	Search order of service capabilities
5G-enabled (N1 mode and/or DCNR capable)	5GC operation	Yes	1. +nc-nr.smf+ue-<uut> 2. +nc-smf+ue-<uut> 3. +nc-nr.smf 4. +nc-smf
5G-enabled	5GC operation	No	1. +nc-nr.smf 2. +nc-smf

5.1.12 Steering option 3x subs to combo nodes for capacity offload enhancement (Feature f13034-01)

The feature enhances *MME support for steering option 3x subs to combo nodes for capacity offload (f10004-01)* by introducing the global parameter `minFqdnLabelMatching`.

When the global parameter `minFqdnLabelMatching` to Yes, the MME can use the minimum FQDN label matching criteria during the first pass and selects SP-GW pairs based on service parameters. Without the feature, the MME gets available S-GWs from the DNS

with TAC NAPTR request. The MME selects the S-GW with the current criteria, resolves S-GW IP with A/AAAA query, and then sends an APN FQDN to resolve the P-GW.

When the feature is enabled by setting `minFqdnLabelMatching` to `Yes` and the requested services are configured properly, the MME does not filter out P-GWs according to which services have been requested by the UE. Instead, the MME selects the SP-GW pair.

Following are the basic logic for the MME to select SP-GW pairs:

- For the first pass, the MME eliminates all FQDNs that do not meet the minimum label matching criteria. The MME selects the closest gateway that is the best service matching based on the service criteria.
- When the `minLabelMatchValue` parameter is set to `8`, it means that in the first pass analysis, the MME can include FQDNs with eight labels matching and FQDNs with nine labels matching.
- When the MME looks for the best service matching, and more than one FQDN matches the service needs, the MME uses label matching to select the closest one (where nine labels matched is better than eight labels matched).
- If no FQDN matches the full set of services, the MME works its way through the service hierarchy until it finds an FQDN that works. The MME finds an FQDN in the first pass if at least one FQDN matches the minimum label matching criteria.
- If the MME finds no FQDN that meets the minimum label matching criteria in the first pass, then the MME runs a second pass analysis without the minimum label matching. So essentially, the MME falls back to existing functionality for selection mode 1.
- The second pass reverts to standard MME behavior: the MME finds the best service matching, regardless how far that P-GW/SMF is.
- The only time that the MME gets to the second pass is when no P-GW/SMF FQDN meets the minimum label matching criteria.

The following combinations are used in P-GW requested services:

- `+nc-nr.smf + ue-<uut>`
- `+nc-nr.smf`
- `+nc-smf+ue<uut>`
- `+nc.smf`

Note:

The first pass means that in case the feature is enabled, the MME tries to select P-GW based on criteria described in the new logic (SP-GW FQDN label matching). If no P-GW matches the criteria in first pass, the MME falls back to the legacy logic. This fallback to the legacy logic of SP-GW selection is referred as the second pass.

The new logic of SP-GW selection is applicable only in selection mode 1.

5.1.13 MME support for steering option 3x subs to combo nodes for capacity offload - phase 3 (Feature f10004-03)

This feature supports configuration of FQDN label matching during SP-GW pair selection for the following service combinations: +nc-nr+ue, +ue, +nc-nr, and no modifiers. The MME supports specification for each service combination whether minimum label matching applies.

When the global parameter `serviceModifiersWithLabelMatching` is set to `Yes`, the MME uses label matching during the first pass, then filters S-GWs and P-GWs based on the service parameters as described in *Steering option 3x subs to combo nodes for capacity offload enhancement* (Feature f13034-01).

Parameters for the `fqdnLabelMatchProfile` CLI command support filtering candidate SP-GW pairs for specified combinations.

The following combinations for P-GW selection are supported, according to services UE requests:

- `+nc-nr+ue-<uut>`
- `+ue<uut>`
- `+nc-nr`
- no modifiers

Counters for the services supported by the selected P-GW are introduced and are incremented if the selection is executed in the first pass. Counters related to selection latency during the first pass are also introduced.

5.1.14 DNS query to obtain MME IP addresses enhancements (Feature f12207-01)

This feature introduces enhancement to the existing MME feature by supporting the reselection of another MME if the response from the target MME times out or the first choice per DNS records is unavailable. The reselection is performed only once.

5.1.15 MME support for improved table management for P-GW isolation/gwNodeAdmin (Feature f10166-03)

This feature changes the processing of SP-GW pairs and P-GW nodes in the `gwNodeAdmin` command when the command is filled.

Prior to this feature, when the size of the `gwNodeAdmin` command reached its maximum, P-GW nodes were purged and then re-built as SP-GW combinations were re-discovered. This resulted in different node names being assigned to SP-GW combinations, even to combinations that had been in the suspend state before the purge, making it more difficult for technicians to follow up with nodes that were having issues.

With this feature, P-GW nodes in the suspend state are not removed during a purge and their node names are preserved.

5.1.16 CMM support for configurable DNS timeout alarm (Feature f12115-02)

This feature enables the capability to delay the raise of `42014 CommunicationDegradationOrLost` alarm from the critical alarm threshold of IPDS unbound RTO time reach or exceed 10 seconds.

This feature introduces a configurable alarm sustained interval which controls the frequency at which the `42014 CommunicationDegradationOrLost` alarm is raised. The alarm sustained interval has a range from 0 to 120 minutes, with a default value of 0 minute. When the unbound round trip timeout (RTO) exceeds the critical threshold, the alarm is only raised when the critical threshold remains exceeded for the entire alarm sustained interval. When the default interval (0 minute) is set, this feature is disabled, and the raising of the alarm is unchanged. The conditions to clear the alarm remain unchanged by this feature.

5.2 APN management

Features for access point name (APN) management and provisioning.

5.2.1 MME support for APN wildcard (Feature m10100-03)

The **MME support for APN wildcard feature** provides a benefit of utilizing the wildcard access point name (APN) that allows a UE to access any unsubscribed APNs. When the wildcard APN is present in the subscription context, the UE is authorized to connect to APNs that are not present in the subscription context.

An APN is used as a reference point for an external PDN that supports the services to be accessed by a UE. The APN information is permanently distributed and maintained in the HSS, P-GW, and DNS. A set of APN labels is defined in the HSS. Each mobile user can subscribe to one or more APNs from this set. The labels of these subscribed APNs are then stored in the UE at subscription time. Among the subscribed APNs there is one default APN.

If a user attempts to access a service without specifying the APN, the default APN is used. Additionally, the HSS can also define a wildcard APN (*) that allows a UE to access any unsubscribed APNs. When the wildcard APN is present in the subscription context, the UE is authorized to connect to APNs that are not present in the subscription context. Default APN cannot be wildcard APN: it always contains an explicit APN. However, if there is more than 1 wildcard APN per UE, the MME should reject it.

5.2.2 Multiple APNs matching the wildcard APN (Feature m10100-07)

The **Multiple APNs matching the wildcard APN feature** removes the limitation of allowing PDN connection to only one APN for wildcard APN in UE subscription by allowing multiple PDN connections to multiple APNs matching the wildcard APN.

This feature provides provisioning of the maximum number of APNs allowed for the wildcard APN per PLMN basis. A UE subscription data may contain a wildcard APN if the HPLMN operator allows subscriber to access any APN. If MME has received such a wildcard APN, MME can allow an APN NI received from the UE even if the APN is not in the UE subscription.

5.2.3 Maximum 16 APNs per UE with engineering for 6 APNs per UE (Feature m10010-05)

The **Maximum 16 APNs per UE with engineering for 6 APNs per UE** feature removes the limitation of supporting only 6 access point names (APNs) that the MME can receive from the UE subscription profile.

This feature removes the limit of the maximum of 6 APNs that the MME can receive in the HSS UE subscription profile. The MME supports up to 16 APNs for any UE, and the total of 3 million APNs per CPPS.

If more than 16 APNs are received in the UE subscription data from the HSS, the MME saves the first 16 APNs in the UE context. The feature is based on the assumption that 30% of the subscribers' messages have up to 16 APNs per subscriber and the average of 6 APNs per subscriber at the maximum UE capacity.

For this feature to work, the HSS node must support the maximum number of APNs.

5.2.4 Wrong APN correction and default APN NI selection strategy (Feature m10137-01)

The **Wrong APN correction and default APN NI selection strategy** feature provides the benefit of correcting an incorrect access point name (APN) requested by UE instead of failing the attach procedure.

With implementation of this feature, if the UE has requested an APN not on the list of the subscribed APNs, in order not to fail an attach procedure, the MME uses the default APN from the list of subscribed APNs.

If this feature is enabled and if during an initial attach procedure the UE sends an APN, the MME checks the APN sent by the UE against the APNs listed in the subscription profile received from the HSS.

If the APN does not match one of the APNs listed in the subscription profile, the MME uses the default APN from the subscription profile.

This feature does not change or add requirements for the MME behavior for standalone packet data network (PDN) connectivity request scenarios. For the above scenario, even if the APN wildcard (*) is on the list of APNs in the subscription profile, the MME uses the default APN from the subscription profile.

5.2.5 Enhanced APN correction (Feature m10137-02)

The **Enhanced APN correction** feature provides various benefits to the base APN correction feature by supporting the access point name (APN) correction with multiple packet data network (PDN) connections. It also provides additional correction mechanisms.

The MME support for provisionable default for an APN correction is an enhancement to the *MME support for APN correction and default APN NI selection strategy* feature for homers. This feature introduces the following enhancements:

- The MME uses the default APN from the subscription data to do an APN correction if the UE-requested APN is incorrect or illegal. Illegal or invalid APN means that the APN is not according to 3GPP TS 23.003 format. Following are examples of an illegal/invalid APN:
 - A user requests the APN that does not follow 3GPP APN format.
 - A user requests the APN with .gprs in the beginning or the APN network identifier starts with any of the strings rac, lac, rnc or with *.
- When there is no ESM Information Transfer exchange during the initial attach or when there is an ESM Information Transfer exchange but the APN field is empty, the MME does the attach with the default APN (not APN correction scenarios).
- However, on a subsequent PDN connectivity request, or upon receipt of the PDN Connectivity Request message, the MME checks whether APN name is included.
 - If no requested APN is included in the PDN Connectivity Request message nor in the ESM Information Response message and the request type is other than emergency, the MME corrects to the default APN if the APN correction feature is enabled.
 - If the feature is not enabled, the MME rejects the PDN connection request.
- Support for APN correction with multiple PDN connections:
 - The MME supports an APN correction on the second PDN connection under the same APN as the first PDN connection.
 - In addition, an additional PDN should be handled when sending or receiving from another SGSN and MME.
 - The PDN type can be the same or different (IPv4, IPv6, IPv4v6).
 - If there are no PDN connections or the first PDN connection is on the same default APN, consequent PDN connection requests with invalid APN are corrected using the default APN.
 - If there are two PDN connections on the same default APN, consequent PDN connection requests with invalid APN are rejected.

The described functionality is applicable only to homers or treat-as-homer UEs.

For roamers, any illegal APN request is rejected with the ESM cause #33 (any unsubscribed APN found in the domain name system (DNS) database is honored if the UE has a wildcard APN subscribed).

- If the wildcard APN profile is populated in the subscription profile, it is ignored when the feature flag is turned on.
- Maximum number of APN corrections to be done is two, that is, two APNs for IPv4 and IPv6, which is four bearers.

This feature requires the *base APN correction* feature.

Related descriptions

- [APN correction \(Feature f10107-01\)](#)

5.2.6 MME support to send the UE-requested APN or the corrected APN (Feature m10107-04)

MME support to send the UE-requested APN or the corrected APN feature provides the benefit to control which APN-NI to send to the UE in the Activate Default EPS Bearer Request message.

The MME supports a global parameter `sendRequestedApn` to determine which APN-NI, the UE-requested or the corrected, to send to the UE in the Activate Default EPS Bearer Context Request message. By default, the corrected APN is sent to the UE.

The allowed values of this parameter are `Yes` and `No` (default). If the parameter is set to `Yes` means that the MME sends the UE-requested APN to the UE. If it is set to `No` means that the MME sends the corrected APN to the UE.

5.2.7 APN correction (Feature f10107-01)

The APN correction feature provides the benefit of correcting an incorrect access point (APN) name provided by the UE with a new network-provided APN instead of rejecting the APN.

With this feature, the MME supports APN correction by overriding the UE-provided APN with a new network-provided APN.

If the UE-provided APN is empty or not found from the APN configuration in the subscription data or not recognized by domain name system (DNS), the MME overrides the UE-provided

APN with a new network-provided APN. The network-provided APN can be either the MME-provisioned APN (M-APN) or the default APN provided by the HSS (H-APN).

MME can be configured for APN correction function to occur for Attach Request and Standalone PDN Connectivity Request on a per PLMN basis.

MME provisioned APN (M-APN) can be configured on a per PLMN basis.

UE may insert APN as part of a PDN Connectivity Request in an Attach Request or Standalone PDN Connectivity Request. UE may request to the MME to provide APN through the ESM information procedure, for either attach or standalone PDN connectivity request procedures. UE provided APN is used as follows:

- If it is found in subscriber's APN configuration subscription data.
- If it is not found in subscriber's APN configuration subscription data but wildcard APN exists in subscriber's APN configuration subscription data.
- Wildcard APN subscription is a special APN subscription with the following attributes:
 - Wildcard APN subscription allows a UE to access any unsubsribed APN.
 - If wildcard APN subscription exists and DNS lookup is successful, PDN establishment is setup to the UE provided APN.
 - If wildcard APN subscription exists and DNS lookup returns either "No such name" or "Name error", UE provided APN is replaced with default H-APN and second DNS lookup occurs using default H-APN.

UE-provided APN is replaced with M-APN for the following conditions:

- PLMN configuration data (UE PLMN services) indicates that procedure being processed (attach or standalone PDN connectivity request) is set to locally configured.
- provisioned default APN (M-APN) (UE PLMN services) is not empty.
- M-APN is found in subscriber's APN configuration data.
- UE-provided APN is empty and either M-APN or wildcard are found in subscriber's APN configuration data.
- UE-provided APN is not found in subscriber's APN configuration data, wildcard APN is not found in subscriber's APN configuration data and M-APN is found in subscriber's APN configuration subscription.
- UE-provided APN is not found in subscriber's APN configuration data, wildcard APN is found in subscriber's APN configuration subscription but DNS lookup using UE provided APN fails.

UE-provided APN is replaced with default H-APN for the following conditions:

- PLMN configuration data (UE PLMN services) indicates that procedure being processed (attach or standalone PDN connectivity request) is set to received from HSS.
- At least default APN exists in subscriber's APN configuration.

- UE-provided APN is empty.
- UE-provided APN is not found in subscriber's APN configuration subscription data and wildcard APN is not found in subscriber's APN configuration subscription.

This feature also introduces support by allowing multiple PDN connections to the same APN with the same PDN type. A maximum of 11 PDNs to the same APN is supported.

When this feature is enabled for Attach Request, Standalone PDN Connectivity Request or both, feature *MME support for Enhanced APN correction* (m10137-02) is considered disabled.

This feature and feature *Intelligent P-GW selection based on requested PDN type* (f10102-01) can both be enabled at the same time. DNS queries when both features are enabled follow this order:

- APNNI followed by “PDN-type-string” appended
- APNNI without “PDN-type-string” appended
- Corrected APNNI (M-APN or H-APN) followed by “PDN-type-string” appended
- Corrected APNNI (M-APN or H-APN) without “PDN-type-string” appended

5.2.8 APN correction configuration enhancements for IMSI ranges (Feature f10107-07)

APN correction configuration enhancements for IMSI ranges feature provides options for APN correction to be configured specific to the UE IMSI ranges level, in addition to the UE PLMN/serving PLMN pair.

The existing APN correction feature (f10107-01) provides the capability of specifying either the HSS default APN or a locally-configured APN as the APN for APN correction when the UE-provided APN is either missing or invalid. The APN correction feature provides the options `apnCorrectionAttach`, `apnCorrectionStandalone`, and `provisionedDefaultApn` in `uePlmnServices` for a UE PLMN or serving PLMN pair.

The APN correction configuration enhancements for IMSI ranges feature (f10107-07) enhances the configuration options to allow APN correction to be configured on an IMSI range basis. The parameters for this configuration are `apnCorrectionAttach` and `apnCorrectionStandalone` in the `imsiRangeServices` defined for the `uePlmnServices`. If both the `uePlmnServices` field is configured for APN correction and the `imsiRangeServices` field is enabled for APN correction for the `uePlmnServices`, the `imsiRangeServices` entry overrides the `uePlmnServices` entry.

Related descriptions

- APN correction (Feature f10107-01)

5.2.9 Enhancement to APN correction to accommodate maximum of 255 APNs (Feature f10107-08)

This feature enhances the **APN correction feature (Feature f10107-01)** by supporting the provisioning of up to 255 APNs.

The maximum number of the APN-NI profiles that can be provisioned is increased from 64 to 255.

5.2.10 CMM support for SGSN national APN database table (Feature f10160-01)

This feature introduces provisioning support for SGSN national APN table in the MME.

APN NI extension applies only to national APN.

The MME can be configured with national APN list that contains specified APN to the list of national APNs. Up to 31 APNs can be added to the list. The default value is null.

5.2.11 APN conversion and correction (Feature f10137-04)

The APN conversion and correction feature enables the operator to define different locally-provisioned APN-NIs per IMSI range.

This feature enables the operator to provision an APN-NI replacement for UE-requested APN-NI in PDN Connectivity Request when the list of subscribed APN-NIs includes the wildcard and does not include the UE-requested APN-NI. The replacement APN-NI will be used in NAPTR query for the P-GW selection. The provisioning is supported per IMSI series. This feature applies to homers, roamers and roamers treated as homers.

Related descriptions

- Autonomous local breakout for roamers (Feature f10165-01)

5.2.12 APN conversion and correction per IMSI series enhancements (Feature f10137-08)

This feature enhances the **APN conversion and correction feature (Feature f10137-04)** feature by introducing a global parameter to control when the MME will reject an unknown/unsubscribed/illegal APN during the attach or the PDN connectivity request procedure.

When the APN conversion and correction feature (Feature f10137-04) is enabled, the MME rejects it with a NAS ESM cause code #33 Requested service option not subscribed, upon receiving an unknown/unsubscribed/illegal APN, that is neither an HSS-provisioned APN nor locally-configured in the MME APN correction/replacement table.

configured MME APN correction/replacement table. Additionally, the MME uses the default APN from the HSS upon receiving an empty APN.

The feature is controlled via the `enhApnCorrectionPerImsi` global parameter. By default, the feature is disabled.

5.2.13 APN correction and conversion per IMSI/IMEI range (Feature f10116-02, f10116-04)

The **APN correction and conversion per IMSI/IMEI range feature enables the operator to replace invalid UE-provided APNs (where the UE provided APN is not in the HSS subscription or is not provided) with a configurable APN for specific IMSI/IMEI ranges.**

To solve practical network issues, for example, in case of bring your own (BYO) devices which have arbitrary APNs configured or specific behavior in how PDN connections are requested and for which purpose, a locally-provisioned APN NI table can be assigned to either PLMNs (MCC/MNC/IMSI ranges) or to IMEI ranges.

If the UE provides no APN or if the UE-provided APN is not in the HSS subscription list, the UE-requested APN NI will be matched against the IMSI/IMEI ranges/APN table and if match is found, it will be replaced with a locally-configured replacement APN NI, provided that the HSS subscription also includes the wildcard APN.

A UE-requested APN that is found in the HSS subscription list is used by the MME as it is. However, if the UE-requested APN is not found in the HSS subscription and is not found in the locally-provisioned IMSI/IMEI tables, the default APN from the HSS subscribed list is used as the replacement APN.

The table is configurable separately per subscriber PLMN and per defined IMSI/IMEI/TAC

range/list of ranges. There are a total of 64 configurable tables.

This feature applies to both homers and roamers for either gateway selection mode 1 or 2.

5.2.14 APN override with GW selection mode 1 enhancements (Feature f10116-06)

This feature enhances the *APN correction and conversion per IMSI/IMEI* feature by introducing a new field and global parameters to control the lookup of a locally provisioned APN NI per IMSI/IMEI range.

A new field, the `replacement_action`, is introduced in the existing IMSI/IMEI table to control the APN override when the feature is enabled and the UE requested APN-NI matches the data in IMSI/IMEI ranges of the APN table. The value of the field determines if the Attach/PDN Connectivity Request should be rejected or use the HSS provided default APN or use the configured APNs in the IMSI/IMEI ranges/APN table.

The MME is provisioned with global parameter `imsiImeiLookupFail` to either use the HSS provided default APN or reject the attach/PDN connection regardless of any provisioned APN in IMSI/IMEI table when the lookup fails. Additionally, the global parameter `anyUeRequestedApn` is used to control the APN override support for rogue APNs. It allows a match on 'any' UE requested APN. If this global parameter is enabled, it replaces the UE requested APN with the string 'any' for the search in the `apnImsiRangeServices` table.

5.2.15 APN override with GW selection mode 1 extensions (Feature f10116-09)

This feature enhances the existing *APN override with GW selection mode 1 enhancements (Feature f10116-06)* by introducing support for multiple PDN connections (dual bearers) for same APN (for example PDN connections with separate IPv4, IPv6 and IPv4v6 default bearers must be supported for the same APN name).

The feature works in parallel with APN correction. Additionally, it extends the current maximum number of APN corrections from two to unlimited.

5.2.16 APN correction and conversion per IMSI/IMEI range enhancements (Feature f10116-07)

This feature adds an enhancement for the APN correction and conversion per IMSI/IMEI range (f10116-02, f10116-04) feature per IMSI/IMEI range to ignore the existence of the wildcard APN if the APN correction occurs and a locally configured APN is found in the IMSI/IMEI table which is not in the HSS subscription data.

The APN correction and conversion per IMSI/IMEI range (f10116-02, f10116-04) feature allows the operator to replace invalid UE-provided APNs, where the UE provided APN is not in the HSS subscription or is not provided, with a locally provisioned APN for specific IMSI/IMEI ranges.

The UE-requested APN NI is matched against the IMSI/IMEI ranges/APN table entries `apnImsiRangeServices`. If a match is found, it is replaced with a locally-configured replacement APN NI, in which the HSS subscription also includes the wildcard APN. This feature allows the locally-configured replacement APN NI to be used even if the wildcard APN is not defined based on a global parameter. Two options are supported with global parameter:

- Use the locally-configured replacement APN and suppress the Notify Report Message
- Use the locally-configured replacement APN and use the default APN context ID in the Notify Report Message

5.2.17 MME support for APN rate control status (Feature f11701-22)

The APN Rate Control IE is exchanged between the UE and the P-GW/SCEF. When the last PDN of an APN is released, the P-GW or SCEF can forward the APN Rate Control Status IE to the MME. This feature enables the MME to store this IE and, upon the next PDN creation, deliver it to the S-GW or SCEF.

With this feature, when the last PDN of a given APN is released, the P-GW or SCEF can request the MME to store the most recent P-GW/SCEF APN Rate Control Status IE as part of the PDN release procedure. Then, when a new first-created PDN is established to the APN, and the feature is enabled, the MME relays the stored status, thus allowing the P-GW or SCEF to continue the proper rate control operation.

When the MME creates the first PDN of an APN, the MME deletes any stored APN Rate Control Status IE for that APN regardless of the feature flag. The MME is provisioned with the global parameter `apnRateControlStatus` to control whether this feature is active or

not. By default, the feature is disabled.

If the feature is enabled, all the following operations apply:

- The MME stores the APN Rate Control Status IE, if provided, in the last PDN release for the APN (from either the T6a or S11).
- The MME stores the APN Rate Control Status IE, if received, in the MM context from a peer MME (that is, in the S10 Context Response, Forward Relocation Request, and Identification Response messages).
- The MME provides the saved APN status, if available, to the applicable P-GW and/or SCEF for the first PDN of the APN creation.

 **Note:**

Regardless of the feature flag, the saved APN status is removed after the first successful PDN establishment.

The MME can include the APN Rate Control Status IEs in the MME context (that is, in the S10 Context Response, Forward Relocation Request, and Identity Response messages) regardless of the feature flag. In such a case, the peer MME ignores unknown IEs.

 **Note:**

The APN status may not exist in the VLR if the feature is disabled; for example, the operator deactivates the feature after the MME has stored the APN Rate Control Status IE. This handling allows more straightforward MME implementation.

5.3 Gateway selection

Features related to S-GW and P-GW selection.

5.3.1 S-GW and P-GW selection enhancements (Feature m10110-01)

The S-GW and P-GW selection enhancements feature supports optimal selection of S-GW on inter radio access technology (IRAT) handover based on UE packet data network (PDN) connections.

This feature provides an MME capability to select an S-GW topologically close to a P-GW at

attach and also whenever an S-GW is selected on X2 handover, S1 handover, tracking area update, and IRAT mobility. This feature provides the following provisioning options:

GW selection mode 1

Select a P-GW topologically close to an S-GW

The MME uses the current scheme of selecting the P-GW and S-GW, that is, first the S-GW is selected and then the P-GW for each PDN is selected geographically close to the S-GW as it is supported currently.

GW selection mode 2

Select an S-GW topologically close to a P-GW

The MME first selects the P-GW of default PDN (normally the P-GW of the first PDN connection at attach) and then the S-GW topologically close to the P-GW for attach and also whenever the S-GW relocation is required.

In the provisioning option Select S-GW topologically close to the selected P-GW, the MME uses the following requirements in selecting an S-GW and P-GW:

- At the initial attach or for a subsequent PDN connectivity request, the MME supporting IRAT mobility always selects a P-GW with collocated GGSN, that is, a P-GW supporting service types “x-gn” and “x-s5” or “x-s8”.
- If a P-GW with a collocated GGSN is not available, the MME selects a P-GW-only node and pegs a counter to keep track of the number of times a P-GW-only node is selected. If there are multiple P-GW straightforward name authority pointer (S-NAPTR) records, the MME uses the order and preference values to select a P-GW (this allows UE sessions to be distributed across multiple P-GWs based on their capacity).
- If PDN-GW-Allocation-Type AVP of UE subscription data is set to type Dynamic, the MME uses the access point name (APN) fully qualified domain name (FQDN) as defined in 3GPP TS 23.003 in the S-NAPTR procedure.
- If PDN-GW-Allocation-Type AVP of UE subscription data is set to type Static, the MME uses the P-GW FDQN if provided by the HSS as follows in the S-NAPTR procedure:
 - If the FQDN starts with topn/topoff, the MME strips the first two labels and uses the FQDN in the S-NAPTR procedure.
 - If the FQDN does not start with topn/topoff, the MME strips the first label and uses the FQDN in the S-NAPTR procedure.
 - If only IP address is provided, the MME uses the IP address with no further selection procedures.

At the initial attach, the collocation of the selected S-GW and the selected P-GW is the most important criteria. Therefore, the MME has to wait for both APN query response and tracking area identity (TAI) query response. Then, the MME starts the topology matching. Collocated

nodes are given the highest preference, that is, the S-GW and P-GW are collocated on the same node. Note that a topologically matched pair might not have the lowest preference or order field. If there are multiple matched pairs on the topology, the MME uses the preference and order fields to decide which matching pair should be used first. For any subsequent PDN connection requests, the MME selects a P-GW topologically close to the selected S-GW in the initial attach procedure. For tracking area update (TAU), X2 handover, S1 handover, and IRAT handover, if there is an S-GW relocation, the MME selects an S-GW as follows for the following scenarios:

- Intra-LTE mobility with or without MME relocation (TAU, X2 handover, and S1 handover): the MME identifies which P-GW is the first PDN gateway that was chosen during the initial attach procedure, if there are multiple P-GWs in the existing evolved packet system (EPS) bearer context records. The MME uses the old S-GW FQDN in the existing EPS bearer context to find a matching topologically closer P-GW in the existing EPS bearer context records. Then the MME uses that P-GW FDQN for the new S-GW selection based on the topology.
- IRAT TAU and handover where the old node is S4-SGSN: the S-GW selection is identical to the intra-LTE scenarios. The MME selects a P-GW of a PDN that is topologically closer to the old/target S-GW by topological matching of the FQDNs of S-GW (S-GW node name information element (IE) in S3 Context Response or Forward Relocation Request) and P-GW FDQNs provided in the P-GW node name of the MME/SGSN UE EPS PDN Connections IE in S3 Context Response or Forward Relocation Request message. The MME uses this FQDN of the P-GW for the topological matching to select the new/target S-GW that is topologically closer to the P-GW.
- In IRAT TAU and handover where old node is Gn-SGSN, the MME uses S-GW selection procedure based on the inclusion of the optional Co-located GGSN-PGW FQDN IE in Gn Context Response or Forward Relocation Request message.
 - If optional IE Co-located GGSN-PGW FQDN is included, the MME uses the first GGSN-PGW FQDN in the list for topological matching. The MME selects an S-GW that is topologically close to the P-GW that is first in the list provided in the Co-located GGSN-PGW IE.
 - If optional IE Co-located GGSN-PGW FQDN is not included, the following procedure is used to obtain P-GW FDQNs of packet data protocol (PDP) Context entry:
 - The MME uses the S-NAPTR procedure on the APNs of the first active PDP context provided in the PDP context IE.
 - The MME only selects a P-GW that supports collocated GGSN, that is, the P-GW must have NAPTR records supporting service type “x-gn” and “x-s5” or “x-s8”.
 - The MME gets A and AAAA records for the NAPTR entry supporting service type “x-gn”.
 - Out of these entries, the MME selects the entry that matches the IP address with

the GGSN Address for User Traffic of the PDP Context. If there is no IP address matching between the APN domain name system (DNS) response and the Gn IP address in the transferred PDP context, the MME ignores the matching IP address and selects the S-GW/P-GW the same way as in the initial attach procedure. Once the S-GW is selected based on the topology matching method used in the initial attach procedure, the original Gn IP address of the PDP context is sent in the Create Session Request message, instead of the selected P-GW IP address from the DNS query. This particular scenario can happen when the operator has configured the S-GW/(P-GW) pool using a load balancer, so that the DNS query returns the IP address of the load balancer and not the actual IP addresses of the gateway. However, when Gn-SGSN contacts the load balancer for the first time, the load balancer assigns an actual P-GW/GGSN for the PDP context. This actual P-GW/GGSN directly responds to the SGSN's first message and the SGSN puts this assigned P-GW/GGSN's IP address in the PDP context (not the load balancer's IP address).

- The FQDN of the entry is used to select an S-GW topologically close to the P-GW-GGSN.

5.3.2 Preference for an S-GW supporting S5 and S8 (Feature m10128-01)

The *Preference for an S-GW supporting S5 and S8 feature modifies the S-GW selection for a roaming UE to select an S-GW supporting S5 interface only if that is the only S-GW available when the UE is allowed local breakout.*

The S-GW and P-GW use S5 interface if both the nodes are visited network (VPLMN) and S8 interface is used if the P-GW is in the UE's home network (HPLMN).

Before this feature, the MME rejects UE attach or TAU request with the S-GW relocation if it cannot select a S-GW supporting both S5 and S8 interfaces for a roaming UE. This feature, for a roaming UE, always prefers the S-GW supporting both S5 and S8 interfaces as currently supported. But if name authority pointer (NAPTR) query only returns the S-GW supporting S5 interface and if the roaming UE is allowed to connect to the P-GW in VPLMN, then the MME selects the S-GW supporting S5 interface. Any subsequent packet data network (PDN) connection requests are rejected if local breakout is not allowed for the requested PDN.

Operators can save costs by allowing the roaming subscriber to use the P-GW in the local network as a connection point to other networks, for example, Internet.

5.3.3 Enhanced S-GW and P-GW isolation (Feature m10113-04)

The **Enhanced S-GW and P-GW isolation** feature enhances S-GW/P-GW selection for the selection mode 2 in the event a load balancer stops responding.

This feature is only applicable for the mode 2 selection of an S-GW and for both mode 1 and mode 2 selection of a P-GW.

The mode 2 selection is specifically developed to support a load balancer in front of S-GW/P-GWs.

When the MME uses domain name system (DNS) query for the S-GW selection, the MME receives IP addresses of the load balancers. So, the MME always sends a Create Session Request message to the load balancer. The load balancer selects an S-GW and forwards the Create Session Request to the S-GW. The S-GW includes its IP address when it responds with the Create Session Response to the MME.

The MME starts sending Echo Request to the IP addresses obtained from the Create Session Response to monitor the S11 path to the S-GW. However, the MME cannot monitor the load balancer as the load balancers do not support GTP echo. This feature provides the MME capability to determine that the load balancer cannot be used for a configurable period of time (the S-GW isolation timer).

The MME determines that a load balancer cannot be used as follows.

- The MME provides provisioning of a create session request time-out threshold and a duration.
- If the number of create session request time-outs crosses the provisioned threshold within the provisioned duration (the S-GW isolation declaration timer), the MME generates a major alarm and does not include the S-GW in the selection. The load balancer is not considered for the S-GW selection until the S-GW isolation timer expires or is manually enabled to be selected.
- If there is only one S-GW remaining, the MME does not suspend the S-GW.
- The MME generates a critical alarm and continues to use the S-GW.
- The MME provides a capability to manually suspend the last remaining S-GW.
- The MME also generates a critical alarm if the MME has not already generated a critical alarm when the last S-GW is manually suspended.

This feature represents S-GW load balancers for mode 2 selection as maintenance objects (MOs). The state of the MO representing an S-GW can be obtained using a command-line interface (CLI) command.

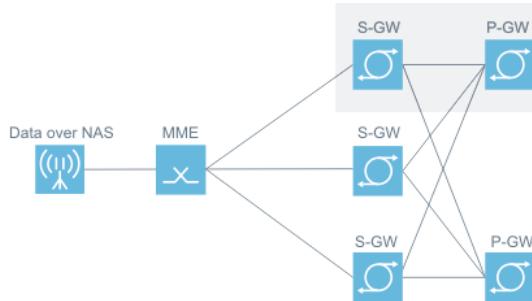
When the MME declares a gateway (GW) is isolated/denylisted, the node is suspended from the selection for a configurable period of time.

The MME provides CLI commands to manually suspend a MO representing an S-GW from the selection and also provides an ability to manually resume selecting a suspended S-GW MO. The collocated MME and SGSN monitor and isolate S-GWs independently.

This feature supports a similar capability for the determination that an S-GW and P-GW pair cannot be used because of P-GW faults.

- The MME provides provisioning of a create session request failure because the remote peer is not responding to a threshold and duration.
- If the number of create session request failures crosses the provisioned threshold within the provisioned duration (the S-GW and P-GW isolation declaration timer), the MME generates an event and does not select the pair for a configurable period of time (the S-GW and P-GW pair isolation timer). The pair is not considered for the selection until the isolation timer expires or is manually enabled to be selected.
- The figure shows the isolation of S-GW and P-GW for create session failures because of the P-GW. In the figure, the S-GW 1 can report the number of Remote peer not responding exceeding the configured threshold whenever the P-GW 1 is selected. This result in not selecting the P-GW 1 whenever the S-GW 1 is selected for mode 1 selection and selecting an S-GW and P-GW pair for mode 2 selection is based on the selection of the topologically closer S-GW and P-GW pair.

Figure 42: Isolation of S-GW and P-GW for create session failures because of P-GW



Note:

The S-GW 1 can still be selected in combination of other P-GWs and also the P-GW 1 can still be selected in combination of with the other S-GWs.

This feature represents an S-GW and P-GW pair for mode 1 and mode 2 selection that has been used at least once as MO. These MO states can be obtained using a CLI command. When the MME declares that a pair is isolated/denylisted, the node is suspended from the

selection for a configurable period of time. The MME provides CLI commands to manually suspend a MO representing an S-GW and P-GW pair from selection and also provides an ability to manually resume selecting a suspended GW MO. The collocated MME and SGSN monitor and isolate the pair independently.

This feature supports a new type of MO, Node, to support the following:

- The MME generates events if it determines to suspend an S-GW load balancer or an S-GW and P-GW pair from selection.
- The MME provides CLI commands to do the following:
 - Manually suspend a node MO. A suspended MO is excluded from the node selection until it is manually enabled to be selected.
 - Manually resume node selection of a suspended node.
 - Obtain node status.

This feature only support MOs for the S-GW and P-GW.

This feature provides the following provisioning:

- Separate parameters to enable the P-GW isolation on the MME and SGSN
- Separate parameters to enable the S-GW isolation on the MME and SGSN
- P-GW isolation declaration timer (default 3 seconds)
- P-GW fault threshold (default 50)
- P-GW isolation duration (default 15 minutes)
- Separate parameters to enable the S-GW isolation on the MME and SGSN
- S-GW isolation declaration timer (default 3 seconds)
- S-GW fault threshold (default 50)
- S-GW isolation duration (default 15 minutes)

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

5.3.4 Provisionable depth of retry for S-GW/P-GW reselection (Feature m10113-06)

The *Provisionable depth of retry for S-GW/P-GW reselection* feature improves user experience by allowing more time to set up the UE bearer before declaring an S-GW failure and rejecting the UE request.

This feature enhances the MME S-GW/P-GW reselection capability.

As defined (for mode 1 selection), the MME generally makes the original Create Session Request attempt and one additional attempt and rejects a subsequent Create Session Requests after the UE is attached.

With the implementation of this feature, and when the feature is enabled through provisioning, the MME makes the original Create Session Request attempt, and up to two additional attempts (if needed) before rejection of subsequent Create Session Requests after the UE is attached.

Before the implementation of this feature, the MME supported the S-GW and P-GW reselection as follows: When a failure cause is received from a Create Session Response or the MME times out waiting for a Create Session Response, criteria for the S-GW or P-GW reselection are based on the failure cause value and failure source in the Create Session Response. Field experience indicates that generally, timers of the S-GW are provisioned to smaller values than timers of the P-GW. Thus, the MME timed out waiting for a Create Session Response is treated as an S-GW failure (as if no response from the S-GW). When the S-GW times out waiting for Create Session Response from the P-GW, the S-GW reports it as a Peer not Responding (cause code 100) failure.

With the implementation of this feature:

- A global provisioning parameter is introduced.
- When the global provisioning parameter is set to value 2, the MME sequentially makes up to two additional tries at selection of an S-GW/P-GW for all of the failure scenarios.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

5.3.5 Additional S-GW and P-GW selection enhancements (Feature m10110-01)

The *Additional S-GW and P-GW selection enhancements* feature supports selection of S-GW and P-GW that is compliant with 3GPP TS 29.303 specifications in selecting first collocated S-GW and P-GW nodes and secondly topologically closest nodes.

This feature adds a provisioned option in the MME to select an S-GW topologically close to the P-GW on top of the existing functionality of selection of P-GW topologically close to S-GW. This feature adds new S-GW and P-GW selection logic in the following procedures:

- Initial attach procedure: the MME obtains S-GW name authority pointer (NAPTR) result and P-GW NAPTR result, and chooses a P-GW first based on order and preference. The

MME only considers P-GWs with collocated P-GW/GGSN (x-gn) when choosing the P-GW, unless no P-GW has x-gn interface. The MME then chooses a collocated S-GW with P-GW, if possible. If no collocation is found, the MME chooses the topologically closest S-GW and P-GW by matching S-GW and P-GW fully qualified domain name (FDQN).

- Initial attach and packet data network (PDN) connectivity request procedures: the MME always tries to choose a P-GW with a collocated GGSN.
- Intra-LTE S-GW relocation: the MME uses an old S-GW FQDN to find a topologically closer P-GW in the existing evolved packet system (EPS) bearer context, and uses that P-GW FDQN for searching a new collocated or the topologically closest S-GW.
- Inter-RAT S-GW relocation where an old node is S4-SGSN and an old S-GW is in the MME's network: the MME uses old S-GW FQDN to find a topologically closer P-GW in the existing EPS bearer context and uses that P-GW FDQN for searching a new collocated or the topologically closest S-GW.
- Inter-RAT S-GW relocation where an old node is S4-SGSN and an old S-GW is not in the MME's network: the MME uses the first P-GW in the existing EPS bearer context to find a topologically closer S-GW.
- Inter-RAT S-GW relocation where an old node is Gn-SGSN: the MME picks access point name (APN) from the first active packet data protocol (PDP) context for P-GW NAPTR query, and builds a candidate list of P-GWs that support x-gn and x-s5 or x-s8. The MME then obtains A and AAAA records for each P-GW (one by one) from the candidate P-GW list and matches the IP from the P-GW IP responses with the Gn IP in the transferred PDP context to select a P-GW. The MME then uses the P-GW FDQN with matched IP address to select a new S-GW topologically. If no P-GW with matching Gn IP address is found for the first APN from the PDP context, the MME selects S-GW or P-GW or both the same way as in the attach procedure.

5.3.6 Topological label matching for S8 P-GW selection (Feature m10136-01)

The *Topological label matching for S8 P-GW selection* feature helps in selecting P-GW closer to the S-GW in visited network (VPMLN) for certain operator deployments.

This feature provides the MME capability to do topological matching for home routed (S8) P-GW selection. The global parameter `topologicalLabelMatchingForS8pgwSelection` controls whether topological matching is used to select an S8 P-GW for home routed scenarios. By default, this parameter is disabled. If it is enabled, the MME does topological matching of the S8 P-GW with the S-GW when selecting a P-GW for home routed scenarios. This parameter is only valid for gateway (GW) selection mode 1, and has no effect on P-GW

selection if GW selection mode 2 is enabled.

There is a dependency to the *Mode 1 selection of GWs* feature.

Related descriptions

- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

5.3.7 P-GW reselection on no response from S-GW (Feature m10112-06)

The *P-GW reselection on no response from S-GW* feature reduces session failures because of P-GW failures by selecting an alternate P-GW.

This feature provides a capability on the MME to handle no response from S-GW as a possible P-GW failure and follow the P-GW reselection logic identical to the case where it receives a CSR with failure cause code 100 (P-GW not responding). This feature can be enabled through provisioning. If the feature is disabled, no response from the S-GW is treated as an S-GW failure.

This feature has a dependency to the *Selectable S-GW and P-GW re-selection methods due to S-GW/P-GW failures* feature.

Related descriptions

- [Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures \(Feature m10113-01, m10113-02\)](#)

5.3.8 Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures (Feature m10113-01, m10113-02)

The *Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures* feature provides fewer procedure failures and lower average latency for processing S11-based procedures because of a failed or non-responding S-GW/P-GW.

This feature adds S-GW and P-GW re-selection capabilities to the MME when a failure cause is received from a Create Session Response or the MME times out while waiting for a Create Session Response.

Criteria for S-GW or P-GW re-selection are based on the failure cause value and failure source in the Create Session Response.

Field experience indicates that generally timers of the S-GW are provisioned to lower values than timers of the P-GW. Thus, the MME that has timed out while waiting for a Create Session Response is treated as an S-GW failure (as if no response from S-GW).

When an S-GW times out while waiting for Create Session Response from the P-GW, the S-GW reports it as a Peer Not Responding (cause code 100) failure.

Related descriptions

- [Alternate GW reselection \(Feature f10125-02\)](#)

5.3.9 Partial label matching on TAC query (Feature m10113-03)

The *Partial label matching on TAC query feature co-locates a S-GW and P-GW if canonical node names match exactly after specified criteria are applied.*

The MME considers a S-GW and P-GW to be co-located if canonical node names match exactly after the following criteria are applied:

- If fully qualified domain name (FQDN) starts with topn/topoff, the first two labels are stripped from FQDN.
- If FQDN does not start with topn/topoff, the first label is stripped from FQDN.

After these criteria are applied, if the S-GW and P-GW canonical node names contain the same number of labels and they match exactly, the S-GW and P-GW are considered to be co-located. When doing topological matching, the MME selects an S-GW and P-GW pair with the longest canonical node name label match, starting from the right. The topological selection is solely determined by the number of labels matched starting from the right, regardless of the number of the total labels in the S-GW FQDN.

This feature complies with topological matching algorithm specified in 3GPP TS 29.303.

5.3.10 Extending Gn S-GW selection for additional scenarios (Feature m30113-04)

The *Extending Gn S-GW selection for additional scenarios feature provides an S-GW selection for Gn tracking area update (TAU) for all S-GW relocation scenarios: intra-MME, inter-MME, and S4-SGSN. It reduces unnecessary network signaling load.*

This feature extends S-GW selection for Gn TAU for all S-GW relocation scenarios, that is,

intra-MME, inter-MME, and S4-SGSN relocation. If there is more than one active packet data protocol (PDP) context, the new MME first picks a P-GW supporting access point names (APNs) in the following order:

1. SOS
2. If there is no active SOS, IP multimedia subsystem (IMS) is picked.
3. If there is no active SOS nor IMS, the first APN in the list is picked.

The selected P-GW is used to select an S-GW by topological matching.

Additionally, this feature prefers the selection of S-GW with S5 service for roammers with local breakout packet data network (PDN) connections for intra-LTE mobility and mobility from S4-SGSN and Gn-SGSN. This feature only applies to mode 2 selection of S-GW and P-GW.

5.3.11 Selection of an S-GW with x-s8-gtp only service (Feature m30113-02)

The *Selection of an S-GW with x-s8-gtp only service* feature allows operators to deploy S-GW supporting the S8 interface only.

This feature addresses an issue with roaming where a local breakout (LBO) is enabled and configured and S8 between the S-GW and P-GW is used. Before the implementation of this feature the MME uses S5 service for all of the S-GW candidates. With implementation of this feature, in addition to S5, S8 is also a valid service. This is especially important for a roamer who uses its own home network P-GW when using a local breakout. More precisely, this feature supports the selection of an S-GW with x-s8-gtp only service.

This feature is dependent on the *Mode 2 selection of GWs* feature.

Related descriptions

- S-GW and P-GW selection enhancements (Feature m10110-01)
- Local breakout enhancements (Feature m10128-02)

5.3.12 Intelligent P-GW selection based on requested PDN type (Feature f10102-01)

The *Intelligent P-GW selection based on requested PDN type* feature allows P-GW selection based on packet data network (PDN) types supported by P-GWs.

During P-GW selection, the initial DNS query for obtaining the NAPTR is performed by

composing an FQDN from the access point names (APN). If there is a need to assign specific P-GWs to a specific group of subscribers based on the PDN type, an operator can configure supplemental information for each PDN type that will be appended to the APN network identifier (APN-NI) used in the FQDN. The MME supports IPv4, IPv6, and dual stack (IPv4v6) PDN types.

If supplemental information is configured for a PDN type, the MME must append that configured information to the APN-NI FQDN that is sent to the DNS. The DNS server will then return a different P-GW IP addresses for different PDN types (a NAPTR record is obtained from the DNS).

This feature is applicable only to the home PLMN and treat-as-home subscribers.

By default, all PDN type entries are empty and the MME does not append any PDN type information to the APN-NI used in FQDN.

Caveats

For roaming subscribers, MME does not use any information on PDN type, even if the feature is configured.

The MME does not append any PDN type information to the APN used in FQDN that the MME sends to the DNS server in the following procedures:

- Emergency attach
- Emergency PDN connectivity
- Handover attach
- PDN connectivity with request type equaled to 'handover'
- Roaming
- Attach and UE requested PDN connectivity in case the HSS provides the P-GW FQDN. In this case MME sends this FQDN to the DNS server as a query for obtaining the NAPTR record, and determine the P-GW IP address and the protocol.
- Attach and UE requested PDN connectivity in case the HSS provides the IP address, either with or without APN OI/NI or FQDN of the P-GW

Feature interactions

The PDN type is appended only after APN correction has been applied.

This feature must be disabled if the feature *MME support for APN NI extension with configurable length of MSISDN digits* is in use.

Related alarm

When an APN DNS query is done using a provisioned supplemental string and the DNS query response has no records, the MME reports a minor alarm.

```
+++ 2016/06/01 17:50:34.386 CRAFT_MAINT HIGH ACTIVE maf:4948 E:5052 S:1499
(MmeDnsAlarm.cpp 272 X-0:9:0 36.04.26.0000:1464821135 fnsman 10.220.161.0)

ERROR:MME-2:ALARM Data[1]: text=[NAPTR-Query]:
fqdn=[wap2.verizon.com.IPV4.SUPP.apn.epc.mnc012.mcc310.3gppnetwork.org]:
protocol=[s5/s8]: reason=[PGW APN FQDN Response failure]
```

Related descriptions

- [Node selection](#)
- [Intelligent roamer P-GW selection based on requested PDN type \(Feature f10102-04\)](#)

5.3.13 S-GW/P-GW selection based on IMSI/MSISDN range (Feature f10110-01)

S-GW/P-GW selection based on IMSI/MSISDN range feature supports local provisioning for S-GW/P-GW without using DNS.

For S-GW selection, area list mapped to TAI list needs to be defined. If the area list is not defined for the range, all TAIs will be allowed. For P-GW selection, an APN list needs to be defined. This feature also provides an option to utilize the locally provisioned S-GW/P-GW when DNS server is not available or DNS selection fails.

IMSI and MSISDN ranges configuration option is only applicable for home subscribers. A maximum of 64 IMSI ranges or MSISDN ranges can be configured.

When this feature is enabled and at least one S-GW/P-GW record is configured for a IMSI/MSISDN range, MME checks whether the UE's IMSI/MSISDN matches with any of the configured IMSI/MSISDN range(s) for the following procedures:

- incoming attach procedure
- PDN connectivity procedure
- MME mobility procedures

If a match is found, MME attempts to select a S-GW based on current TAI mapping from a pool of S-GWs. The S-GW pool is applicable for attach, PDN connection, and MME mobility

procedures.

MME also attempts to select a P-GW based on current APN mapping from a pool of P-GWs. The P-GW pool is applicable for attach and PDN connectivity (standalone and first) procedures.

In case of multiple S/P-GWs the MME randomly picks one of the candidates.

If the MME fails to select the S-GW/P-GW from the pool, the MME attempts to select the S-GW/P-GW by DNS query, when S-GW selection with straightforward name authority pointer (SNAPTR) and P-GW selection with SNAPTR features are enabled.

In addition, the MME attempts to select a S-GW/P-GW by DNS query, if the MME finds:

- the selected gateway link is down.
- the selected gateway is overload.
- the selected gateway is not supporting CP-CIOT while the UE is supporting CP-CIOT.

If the DNS query fails, or S-GW selection with SNAPTR and P-GW selection with SNAPTR features are disabled, the MME attempts to select the S-GW/P-GW from local provisioning again.

If the MME fails to select a S-GW/P-GW after all the steps mentioned above, the incoming procedure must be rejected as there is no S-GW/P-GW available to establish sessions. In this case, alarm `40874 LSS_gwSelectionUsingImsiMsisdnRangeFailed` is raised.

The feature requires activation through global parameter `locallyProvisionedSgwPgw` in addition to local GW provisioning.

There are also two global parameters, `sgwSelectionWithSnaptr` and `pgwSelectionWithSnaptr`, to enable resolving GW IP using DNS if static selection fails.

Note:

- Only 3 S-GWs and 3 P-GWs can be locally provisioned.
- Remote S11 GTP-C IP address used in CMM provisioning (the statically configured S-GW address) must differ from the dynamically configured S-GW address (the one returned by a DNS lookup).

Figure 43: S-GW selection based on IMSI/MSISDN range

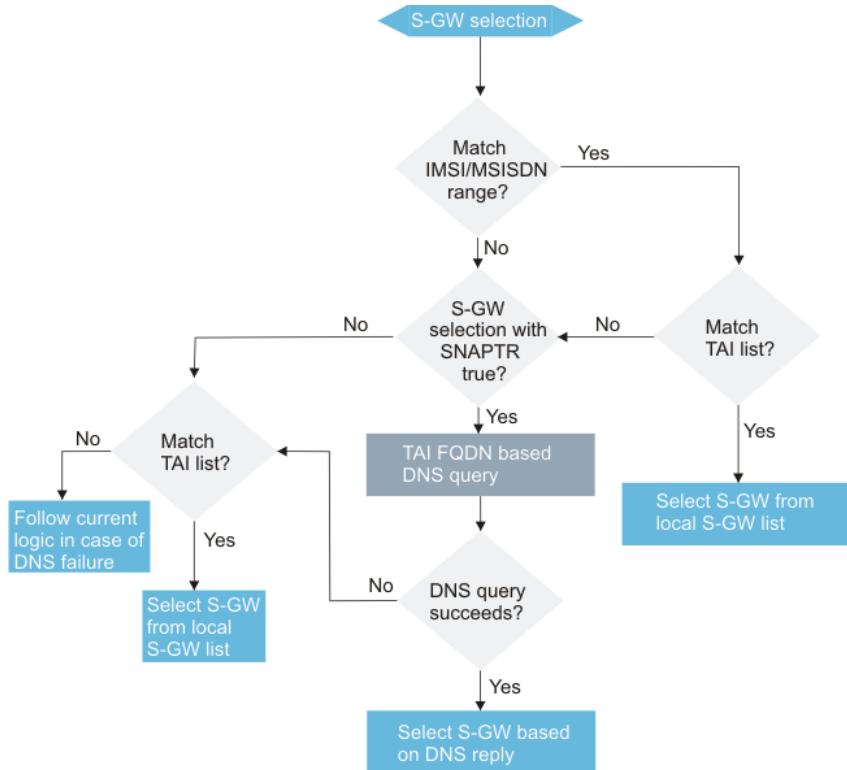
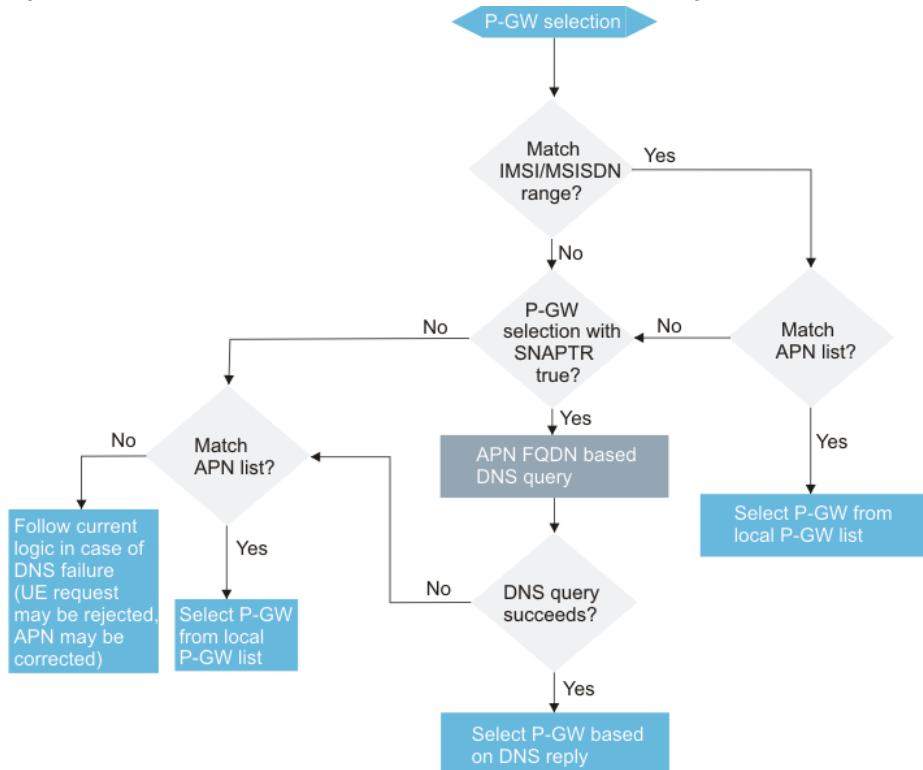


Figure 44: P-GW selection based on IMSI/MSISDN range



5.3.14 P-GW selection based on charging characteristics (Feature f10106-01)

The **P-GW selection based on charging characteristics** feature makes it possible to assign dedicated P-GW to support different kind of traffic. For example, postpaid and prepaid users can be served by different P-GWs.

With this feature, operator is able to configure the bits of the charging characteristics to be utilized for P-GW selection. The MME can recognize charging characteristic parameter which is inserted by the HSS to the MME via S6a interface.

The MME supports 2 bytes CC via S6a.

 **Note:**

The HSS Charging Characteristic is a part of subscription information and has altogether 16 bits. For this solution, the MME appends configured bits of charging characteristics, starting from bit 0, to the APN-NI used to perform the P-GW selection. The operator is able to configure CC bits (or ccLength) to be used to select the P-GW for specific UE PLMN/serving PLMN pair and optionally also for only specific APN(s).

The MME supports standard CC values (4 Bits) as well as rest of Bits within 2 bytes with specific behavior defined on a per-Operator basis.

The feature is considered to be activated when a table is provisioned for UE PLMN/serving PLMN pair. The configured table in a PLMN defines length of CC to be used for P-GW selection for each APN.

- Default configuration on the table exists if a default entry on the table has been added.
- Default entry applies to all APNs unless a specific APN-NI entry matching the APN exists on the table.
- Each specific APN that may be added to the table may include length of CC to be used for P-GW selection.
- Entries in the table that do not specify length CC will use length of CC assigned to default entry.

The APN that is used for P-GW selection based on CC is the same APN that the MME selected for PDN establishment.

Example: CC bits used in P-GW selection

As an example, the first 4 bits of the CC (B0, B1, B2 and B3) can be used in the PGW selection. Operators can define these bits to indicate the following:

Figure 45: CC bits in P-GW selection

Octets	Bits							
	7	6	5	4	3	2	1	0
1	B7	B6	B5	B4	B3	B2	B1	B0
2	B15	B14	B13	B12	B11	B10	B9	B8

- B3 bit set to 1 indicates normal/postpaid charging - represented as string 1000
- B2 bit set to 1 indicates prepaid charging - represented as string 0100
- B1 bit set to 1 indicates flat rate charging - represented as string 0010
- B0 bit set to 1 indicates hot billing charging - represented as string 0001

Examples of how APN FQDNs are structured

P-GW selection based on CC is not enabled:

- mobile.internet.apn.epc.mnc260.mcc310.3gppnetwork.org

P-GW selection based on CC is enabled:

- mobile.internet.1000.apn.epc.mnc260.mcc310.3gppnetwork.org: String 1000 (normal charging) is inserted, assuming that first 4 CC bits assigned to mobile.internet APN are 1000.
- fast-internet.0100.apn.epc.mnc260.mcc310.3gppnetwork.org: String 0100 (prepaid charging) is inserted, assuming that first 4 CC bits assigned to fast.internet APN are 0100.

Interactions of P-GW selection based on CC with other features

P-GW selection based on MSISDN and P-GW selection based on CC are both enabled:

MSISDN based selection has priority

P-GW selection based on PDN type and P-GW selection based on CC are both enabled: CC

based selection has priority

APN correction function and P-GW selection based on CC are both enabled: APN that MME uses for P-GW selection based on CC may be the APN result of feature APN correction function.

5.3.15 Mode 2 enhanced S-GW selection for IRAT TAU (Feature f10125-01)

This feature supports using IP match to determine a P-GW in S-GW selection. The feature ensures that a S-GW selected in Gn relocation is collocated or topologically close to P-GW of active PDN sessions.

If the *Mode 2 enhanced S-GW selection for IRAT TAU* feature is activated, MME's S-GW selection scheme on IRAT mobility consists of selecting a S-GW close to the P-GW of active PDN sessions received in Gn Context Response or Forward Relocation Request.

If there are multiple PDP contexts in Gn Context Response or Gn Forward Relocation Request, the new MME first chooses a PDP context. The following cases define the MME behavior:

- If the IMS APN exists and APN-OI matches MME's home network, the new MME picks this PDP context.
- If the phone APN exists and APN-OI matches the serving PLMN, the new MME picks this PDP context.
- If the broadband APN exists and APN OI matches the serving network PLMN ID, the new MME picks this PDP context.
- If there are no IMS, phone and broadband APNs in the PDP context within the serving network, the new MME selects the first PDP context in the list of PDP contexts received. The APN OI of the APN of the selected PDP context matches the serving network PLMN ID.

Once the PDP context is selected, the MME carries out reverse mapping to find the P-GW FQDN associated with IPv4/Ipv6 address of the P-GW in the selected PDP context. The FQDN is used to find S-GW topologically close to the P-GW. If MME fails to resolve IP address to a P-GW FQDN, it ignores the IP address matching and selects the S-GW/P-GW as in the initial attach procedure, that is, the MME launches a NAPTR query with APN of the selected PDP context and selects a P-GW supporting both Gn and S5 topologically close to the S-GW.

The reverse lookup consists of searching the CPPS DNS cache or using APN query for P-GWs supporting the IP address, or both. First, the MME searches the CPPS DNS cache. If the IP is

not found in the cache, the MME launches an APN NAPTR query to obtain all candidate P-GWs that support Gn and S5/S8 interfaces and their IP addresses. If IP address resolves to multiple P-GWs, the MME uses all these P-GWs to find the best topologically close S-GW and P-GW. The selection of P-GW supporting Gn and S5 and/or S8 interface takes place as currently specified.

By default, the feature is activated.

Related descriptions

- [MME support to obtain P-GW FQDN for SGSN to MME relocation \(Feature f10125-03\)](#)

5.3.16 Alternate GW reselection (Feature f10125-02)

The **Alternate GW selection feature provides the capability through provisioning to select alternate GW based on the cause received in Create Session Response message instead of checking the source bit of the cause IE. The feature only applies to mode 2 selection of GWs.**

In GW selection mode 2, the MME selects the S-GW/P-GW simultaneously, based on topological matching of each S-GW returned from the TAC NAPTR query and each P-GW returned from P-GW/APN NAPTR query plus any associated NAPTR “” and NAPTR “s” query response, irrespective of S-GW and P-GW Order and Preference values. However, in case multiple S-GW/P-GW pairs have the same topological closeness, the MME will select on S-GW order and preference.

If the *Alternate GW selection* feature is enabled, MME's behavior for reselection of S-GW or P-GW is solely based on the cause value received in the Create Session Response message. MME does not check the source bit of the Cause IE in the reselection.

By default, the feature is disabled.

When the global parameter `supportAlternateGwReselection` is set to `Yes` (the feature is enabled), MME's behavior is based on the received cause value as follows:

Table 46: S-GW and P-GW reselection in attach procedure

Cause value of Create Session Response	MME actions
100 (Remote peer not responding)	MME selects an alternate P-GW as currently supported for mode 2 GW selection.
73 (No resources available)	MME selects an alternate S-GW and P-GW pair as currently supported for mode 2 GW selection.
94 (Request rejected (reason not specified))	MME selects an alternate S-GW and P-GW pair as currently supported for mode 2 GW selection.
All other cause values	MME rejects the attach request.

Table 47: P-GW reselection in standalone PDN connectivity request

Cause value of Create Session Response	MME actions
100 (Remote peer not responding)	MME selects an alternate P-GW as currently supported for mode 2 GW selection.
73 (No resources available)	
94 (Request rejected (reason not specified))	
All other cause values	MME rejects the PDN connectivity request with an appropriate NAS cause code.

Table 48: P-GW reselection in standalone PDN connectivity request with Request Type Handover

Cause value of Create Session Response	MME actions
All cause values	MME rejects the PDN connectivity request with an appropriate NAS cause code.

Table 49: S-GW selection during intra-LTE handover, inter-RAT handover and intra-LTE and inter-RAT idle mobility

Cause value of Create Session Response	MME actions
100 (Remote peer not responding) 73 (No resources available) 94 (Request rejected (reason not specified))	MME selects an alternate S-GW as currently supported for mode 2 GW selection.
All other cause values	MME fails the procedure.

Related descriptions

- Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures (Feature m10113-01, m10113-02)

5.3.17 S-GW relocation on modify bearer request failures (Feature f10148-02)

The *S-GW relocation on modify bearer request failures* feature supports S-GW relocation when the modify bearer request procedure fails due to timeout for all the PDN connections of a UE. This feature only supports the capability for service request procedure.

In service request procedure, if the S-GW does not respond to the Modify Bearer Request or Modify Access Bearer Request message, the MME relocates the UE to another S-GW. The MME does not set up radio bearers after S-GW relocation. The old S-GW request is dropped during or after the relocation.

This feature is only valid for UE-initiated service request and S-GW-initiated service request procedures triggered by the Downlink Notification message, Idle mode create bearer request and update bearer request procedures. TAU procedure is not included.

This feature is applicable to both mode 1 and mode 2 GW selection.

This feature is disabled by default and can be enabled using global parameter `sgwRelocationOnMbrFailure`.

This feature can only be activated when the global parameter `detachUponSrMbrTimeout` is set to `No`.

5.3.18 Restricting S-GW relocation (Feature f10166-01)

With this feature, the S-GW relocation is restricted for tracking area update request, X2 handover, S1 handover and MME relocation procedures.

This feature can be enabled and disabled via provisioning and only applies to GW selection mode 2. This feature is not applicable for S3 and Gn based inter-RAT handover and TAU. Even when the feature is enabled, S3 and Gn based HO and TAU still perform the S-GW relocation.

With this feature, the operator is able to restrict S-GW relocation procedures and deploy collocated S-GW and P-GW. When this feature is enabled, S-GW selection is only performed in the attach procedure and the UE is not relocated to any new S-GW afterwards.

This feature and feature *MME support for enhanced S-GW restoration procedure (m10538-08)* should not be enabled at the same time.

 **Note:**

If GW restoration is enabled, the S-GW relocation may still be performed for restoration triggering events.

Related descriptions

- [Enhanced S-GW restoration procedure \(Feature m10538-08\)](#)

5.3.19 Optional P-GW ID determination for statically allocated P-GW (Feature f10132-01)

This feature supports using the MIP6 Agent IP address instead of the MIP6 Agent FQDN to determine P-GW identity when both the IP address and FQDN are present in subscription data for a statically allocated P-GW.

MME can be provisioned with global parameter `preferredPgwid`. When it is enabled (`Yes`), MME uses MIPv6 Agent IP address instead of MIP6 Agent FQDN in order to determine P-GW identity. When it is disabled (`No`), MME will use the FQDN when both the IP address and FQDN are present. This feature is by default disabled.

5.3.20 Intelligent roamer P-GW selection based on requested PDN type (Feature f10102-04)

With this feature, the MME supports P-GW selection based on requested PDN type so an operator can select different P-GWs to serve different PDN types for roamer local breakout (LBO) PDN connections.

This feature extends the capability of feature *Intelligent P-GW selection based on requested PDN type (f10102-01)* to roamer LBO PDN connections.

Related descriptions

- [Intelligent P-GW selection based on requested PDN type \(Feature f10102-01\)](#)

5.3.21 Sending P-GW IP in NOR (Feature f10169-01)

The *Sending P-GW IP in NOR* feature provides new (non-standard) options for the S6a interface to provide the selected P-GW information towards the HSS in different formats.

The 3GPP standard based format (FQDN only, if available) is problematic in some environments. The P-GW IP address is required to be directly provided.

The feature provides possibility to utilize the IP address of the P-GW directly in non-3GPP mobility as the ePDG may not have access to DNS (to resolve a P-GW FQDN).

Global parameter `selectedPgwFormat` controls how the MME formulates the selected P-GW information inside the MIP6-Agent-Info AVP, which the MME sends on the S6a NOR and the S6a ULR (Active-APN AVP(s)).

The feature provides three provisioning options for the MME to send the HSS either

- only the P-GW IP addresses
- P-GW IP addresses and additionally the P-GW FQDN, when available
- only P-GW FQDN when it is available in the MME, otherwise only the P-GW IP addresses, which is the standard option.

Global parameter `pgwAddrOnS6aAndPgwFinding` has two purposes for VoLTE - VoWiFi handovers, for example: it controls

- which received P-GW IP addresses the MME uses when the MME sends the selected P-GW information inside the MIP6-Agent-Info AVP on the S6a NOR and the S6a ULR (Active-APN AVP(s)).
- how the MME finds the P-GW for the PDN when the MME receives Attach Request or PDN Connectivity Request with Request type Handover and establishes the PDN with Create

Session Request.

5.3.22 MME support to obtain P-GW FQDN for SGSN to MME relocation (Feature f10125-03)

This feature supports the capability to obtain P-GW FQDN by reverse DNS look up if P-GW FQDN is not provided by SGSN in Context Response message when a UE moves from SGSN to MME.

This feature uses the reverse look up supported by feature *Mode 2 enhanced S-GW selection for IRAT TAU (f10125-01)* and the feature capability is only enabled if f10125-01 is enabled. This feature, during IRAT mobility, makes use of reverse lookup to determine P-GW FQDN associated with the IPv4/IPv6 address of the P-GW.

This feature enhances feature f10125-01 which only obtains P-GW FQDN of a single selected PDP context to support selection of S-GW but does not send the P-GW FQDN to the target/new MME. For intra-LTE mobility with MME relocation, the source/old MME must send the P-GW FQDN used for P-GW/S-GW selection to the target/new MME.

This feature only applies to GW selection mode 2.

Related descriptions

- Mode 2 enhanced S-GW selection for IRAT TAU (Feature f10125-01)

5.3.23 MME support for enhanced alternate S-GW/P-GW reselection and isolation (Feature f10125-04)

This feature enhances the S-GW and P-GW reselection and isolation. Additional error codes returned from the S-GW/P-GW are considered to reselect and/or isolate the S-GW/P-GW according to the returned cause source.

This feature requires that the following previous features are also enabled:

- Selectable S-GW and P-GW reselection methods due to S-GW/P-GW failures (Feature m10113-01, m10113-02)
- Enhanced S-GW and P-GW isolation (Feature m10113-04)
- Alternate GW reselection (Feature f10125-02)

In both S-GW and P-GW reselections, the MME allows number of reselections similarly to the legacy features. If the number of reselections exceeds the limit set by legacy functionality,

the MME returns an error to the UE. The MME only reselects P-GW if the request type on NAS PDN Connectivity Request message is not Handover or handover of emergency bearer services.

The MME reselects another S-GW if global parameters `supportAlternateGwReselection` and `enhancedAlternateGwReselection` are set to yes, if the following cause values are received in Create Session Response message and the CS flag is set to 0:

- #72 System failure
- #91 No memory available

The MME reselects another P-GW if global parameters `supportAlternateGwReselection` and `enhancedAlternateGwReselection` are set to yes, if the following cause values are received in Create Session Response message and the CS flag is set to 1:

- #72 System failure
- #78 Missing or unknown APN
- #84 All dynamic addresses are occupied
- #91 No memory available

MME proceeds with the P-GW reselection in case that the cause value cause #100 Remote peer not responding is received in the Create Session Response message and the CS flag is set to 0.

Isolation functionality follows previous principles: When the total number of the P-GW-related or S-GW-related errors received exceeds the isolation threshold during the threshold declaration timer, the MME isolates the P-GW until the isolation duration timer expires. The MME cancels/ends the P-GW isolation.

The MME isolates the S-GW when the following cause values are received in the Create Session Response message and the CS flag is set to 0:

- #73 No resources available
- #91 No memory available

The MME isolates the P-GW when the following cause values are received in the Create Session Response message and the CS flag is set to 1:

- #73 No resources available
- #91 No memory available

5.3.24 Restricting S-GW relocation enhancements (Feature f10166-02)

This feature enhances feature **Restricting S-GW relocation (f10166-01)** by introducing new flag `sgwRelocationAllow` in UEPLMN services table which overrides the existing global parameter `sgwRelocationRestriction` for TAU procedures.

5.3.25 MSISDN number based home GGSN/P-GW selection enhancement (Feature f10176-01)

This feature allows selection of home GGSN/P-GW based on MSISDN and introduces a new list of APNs.

If the UE's APN is not in the new APN list for the MME, the MME falls back to the behavior of feature *MME support for APN NI extension with configurable length of MSISDN digits* (*m10121-03*).

If the UE's APN is in the new APN list for the MME, the MME decides whether to insert MSISDN digits in the string used for the APN DNS query depending on charging characteristics bit 15:

- When charging characteristics bit 15 is 0, the selected MSISDN digits are inserted.
- When charging characteristics bit 15 is 1, the MSISDN digits are not inserted.

For the MME provisioning, APN list can be defined with command `hpGwCcApnList`, and APNNI names are configured with command `hpGwCcApn` for a given APN list.

5.3.26 MME support for enhanced NR S-GW/P-GW selection after 3G to 4G IRAT idle mode TAU (Feature f10185-01)

This feature supports enhanced NR S-GW/P-GW selection after 3G to 4G IRAT idle mode TAU.

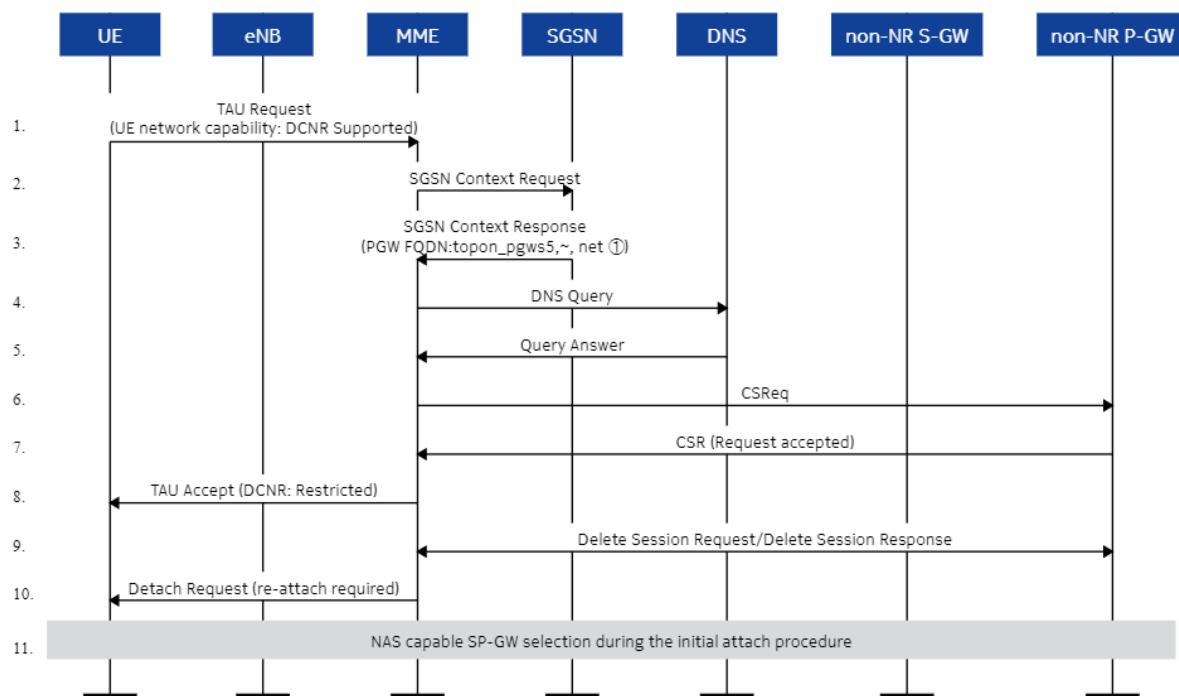
The MME sends a Detach Request message to the UE with detach type equal to re-attach required and optionally EMM cause set to Implicitly Detached, during IRAT TAU in idle/active mode from Gn-SGSN to MME, when the feature is activated and any of the following conditions is met:

- The S-GW/P-GW FQDN (+nc-nr) list included in the DNS response does not include all P-GW FQDNs (co-located P-GW FQDN list) that were previously received in the SGSN Context Response message.
- There is no DCNR capability either for S-GW or P-GW entry in the list of the DNS response for at least one matching P-GW FQDN that was received in the SGSN Context Response message.
- The SGSN Context Response message does not carry complete list of Co-located P-GW FQDN IEs for all associated PDP IEs.
- The DNS response in the P-GW FQDN NAPTR query contains no records or the actual DNS query times out.

This feature applies only to gateway selection mode 2.

Steps in the handover procedure:

Figure 46: 3G to 4G IRAT handover SP-GW reselection for NSA capable UE



- A 5G UE attaches to the core network via 3G network. It is assumed that non-NR P-GW/GGSN is selected here.
- The 5G UE moves from 3G to LTE/NR and TAU (UE capability: DCNR Supported) is triggered.
- The MME receives SGSN Context Response (P-GW FQDN=XXX).
- The DNS procedure is triggered for S-GW/P-GW selection.
- The MME receives S-GW/P-GW FQDN entries that has NR capable S-GW/P-GW "+nc-nr" flag.

- If P-GW FQDN entries list does not include current P-GW FQDN=XXX with +nc-nr support or the SGW entries list does not support +nc-nr, following detach procedure is initiated to reselect NR S-GW/P-GW.
- To complete IRAT TAU, the MME sends CSReq to current P-GW/GGSN and replies with TAU Accept. The DCNR setting in the TAU accept is set based on parameter `accRestNrAllowGwNotNrCapable` of `enhancedDualConnectivityProfile`.
- Detach procedure is initiated by the MME with detach type = re-attach required and optionally includes ESM cause code = Implicit detached.

5.3.27 MME support for using topological label matching for GW selection (Feature f10125-05)

The feature enables the MME to always perform topological matching when selecting GWs by using GW selection mode 2.

The `useTopologicalLabelMatchingAlways` global parameter controls whether topological matching is used to select S-GW and P-GW, regardless of whether S-GW/P-GW FQDN MNC/MCC identifies a PLMN (such as UE PLMN, serving PLMN, MME home PLMN, and so on) during attach request procedures and to select a P-GW during PDN connectivity request procedures.

This feature is effective for all homer scenarios (including with shared network), for all roamer scenarios (including both home routed and local break out), and for treat roamer as homer scenarios. Additionally, topological matching for S-GW/P-GW in another network applies to S-GW selection during S-GW relocation scenarios.

By default, this parameter is disabled.

This parameter is only valid for GW selection mode 2 and has no effect if GW selection mode 1 is enabled.

5.3.28 MME support for GW selection considering more than two IP addresses per FQDN (Feature f10191-01)

This feature supports the option of as many as two or eight IPv4 and IPv6 addresses per P-GW FQDN for P-GW selection in inter radio access technology (IRAT) mobility to ensure the selection of collocated S-GW/P-GW, when the DNS allows the configuration and the P-GW FQDN Information Element is not present in SGSN Context Response received from the source SGSN.

5.3.29 MME support for enhanced S-GW selection for roammers for GW selection mode 1 (Feature f10190-01)

For GW selection mode 1, when this feature is enabled by setting the global parameter

`sgwSelForHomeRoutedGwSelMode` to Yes and the UE is a home-routed roamer, the s8-gtp order and preference for each of the S-GW candidates are used to determine which S-GW to select instead of the order and preference for s5-gtp. The selection of an S-GW supports only s8-gtp and s5-gtp is not supported.

For GW selection mode 1, prior to this feature:

- When there are multiple valid S-GW candidates that have operational S11 links and these S-GW candidates are not overloaded, the order received in the s5-gtp DNS NAPTR answer is used to determine which S-GW to select.
- When there are multiple S-GW candidates with the same s5-gtp order, the s5-gtp preference values are used to determine how load balancing is performed among them.
- The S-GW selection logic is the same for both homers and roammers. The s11 and s8-gtp order and preference values are not considered.

5.3.30 MME support for roamer co-located GW selection (Feature f10110-08)

With this feature, the search for co-located GWs for UEs is supported when the served PLMN does not match the P-GW FQDN PLMN for GW selection mode 2.

5.3.31 MME support for locally configured S-GW/P-GW selection based on IMSI/MSISDN range for inbound roammers (Feature f12208-02)

This feature supports the selection of the locally configured S-GW/P-GW for the inbound roammers based on IMSI/MSISDN range plus APN. This feature builds upon S-GW/P-GW selection based on IMSI/MSISDN range (Feature f10110-01) for home subscribers only.

A new parameter `combinedSmfPgwc` of the command `pgw` is introduced to support the N26 interworking.

5.3.32 MME support for statically configured S-GW/P-GW selection with Topon option for roamers based on IMSI/MSISDN range plus APN (Feature f12208-01)

This feature supports statically configured S-GW/P-GW selection for the inbound roammers based on the IMSI/MSISDN range plus the APN with the option to support TOPON topological label matching for both the home subscribers and the inbound roammers.

If this feature is enabled with global parameter `locallyProvisionedSgwPgwtTopon`, the MME uses collocation or topological closeness for the S-GW/P-GW selection, when:

- selecting the S-GW/P-GW from the statically configured list,
- or, either the S-GW/P-GW or both are selected via the DNS, because no match is found in the statically configured list.

End to end scenarios supported

If both the S-GW and the P-GW are from range selection:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for the topological closeness.
- When no topological closeness is available, then select the S-GW and the P-GW with lowest entry ID.

If the S-GW is from the DNS, and the P-GW is from the range selection:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW based on the NAPTR order and select the P-GW with lowest entry ID.

If the S-GW is from the range selection, and the P-GW is from the DNS:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW based on the entry ID order and select the P-GW based on the NAPTR order.

If both the S-GW and the P-GW are from the DNS, then based on the GW SEL Mode 1 or 2,

current MME behavior is retained.

If the S-GW is from the range selection, and the P-GW is from the locally provisioned S-GW/P-GW:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW based on entry ID order and select the P-GW with the first entry.

If the S-GW is from the locally provisioned S-GW/P-GW and the P-GW is from the range selection:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW with the first entry and select the P-GW based on the entry ID order.

If the S-GW is from the DNS and the P-GW is from the locally provisioned S-GW/P-GW:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW based on the NAPTR order, and select the P-GW with the first entry.

If the S-GW is from the locally provisioned S-GW/P-GW and the P-GW is from DNS:

- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select the S-GW with the first entry and select the P-GW based on the NAPTR order.

If both the S-GW and the P-GW are from locally provisioned S-GW/P-GW:

- When the range selection and the DNS selection are both failed, then the S-GW/P-GW are selected from the locally provisioned S-GW/P-GW.
- When the collocated GWs are available, then select the S-GW/P-GW pair.
- When no collocated GWs are available, then check for topological closeness, and select the topologically closer GWs.
- When no topological closeness is available, then select 1st the S-GW entry and NAPTR

order the P-GW will get selected.

5.3.33 MME support for handling nc-smf tagged service type for non-N1-mode UEs (Feature f20003-15)

This feature enables the MME to select the P-GW candidates which do not have the nc-smf service type for non-N1-mode UEs.

When the feature is enabled by setting the global parameter

`pgwSelectionWithNonNcSmf` to `Yes`, the MME prefers P-GWs which do not have the nc-smf tagged service type for non-N1-mode UEs. Non-N1-mode devices prefer P-GWs which do not offer the nc-smf service. However, The nc-smf P-GW selection is allowed if it is the only available option.

5.3.34 MME support for sending P-GW FQDN in EPS to 5GS mobility (Feature f10125-09)

This feature introduces enhancements to resolve the P-GW FQDN of 5G-capable PDNs and ensure service continuity in EPS to 5GS mobility.

The P-GW FQDN may not be available during 5GS interworking at the source MME even if the associated PDN was established at the same MME. When this feature is enabled via a global parameter, it ensures that the MME always propagates the P-GW FQDN to the AMF during mobility procedures if it is properly provisioned in the DNS.

When this feature is enabled, during 4G to 5G idle mode mobility or handover, the MME checks if the VLR contains the P-GW FQDN for all 5G-capable PDNs before sending a Context Response or a Forward Relocation Request message to the AMF. If there is a missing P-GW FQDN for a 5G-capable PDN, the MME attempts to resolve the missing P-GW FQDN by using a reverse lookup.

First, the MME checks if the P-GW IP is stored in the DNS cache. If the IP address of the P-GW-C is stored in the VLR and can be resolved from the DNS cache, the MME updates the VLR with the resolved P-GW FQDN for this PDN, which is then available when a Context Response or a Forward Relocation Request is built.

If the IP address of P-GW-C is stored in the VLR and cannot be resolved by the DNS cache, the MME triggers a NAPTR request against the DNS with the APN FQDN for each PDN. If there are “s” records or “empty flag” records in the NAPTR response, the MME triggers an

SRV Request or a NAPTR request to resolve the “empty flag” records.

When all P-GW FQDNs are available, the MME triggers A/AAAA DNS requests with the P-GW FQDN to retrieve their IP addresses, depending on the P-GW-C IP address that is stored in the VLR. The MME locally stores only the P-GW FQDN for which the IP address received from the DNS matches with the IP address that is stored in the VLR. Then, the MME filters the P-GWs according to the requested services.

For the P-GWs that fulfill the requested services, the MME first selects the P-GW FQDN by matching the label with the S-GW (if the S-GW FQDN has the Topon option), then according to order preference. The MME also selects the P-GW FQDN in consideration of priority and weight in case that P-GW FQDN from the "s" NAPTR record has been selected.

5.3.35 CMM support for configuration control for restriction of P-GW selection to colocated GGSN/P-GW during IRAT mobility (Feature f10172-01)

This feature provides configuration control over the P-GW selection for mode 2 during the inter-RAT mobility procedure. A global parameter is introduced to either require or not require the candidate P-GWs for the inter-RAT mobility procedure to support the GGSN and P-GW capabilities.

In a Gn TAU or handover scenario with a target MME, the MME requires from the P-GW, retrieved by the DNS, to support the Gn service for home subscribers and the Gp service for roamer. If the MME fails to find such a P-GW, it rejects the TAU or the Handover Request message.

When the feature is enabled, the restriction for the Gp service for roamer and the Gn service for homers is removed. A P-GW that supports only S5/S8 interfaces is accepted.

The feature is controlled through the global parameter

`pgwSelectionRestrictedToColocatedGgsnPgw`. By default, the feature is disabled.

5.4 Node selection for emergency services

Features enabling gateway selection for IMS emergency services.

5.4.1 Enhanced P-GW selection for emergency PDN (Feature m10123-01)

The **Enhanced P-GW selection for emergency PDN feature provides flexibility to select a P-GW supporting emergency service either by fully qualified domain name (FQDN), access point name (APN) NI, or static IP address.**

This feature supports reselection of an emergency P-GW for mode 2 of the S-GW and P-GW selection if the P-GW fails to create an emergency session. The MME attempts to support two additional P-GWs if the selected P-GW fails to set up an emergency session in the following order if static address, P-GW FDQN, and emergency APN are provisioned:

1. First attempt: the MME always uses the static IP address if provisioned in the emergency profile.
2. Second attempt: the MME uses the P-GW FDQN if provisioned in the emergency profile.
3. Third and final attempt: the MME uses the straightforward name authority pointer (S-NAPTR) procedure on the emergency APN, if provisioned in the emergency profile, to select a P-GW with an FQDN different from the failed FQDN. If the first attempt is using emergency APN, the MME attempts to select up to two additional P-GWs from the candidate list obtained using the S-NAPTR procedure. The MME S-GW NAPTR selection procedures for an emergency attach request are identical to a non-emergency attach procedure.

Operators can choose one of the two options. The term selection option is used to indicate which of the following two combination options is used by the MME in selecting a P-GW for the emergency bearer:

- Emergency P-GW FDQN and APN
- Emergency P-GW static IP address (IPv4 or IPv6), FQDN and APN NI.

The MME attempts reselection of an emergency P-GW for the following cause values received in a response to the Create Session Response:

- Remote peer is not responding (cause value 100)
- No resources available (cause value 73) if the cause source is a P-GW
- Request rejected (cause value 94) if the cause source is a P-GW

For all other cause values, the MME simply rejects the attach request with provisionable non-access stratum (NAS) evolved packet system session management/evolved packet system mobility management (ESM/EMM) cause codes. The MME rejects a standalone packet data network (PDN) connectivity request with ESM cause code #38 (Network failure). The MME also attempts reselection of an emergency P-GW for the following conditions:

- If there is no response to any of the maximum number of Create Session Request transmissions.
- Domain name system (DNS) server failed to provide A or AAAA record.

There is a dependency to the *IMS emergency services* feature.

Related descriptions

- [IMS emergency services \(Feature m10106-01\)](#)

5.4.2 Mode 1 P-GW node selection using E911 APN NI (Feature m10123-02)

The *Mode 1 P-GW node selection using E911 APN NI* feature provides flexibility in the selection of P-GW supporting IP multimedia subsystem (IMS) emergency services.

This feature supports use of E911 access point name (APN) NI for the selection of P-GW for emergency attach and packet data network (PDN) connection request to E911.

The MME uses straightforward name authority pointer (S-NAPTR) procedure to select a P-GW. In case of an emergency attach, the MME selects a P-GW using topological matching if there are multiple S-NAPTR records. The MME also supports reselection of the S-GW or P-GW or both based on the Create Session Request failure and source of the failure. If the S-NAPTR domain name system (DNS) query fails, the MME uses the provisioned static IP address.

If the feature is enabled, the MME uses the S-NAPTR procedure in the selection of the E911 P-GW using the provisioned APN NI. In an emergency attach, the MME selects a P-GW using topological matching if there are multiple S-NAPTR P-GW resource records (RRs).

The MME uses the provisioned static IP address of the emergency P-GW if the DNS server fails to return a response to S-NAPTR query for the E911 APN NI.

This feature is dependent on the *IMS emergency services* feature.

Related descriptions

- [IMS emergency services \(Feature m10106-01\)](#)
- [S-GW and P-GW selection enhancements \(Feature m10110-01\)](#)
- [Local breakout enhancements \(Feature m10128-02\)](#)

5.4.3 Selecting P-GW for emergency sessions based on requested PDN type (Feature f11010-01)

The feature allows an operator to assign a specific emergency P-GW to a specific group of subscribers based on the PDN type requested by the UE in the emergency PDN connection request.

This capability is achieved by using provisioned tagging for a PDN type in the provisioned emergency APN when MME launches NAPTR query to select a P-GW.

This feature provides provisioning capability to activate the feature per MME and capability to provision tag to be used for UE requested PDN types IPv4, IPv6 and IPv4Ipv6. This feature applies to all types subscribers (for example, home subscribers, roamers, SIMless UE) allowed to access emergency session.

By default, the feature is deactivated.

This feature does not change or alter how emergency P-GW selection is performed for GW selection mode 1 or 2. Rather, it alters the contents of the APN FQDN DNS query, when such a query is issued from the CMM.

5.5 SGSN selection

Features for DNS-based SGSN discovery.

5.5.1 DNS SGSN discovery query method based on provisioning SGSN (Feature m10103-08)

The DNS SGSN discovery query method based on provisioning SGSN feature supports smooth domain name system (DNS) server migration to support Release 8 name authority pointer (NAPTR) queries by providing a selection of pre-Release 8 DNS procedures or Release 8 NAPTR procedures.

This feature supports provisioning option to use pre-Rel 8 SGSN fully qualified domain names (FQDNs) or Rel 8 straightforward name authority pointer (S-NAPTR) procedures to discover SGSN. Additionally, this feature provides provisioning option to specify length of the network resource identifier (NRI) in number of bits in packet temporary mobile subscriber identity (P-TMSI) so that the MME can extract the correct number of NRI bits. If pre-Rel 8 SGSN FQDN provisioning option is selected, the MME only uses the Gn interface and the following FQDNs as specified in 3GPP TS 23.003 Annex C for discovering SGSN:

- 2G handover: racAAA.lacBBB.mncYYY.mccZZZ.gprs
- 3G handover: rncXXX.mncYYY.mccZZZ.gprs
- tracking area update (TAU) and attach: nriCCCC.racDDDD.lacEEEE.mncYYY.mccZZZ.gprs. If NRI query fails, the MME falls back to use the RAI query.

The MME uses these FQDNs to get A and AAAA records.

If Rel 8 S-NAPTR provisioning is selected, the MME constructs FQDNs as specified in 3GPP TS 23.003 and runs the S-NAPTR procedures as specified in 3GPP TS 29.303. The MME uses the following FQDNs for SGSN discovery:

- The MME gives preference to S3 SGSN if SGSN supports both "x-s3" and "x-gn" service types.
- In handover, the MME uses the following logical names:
 - UTRAN if RNC ID is available (Target ID information element (IE) in S1 Handover Required message):


```
rncc<RNC>.rnc.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```
 - GERAN/UTRAN if only CGI is available (Target ID IE in S1 Handover Required message):


```
rac<RAC>.lac<LAC>.rac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```
- In attach and TAU if there is a need to contact old SGSN: `nri-`
`sgsn<NRI>.rac<RAC>.lac<LAC>.rac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`. If NRI query fails, the MME falls back to use the RAI query directly.

5.5.2 DNS fallback for SGSN call scenarios (Feature m10125-01)

The *DNS fallback for SGSN call scenarios* feature supports smooth domain name system (DNS) server migration to support fallback to pre- Release 8 queries if DNS server has not provisioned DNS records to support name authority pointer (NAPTR) queries.

This feature supports the option of DNS query fallback to a pre-Rel 8 query upon failing the Gn-SGSN selection via the default Rel 8 NAPTR query selection mechanism.

If a Rel 8 DNS query for the SGSN selection fails (no S3/Gn records in the response), the MME falls back to pre-Rel 8 DNS query.

If MME is provisioned to use straightforward name authority pointer (S-NAPTR) for SGSN selection and the DNS NAPTR query fails to return any related DNS records, the MME tries another DNS query using a pre-Rel 8 fully qualified domain name (FQDN) for the SGSN.

This is to cover cases where customer does not want to update all SGSN records to NAPTR

but wants some SGSNs to use NAPTR and others to use pre-Rel 8. The current network resource identifier (NRI) to RAC fallback cases still apply. The MME falls back only to pre-Rel 8 FQDN if no records are returned in the NAPTR query for SGSN S3/Gn. It is assumed that the customer enters NAPTR records that they want to be used and there is a need to fix the DNS entries for IP addresses related to the NAPTR records.

5.5.3 Fallback to GTPv1 support (Feature m10119-02)

The *Fallback to GTPv1 support feature supports switching to GTPv1 when a target node only supports GTPv1*.

This feature supports the MME fallback to GTPv1 support when the MME receives the cause code Fallback to GTPv1 in a GTPv2 Context Response message over the S3 interface.

When a UE has activated a packet data protocol (PDP) context through S4 SGSN to a GGSN and a tracking area update (TAU) procedure is underway, the old S4 SGSN includes the cause code Fallback to GTPV1 to force the MME to do inter radio access technology (IRAT) TAU procedure as specified in 3GPP TS 23.401 Annex D. The MME aborts the ongoing GTPv2 procedure and sends GTPv1 SGSN Context Request messages to the old S4 SGSN over the Gn interface. The SGSN DNS query response contains S3 and Gn interface records. The MME saves the Gn interface record and uses the record to obtain Gn interface IP address if Fallback to GTPv1 interface cause code is received. If a generic number (GN) interface record is not received, the MME rejects the TAU resulting in the UE to reattach.

5.5.4 DNS fallback enhancements from Rel 8 DNS query to pre-Rel 8 DNS query (Feature m10133-01)

The *DNS fallback enhancements from Rel 8 DNS query to pre-Rel 8 DNS query feature enhances domain name system (DNS) fallback. It reduces unnecessary network signaling load.*

This feature enhances DNS fallback as follows:

- The MME uses the Gn interface if Rel 8 DNS query fails when doing Rel 8 network resource identifier-routing area identity fully qualified domain name (NRI-RAI FQDN) query, that is, if the S3 interface hostname query fails, the MME uses the Gn interface to continue the processing of the query. However, if the name authority pointer (NAPTR) query succeeds but fails to obtain a valid IP address, the MME does not do a fallback but issues an alarm instead.
- The MME, after having done Rel 8 NRI-RAI FQDN, does Rel 8 RAI FQDN next and if the DNS

responds including both S3 interface and Gn interface, the MME prefers the S3 interface and starts with the S3 interface list. If the current chosen S3 interface hostname query fails, the MME works its way down the list to choose another one until the S3 list is exhausted, and then the MME works down the Gn list. If none of the hostnames yields any record, then the MME falls back to the pre-Rel 8 NRI query.

- If the DNS responds including only the S3 interfaces and the current chosen S3 hostname query fails, the MME works down the list to choose another one until the S3 list is exhausted. If the S3 list is exhausted, the MME falls back to the pre-Rel 8 NRI query.
- If the DNS responds including only the Gn interface list and the current chosen Gn interface hostname query fails, the MME works down the list to choose another one until the Gn list is exhausted. If the Gn list is exhausted, the MME falls back to the pre-Rel 8 NRI query.
- The MME uses DNS service to query Rel 8 RNCid FQDN that is used for the packet switching (PS) handover case to find out the target SGSNs.

5.5.5 MME support for 4-digit legacy MNC-MCC DNS query to find Gn-SGSN (Feature f12202-01)

The feature supports an optional legacy 3GPP R99 4-digit MNC/MCC in routing area identity (RAI) and RNCID fully qualified domain name (FQDN) DNS queries for Gn-SGSNs in inter-system mobility procedures.

The MME supports 4-digit MNC/MCC in RAI and RNCID FQDN DNS queries by padding a zero (0) at the beginning of MNC/MCC for Gn-SGSN inter-system procedures including:

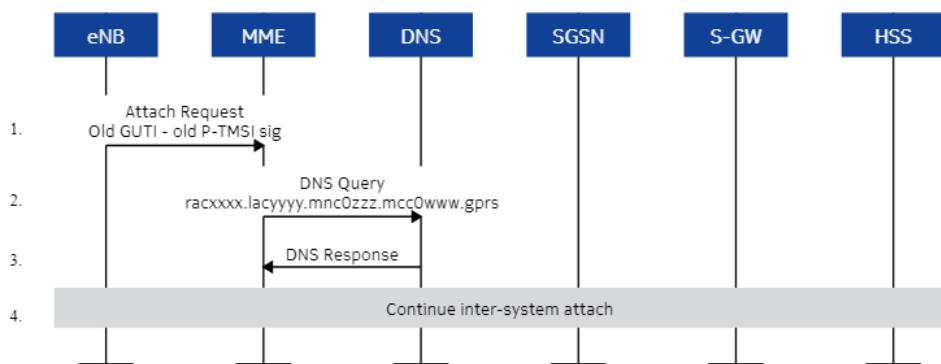
- inter-system attach
- inter-system tracking area update (TAU)
- (Gn-based) inter-system handover from 4G to 3G
- inter-system RAN information management (RIM) (E-UTRAN to UTRAN/GERAN)

To enable the feature, set the global parameter `fourDigitMncMccSuppt` to `ON`. When the parameter is set to `OFF`, 3-digit MNC/MCC RAI and RNCID FQDN DNS queries remain unchanged.

This feature affects only pre-Rel8 type DNS queries. If 4-digit MNC/MCC query fails, the MME falls back to 3-digit MNC/MCC query.

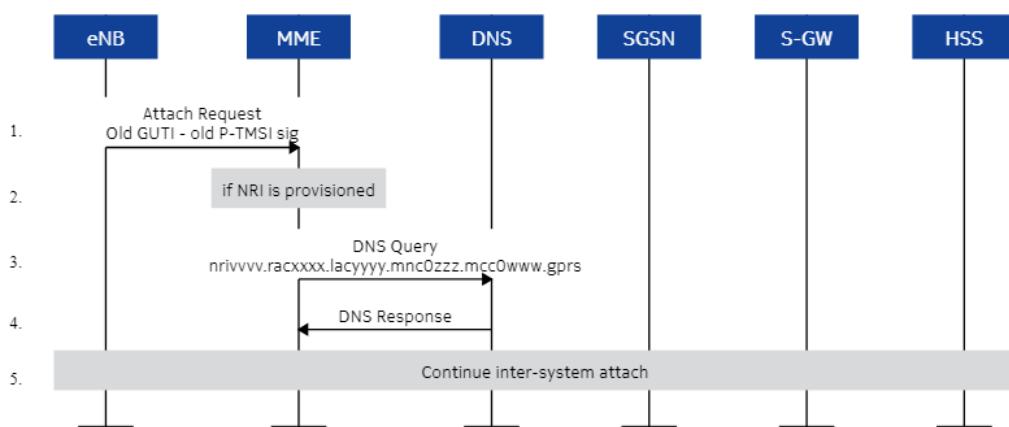
Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query is shown as follows:

Figure 47: Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query



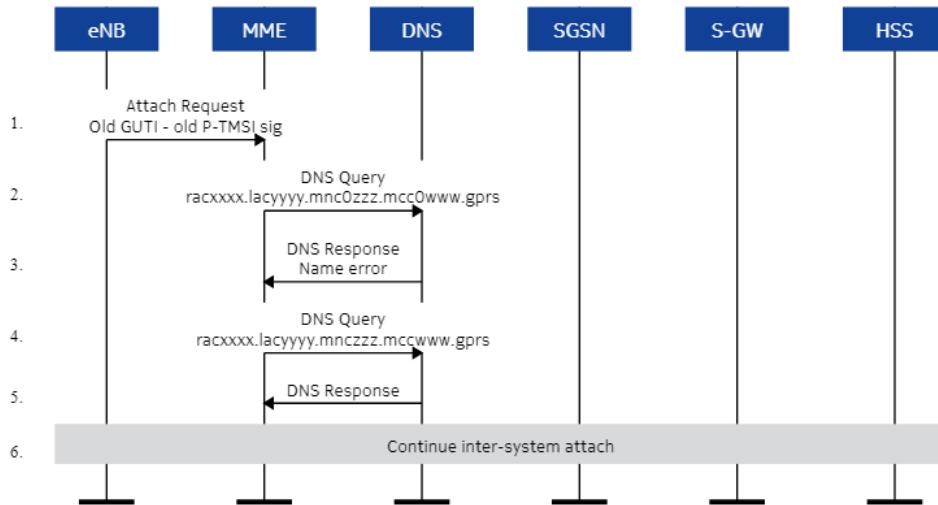
Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (network resource identifier (NRI) provisioned in the MME) is shown as follows:

Figure 48: Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (NRI provisioned in the MME)



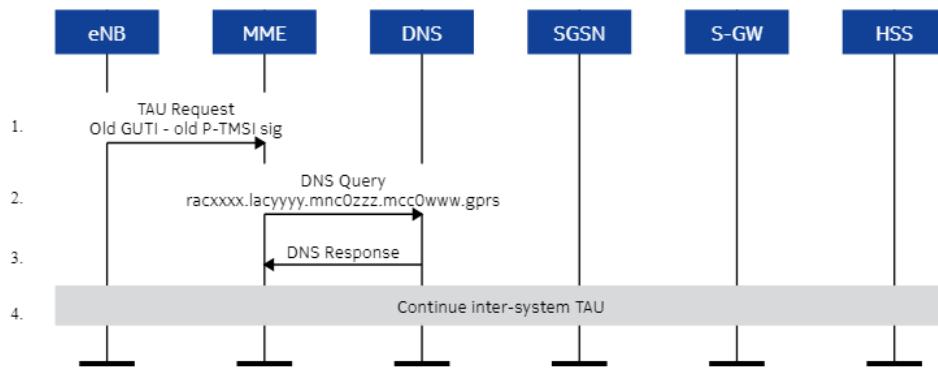
Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 49: Inter-system attach with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



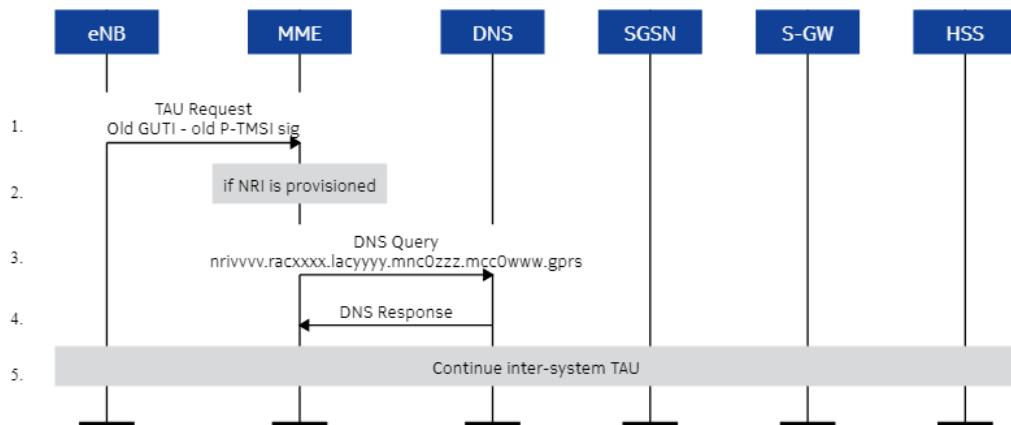
Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query is shown as follows:

Figure 50: Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query



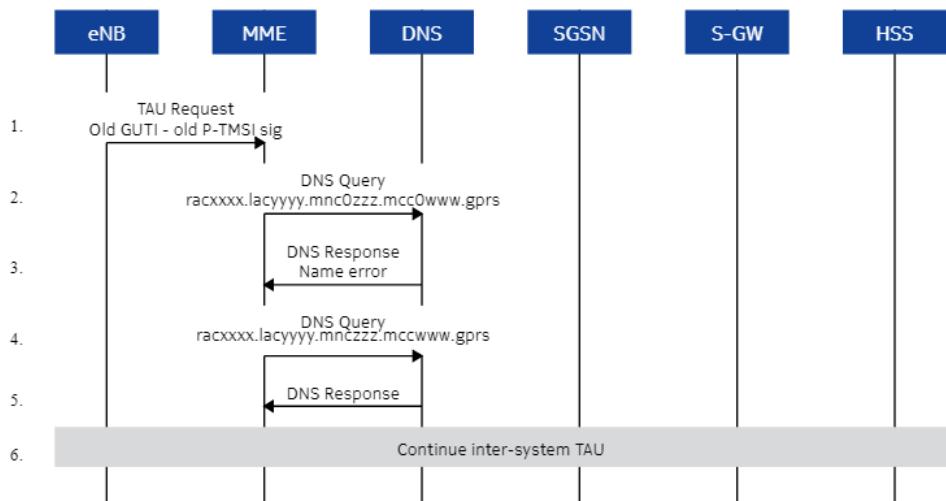
Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (NRI provisioned in MME) is shown as follows:

Figure 51: Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (NRI provisioned in MME)



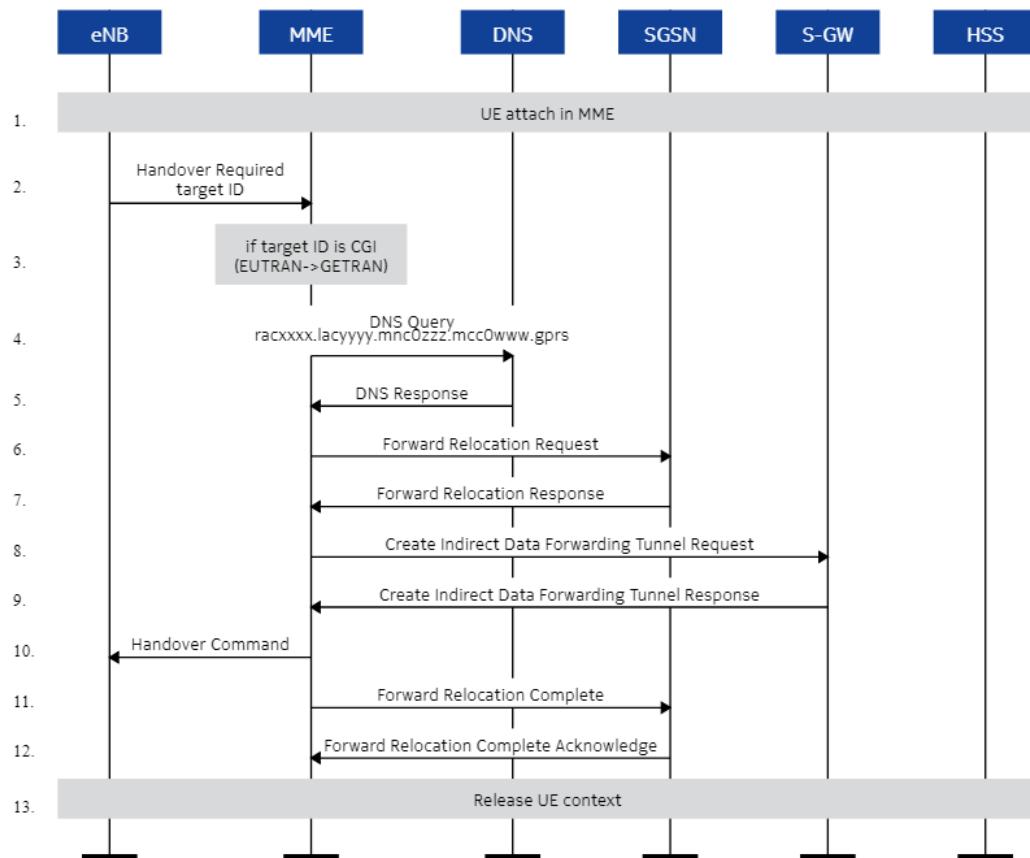
Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 52: Inter-system TAU with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



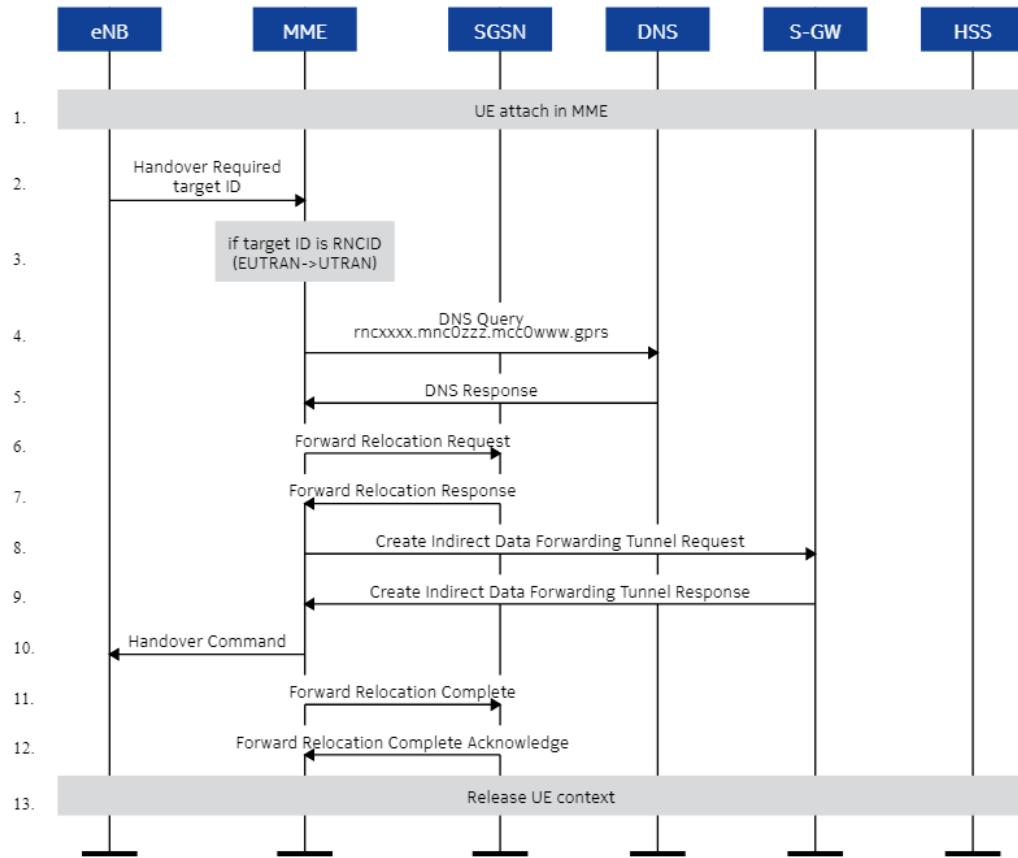
Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN) is shown as follows:

Figure 53: Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN)



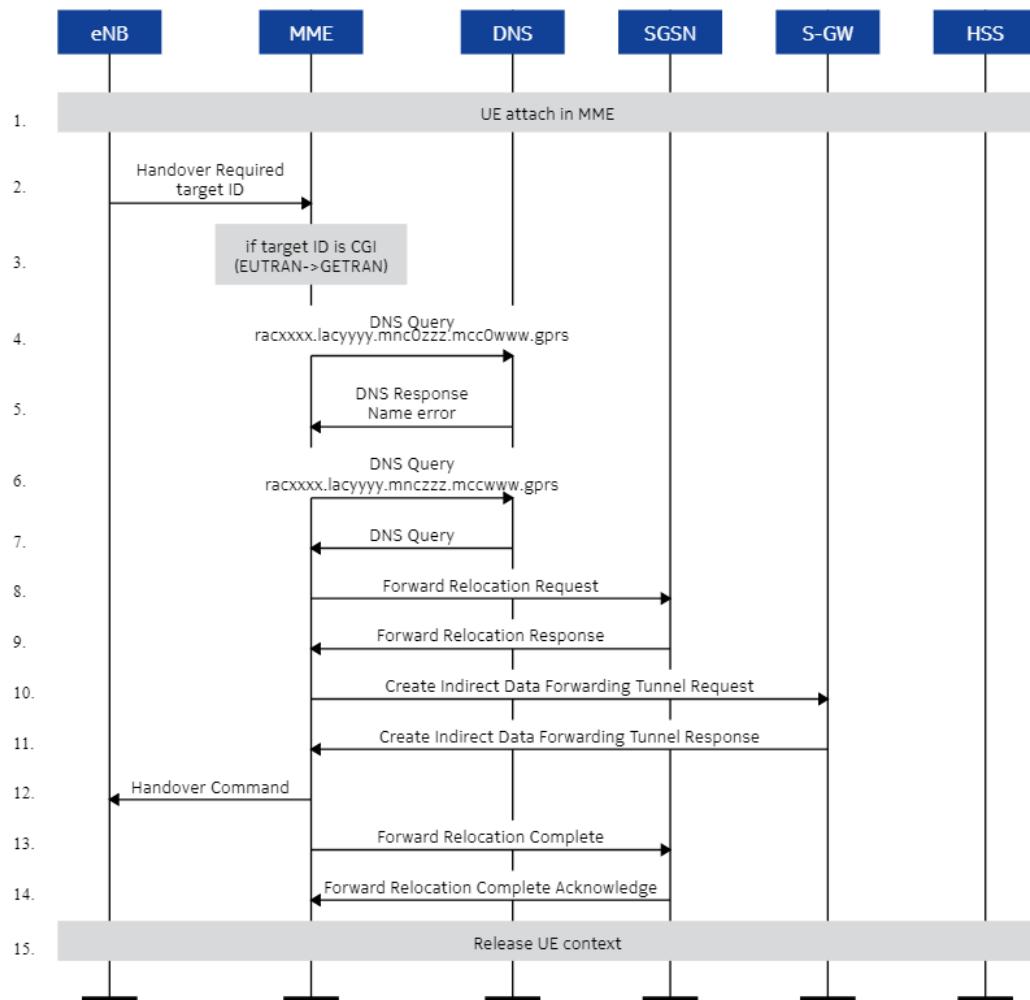
Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) is shown as follows:

Figure 54: Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN)



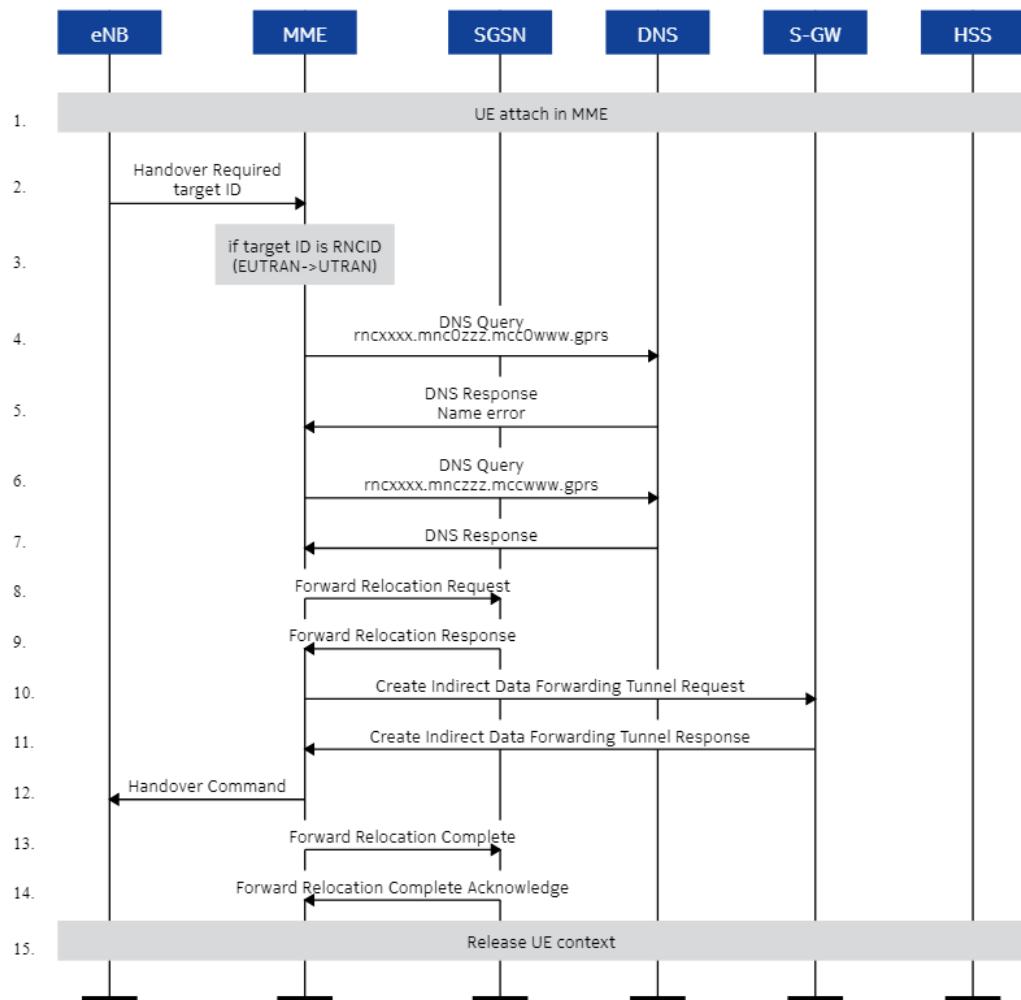
Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 55: Inter-system handover with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



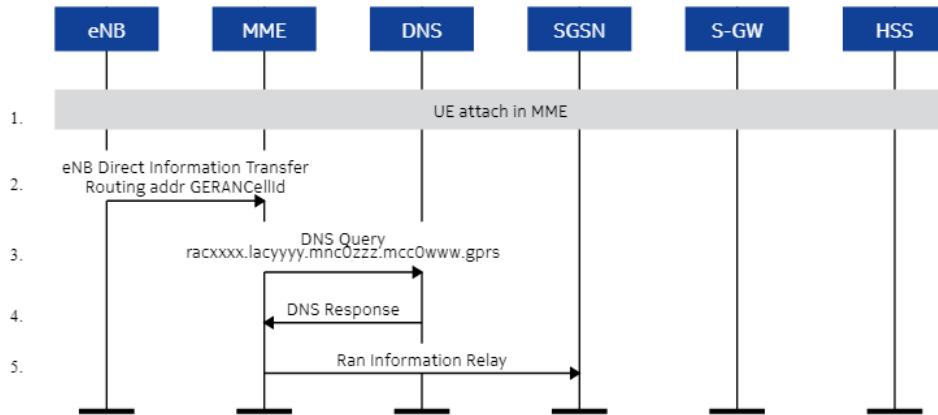
Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 56: Inter-system handover with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



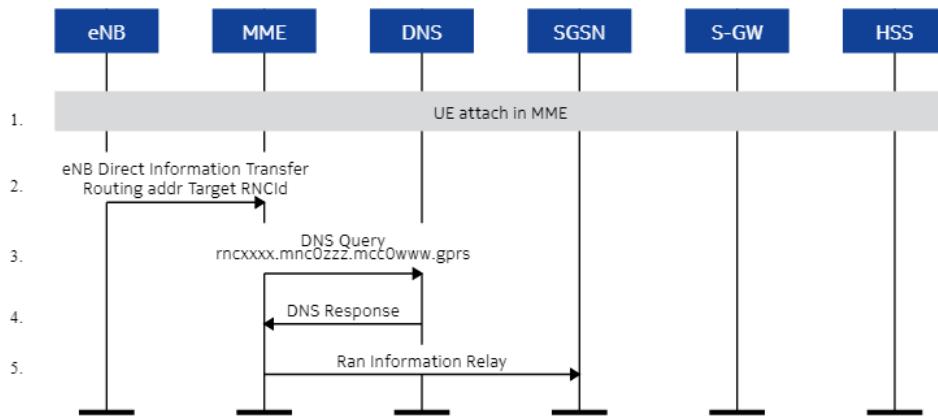
Inter-system RIM with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN) is shown as follows:

Figure 57: Inter-system RIM with Gn-SGSN using pre-Rel8 RAI FQDN DNS query (EUTRAN to GERAN)



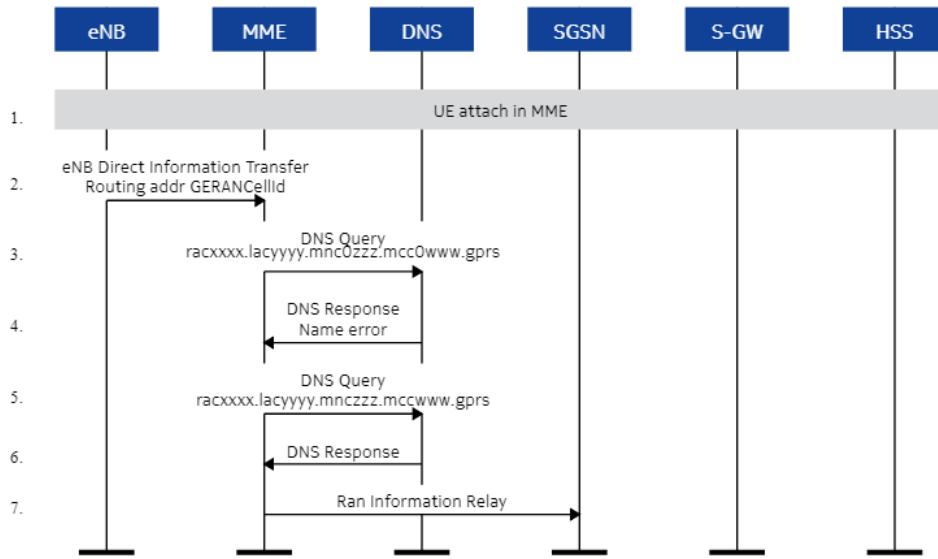
Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) is shown as follows:

Figure 58: Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query



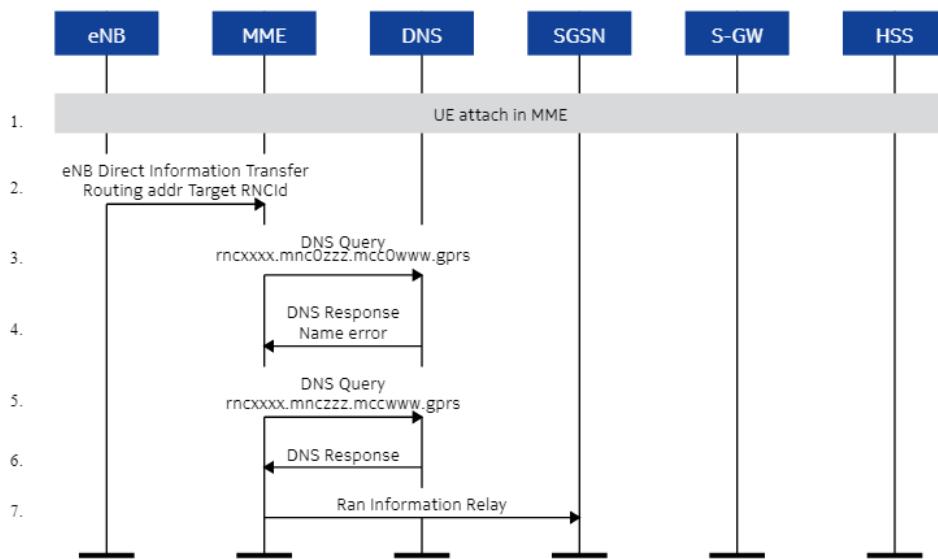
Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 59: Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query) is shown as follows:

Figure 60: Inter-system RIM with Gn-SGSN using pre-Rel8 RNCID FQDN DNS query (EUTRAN to UTRAN) (the DNS returns error and the MME falls back to pre-Rel8 3-digit query)



5.6 MSC selection

Features related to MSC selection (for SRVCC and CSFB).

5.6.1 MSC selection for SRVCC based on DNS procedures (Feature f11803-01)

By default, the MSC server is selected based on configured data in the location area identification (LAI) to MSC mapping tables for single radio voice call continuity (SRVCC). The *MSC selection for SRVCC based on DNS procedures* feature enables operators to use the domain name system (DNS) procedures to select the MSC server for SRVCC.

This feature supports selection of MSC server for SRVCC using the straightforward name authority pointer (SNAPTR) procedure. The MME constructs the routing area identity fully qualified domain name (RAI FQDN) based on routing area code (RAC), location area code (LAC), mobile network code (MNC), and mobile country code (MCC) received in the Target identity information element (ID IE) of the S1AP Handover Required message for the S-NAPTR procedures for the selection of the MSC server. The MME uses the configured LAI to MSC server mapping to select a MSC server if DNS fails for one of the following reasons:

- no NAPTR records are received
- there is no active Sv interface
- DNS query times out

In addition to DNS query for the NAPTR record with "a" flag, the MME supports DNS query for the NAPTR record with "s" flag. When the DNS SRV support features is enabled, the MME attempts DNS query for the NAPTR record with "s" flag to obtain SRV records for the selection of MME, P-GW, S-GW, and SGSN.

Alarm 40661 `LSS_mmeDnsError` is raised when the DNS query fails to obtain a valid record for the Sv interface.

This feature is dependent on the *Support for SRVCC handovers* feature.

Related descriptions

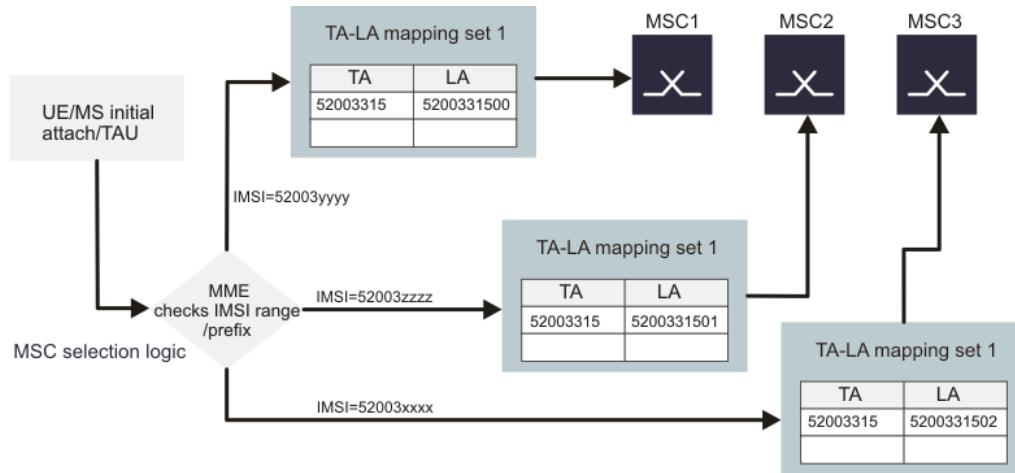
- [Sv-based UMTS hand down \(Feature m30102-01\)](#)

5.6.2 Provisioning of MSC selection for multiple 3G networks (Feature f11809-01)

This feature introduces provisioning of MSC selection for multiple 3G networks. The selection is based on IMSI range/prefix to TAI-LAI mapping.

If the feature is enabled, MSC selection (SGs MSC selection) is based on IMSI range/prefix to TAI-LAI mapping. Subsequently, MSC is selected. The MME supports multiple copies of TA to LA mapping tables. This feature applies to CSFB scenarios.

Figure 61: MSC selection based on IMSI range/prefix to TAI-LAI mapping



The feature is controlled by the global parameter `mscSelMultipleCsCoreSuppt` (by default, disabled). In addition, TAI to LAI mapping with IMSI range as the key is required.

5.6.3 CMM support for use HPLMN for SGs interface towards MSC (Feature f11815-01)

This feature introduces provisioning control for MME to always use the home PLMN on the SGs interface for specific procedures.

This feature, when activated by setting the global parameter `useHplmnforSgsInterface` to `Yes`, changes the way in which the MMENAME is constructed in SGsAP messages. When the feature is activated, the MME home PLMN will be used in the MMENAME. By default, this functionality is disabled.

5.6.4 CMM support for 3GPP IMSI hash for assigning a UE to an MSC over SGs (Feature f11823-01)

To align with the FNS algorithm, this feature supports 3GPP algorithm for assigning a UE to an MSC over the SGs interface. The benefit is to reduce HLR signaling in the circuit core in networks with mixed FNS and CMM.

The global parameter `use3gppImsiHashForSgs` controls whether the CMM uses its current hash algorithm or the 3GPP-based algorithm.

This feature allows the IMSI hash method defined in 3GPP TS23.236 to be used for MSC selection.

5.6.5 MME support for enhanced MSC/VLR selection (Feature f11807-01)

This feature enhances the existing 3GPP hash algorithm for assigning UEs to an MSC over the SGs interface. The selection is based on the provisioned relative capacity for each MSC, where the default relative weight is 50, maximum relative capacity is 100, and range is 1 to 100.

With enhanced MSC/VLR selection, the MME supports a weighted SGs distribution of the 3GPP hash algorithm.

Each defined MSC for SGs interface has a provisioned weight from 1 to 100.

The MME assigns to each MSC a portion of the 1000 hash buckets defined in the 3GPP algorithm, based on the MSC's proportion of all provisioned weights. Only active MSCs are included in the bucket list, and the per-MSC hash buckets are consecutive. If an MSC becomes unavailable (SGs/SCTP is not up), its buckets are reassigned to the available MSCs. The buckets for available MSCs are not updated so as to avoid registration storms on the circuit side. When the unavailable MSC becomes available, its buckets are reassigned to the original MSC.

This feature is enabled with gParm `weightedSgsImsiHash`.

6. Voice over LTE (VoLTE)

Voice over LTE (VoLTE) is a fully packet-switched (PS) voice over IP (VoIP) where LTE and evolved packet core (EPC) provide access control and connectivity functionalities and IP multimedia subsystem (IMS)/telecommunication application server (TAS) provide voice services and call control.

6.1 IMS voice over PS (VoLTE) critical CRs (Feature m10099-11)

The **IMS voice over PS (VoLTE) critical CRs feature supports 3GPP 29.280 CR 048r3 and 3GPP 29.272 CR 0405**.

The following 3GPP CRs are supported by this feature:

29.280 CR 048r3: The MME supports addition of single radio voice call continuity (SRVCC) post failure Cause information element (IE) to the SRVCC PS to CS Complete Notification message from the MSC server to the MME and addition of two SRVCC cause values Permanent session leg establishment and Temporary session leg establishment.

The MME simply logs the cause value and proceeds with the handover.

29.272 CR 0405: If the UE is in a detached state, the MME answers successfully to the T-ADS request from the HSS, but it does not include any of the T-ADS IEs in the response (IMS Voice over PS Sessions Supported, RAT Type and Last UE Activity Time).

The operator is able to provide voice service with related critical standard updates.

6.2 Capability of several ways to configure IMS APN (Feature f14616-01)

This feature introduces an enhancement to the existing CMM support for IMS APN.

This feature is controlled by global parameter `checkMatchApnConfig` (by default, disabled).

With this feature enabled (global parameter set to `Yes`) and when `matchApn` is not configured, APN with QCI = 5 will be considered as a non-IMS APN.

6.3 Rejection of IMS PDN connection when only wildcard is provided in subscription data (Feature f10100-01)

This feature introduces MME support for rejection of standalone IMS PDN connection and initial attach with cause value #33 Requested Service Option Not Subscribed in the PDN Connectivity and Attach Reject messages when IMS APN is not subscribed or it is subscribed only via the wildcard APN.

When this feature is enabled and the subscription does not have an IMS APN specifically subscribed, the attach or standalone PDN connectivity procedure with IMS APN is rejected with cause #33. This means the procedure is rejected even if the subscription has the wildcard APN with QCI 5.

6.4 Back-off timer inclusion when IMS APN not subscribed (Feature f10170-02)

With this feature, the MME supports sending T3396 back-off timer to PDN Connectivity Requests for unsubscribed IMS APN to stop UE retrying while personnel performs the necessary configuration updates.

The MME sends the T3396gen timer when rejecting an IMS PDN Connectivity Request message sent either as standalone or as part of the attach procedure because the IMS APN is not subscribed or the IMS APN is subscribed via the wildcard APN.

In case that the IMS APN is subscribed via the wildcard APN, the MME rejects the attach or PDN connectivity procedures towards the IMS APN when this feature is enabled. Otherwise, both procedures are allowed to continue.

The default ESM reject cause is #33 Requested service option not subscribed in PDN Connectivity and Attach Reject messages.

Note:

When the PDN Connectivity Request message is rejected as part of the attach procedure, the EMM cause ESM failure also needs to be included.

When timer `t3396genmax` has value higher than 0, whenever the MME rejects an IMS PDN Connectivity Request message sent as standalone or as part of the attach procedure because the IMS APN is not subscribed or subscribed only via the wildcard APN, the T3396 IE

is included in the PDN Connectivity Reject message to force the UE only to re-attempt after the timer expires.

Figure 62: Attach reject due to unsubscribed APN

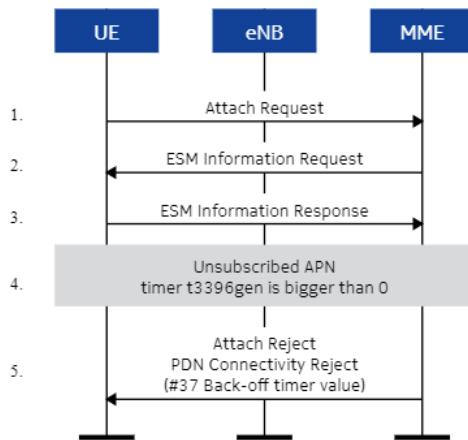
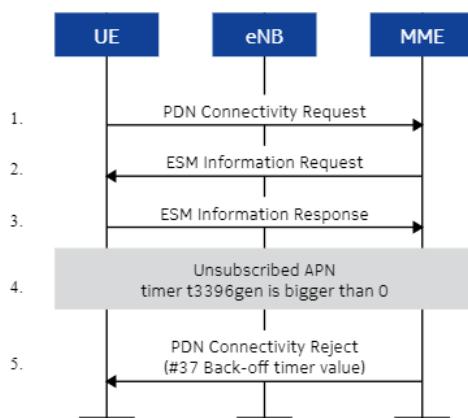


Figure 63: PDN connectivity reject due to unsubscribed APN



6.5 SRVCC

Features supporting single radio voice call continuity (SRVCC) for legacy 2G/3G network via Sv and for CDMA (1xRTT) via S102.

6.5.1 MME support for UE radio capability match request (Feature m10099-06)

MME supports query to eNB to find out whether a UE supports SRVCC and PS voice

frequency bands. MME uses this information to appropriately set the IMS voice over PS Session Supported Indication so that lost voice calls and/or degraded user experience can be eliminated.

MME supports UE radio capability match request procedure as specified in *3GPP TS 23.401* during initial attach procedure, during TAU procedure or when MME has no Voice Support Match Indicator. MME stores the Voice Support Match Indicator in the UE context.

The procedure is only used if UE radio capability match request procedure is enabled through provisioning.

Also, for the UE radio capability match request to occur, IMS voice over PS indication must be determined based on TAI provisioning of the `imsSupported` flag. Further restrictions may be placed for a given UE through service agreement provisioning (command `svcAgreementProfile`, parameter `imsOverPs`).

MME sets the IMS voice over PS support indication in Attach Accept and TAU Accept messages if IMS voice over PS as specified in the table:

Table 50: IMS voice over PS support

UE PLMN IMS Voice	IMS support in all TA in the TA neighbor list	UE SRVCC capability / local provisioning	Voice support match indicator	IMS voice over OS support indication to UE
Enabled	Supported	Capable / Enabled	Supported	Supported
Enabled	Supported	Capable / Enabled	Not supported	Not supported
Not enabled	Any value	Any value	Any value	Not supported
Any value	Not supported	Any value	Any value	Not supported
Any value	Any value	Not capable / Any value	Any value	Not supported
Enabled	Supported	Capable / Enabled	Not available	Supported
Any value	Any value	Capable / Not enabled	Any value	Not supported

MME supports the provisioning of the following:

- Enable/disable UE radio capability match request procedure
- Use UE SRVCC capability and local provisioning in determining the IMS voice over PS support for a UE.

The relevant parameters are `ueRadioCapabilityMatch` and `ueSrvccCapability` of the `plmn` command.

6.5.2 S102-based 3G1X circuit voice hand down (Feature m20102-01)

The *S102-based 3G1X circuit voice hand down feature provides ability to hand down voice call from the voice over long-term evolution (VoLTE) to code division multiple access (CDMA) circuit-switched network and call continuity across hand down.*

This feature supports single radio voice call continuity (SRVCC) across the S102 interface from voice over IP (VoIP) to circuit-switched (CS) voice access for calls that are anchored in IP multimedia subsystem (IMS), when the UE is capable of transmitting and receiving on only one radio access technology (RAT) at a specified time.

This feature is triggered when the UE, while having an ongoing IMS VoIP session, moves out of the LTE coverage, and the eNB determines that the target network does not support IMS-based VoIP.

If the UE has concurrent non-voice packet-switched (PS) sessions while in the LTE network, these non-voice PS sessions might be handed over to the target network during the SRVCC handover procedure, depending on the UE and target network capabilities.

The MME interacts with IWS over the S102 interface to complete the SRVCC procedure.

This feature covers SRVCC from E-UTRAN to 1xRTT. For SRVCC from E-UTRAN to 1xRTT, the MME first receives the SRVCC-handover indicator request from the eNB with the indication that this is for SRVCC handling. The MME then triggers the SRVCC procedure with the IWS over the S102 reference point if the MME has SRVCC STN-SR information for this UE. This feature does not cover SRVCC from UTRAN (HSPA) to UTRAN/GERAN nor SRVCC from E-UTRAN to UTRAN/GERAN.

E-UTRAN attach or emergency attach procedure for 3GPP2 SRVCC UE is done as defined in 3GPP TS 23.401 with the following additions:

- SRVCC UE includes the SRVCC capability indication as part of the UE Network Capability in the Attach Request message. The MME stores this information for SRVCC operation.
- SRVCC UE capable for IMS emergency calls include the SRVCC capability indication as part of the UE network capability in the Emergency Attach Request message. The MME stores

this information for emergency SRVCC operation.

- The MME includes a SRVCC operation possible indication in the S1 AP Initial Context Setup Request, meaning that both the UE and MME are SRVCC capable.

The UE can initiate an IMS service emergency session over E-UTRAN as specified in 3GPP TS 23.167 and 3GPP TS 23.401. To facilitate session transfer of the IMS emergency session to the CS domain, the IMS emergency session must be anchored in the serving IMS. The eNB initiates the SRVCC procedure as specified for regular voice over IMS session. The MME is aware that this is an IMS emergency session and sends an indication to the IWS across S102 interface. The IWS through MSC Server then initiates the IMS service continuity procedure with the locally configured E-STN-SR to the serving IMS. When the handover of the emergency upon detecting handover is required from E-UTRAN to CDMA 1x, the SRVCC emergency procedure applies. To support handover of emergency session the network is aware that the UE and core network support SRVCC and has information to identify emergency session. When handover of the emergency session has been completed, the MME or the 1xRTT side can initiate location continuity procedures for the UE as defined in 3GPP TS 23.271.

To support SRVCC emergency session domain transfer for UEs in limited service mode (for example, UICC-less), the MME supports limited service mode UE emergency attach as defined in 3GPP TS 23.401 using unauthenticated international mobile subscriber identity (IMSI) or equipment identifier. When E-UTRAN determines that SRVCC is needed, the MME invokes SRVCC procedures to the 1xCS IWS including the UE's equipment identifier.

This feature also supports UE-SRVCC-Capability attribute-value pair (AVP) in ULR command and also notifies the HSS any changes to UE SRVCC capability using Notify Request command to support enhanced SRVCC (eSRVCC).

The MME supports the following procedures as specified in 3GPP TS 23.216 section 6.1:

- E-UTRAN attach procedure for SRVCC
- Service request procedure for SRVCC
- PS handover procedure for SRVCC

This feature requires IWS support for S102 and SRVCC, LTE VoLTE services.

6.5.3 Sv-based UMTS hand down (Feature m30102-01)

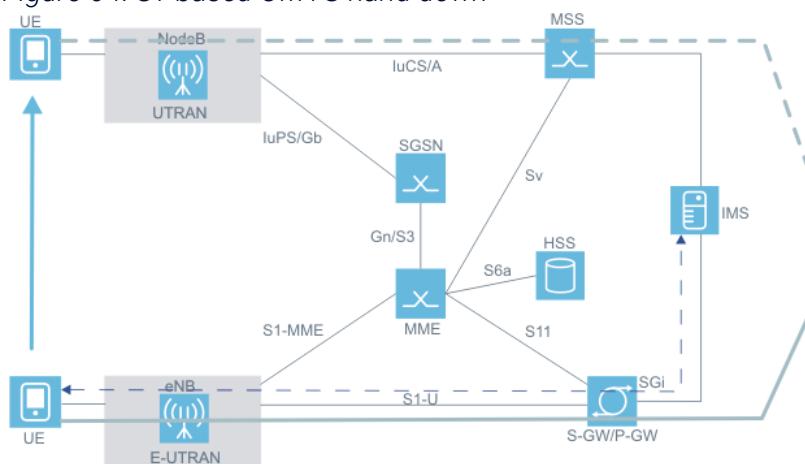
The handover of non-voice packet switching (PS) bearers, if done, is done according to inter radio access technology (IRAT) handover procedure as defined in 3GPP TS 23.401.

The MME coordinates the Forward Relocation Response from the PS-PS handover

procedure and the single radio voice call continuity (SRVCC) PS to circuit switching (CS) Response.

The UE can initiate an IP multimedia subsystem (IMS) service emergency session as specified in 3GPP TS23.167 and 3GPP TS 23.401. To facilitate session transfer (SRVCC) of the IMS emergency session to the CS domain, the IMS emergency session must be anchored in the serving IMS. The eNB initiates the SRVCC procedure as a regular voice over IMS session. The MME is aware that this is an emergency session and sends an indication to the MSC Server enhanced for SRVCC. The MSC Server then initiates the IMS service continuity procedure with the locally configured ESTN-SR to the serving IMS.

Figure 64: Sv-based UMTS hand down



The MME supports the IMS emergency service for UEs in limited service mode (for example, the UE does not have a universal integrated circuit card, that is, it is UICC-less). When the eNB determines that SRVCC is needed, the MME invokes SRVCC procedure to the MSC Server enhanced with SRVCC, including the UE's equipment identifier. The MSC Server sets up the call leg towards the emergency access transfer function (EATF) with the UE's equipment identifier. This procedure is defined in 3GPP TS 23.237.

This feature also includes support for the network based terminating access domain selection (T-ADS) to support incoming voice calls to the correct PS/CS domain.

The MME includes the Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions attribute-value pair (AVP) in ULR.

The MME also supports IDS-Flag T-ADS Data Request in IDR defined in 3GPP TS 29.272 CR 0211.

The MME includes IMS-Voice-Over-PS-Sessions-Supported (SUPPORTED or NOT_SUPPORTED), Last-UE-Activity-Time, and RAT-Type AVPs based on what is indicated to the UE.

This feature also supports Release 10 UE-SRVCC-Capability AVP in ULR command defined in *3GPP TS 29.272 R10* and notifies the HSS of any changes to the UE SRVCC capability using the Notify Request command to support eSRVCC.

IMS emergency session is able to continue on 2G/3G over CS.

6.5.4 1xRT SRVCC emergency call handling (Feature m11019-01)

The 1xRT SRVCC emergency call handling feature allows early introduction of IP multimedia subsystem (IMS)-based voice services in combination with code division multiple access (CDMA) networks.

This feature deals with a scenario where the UE is attached with emergency bearers only.

The UE/eNB sends an Uplink CDMA 2K message to the MME and the MME relays this message to the infoware system (IWS) using an A21 signaling message:

- The A21 signaling message to the IWS can only contain one type of mobile identity.
- When the MME has both the international mobile subscriber identity (IMSI) and international mobile equipment identity (IMEI), the MME sends the IMEI instead of the IMSI.
- Upon receipt of the IMEI from the IWS, the MME internally maps the IMEI to IMSI for routing.

If the IWS needs to send a message to the UE through the MME, the MME uses the IMEI as the mobile identity.

S102 interface support is required from 1xCS IWS.

6.5.5 Sv MSC Server selection enhancement for SRVCC HO (Feature m30102-07)

With the Sv MSC Server selection enhancement for SRVCC HO feature multiple MSCs can be deployed per location area identification (LAI).

This feature supports configuration of up to four Sv MSC servers (that is, MSC servers enhanced for single radio voice call continuity (SRVCC)) per LAI. The provisioned MSC servers for LAI are selected in round-robin fashion.

6.5.6 VoLTE support determination enhancements (Feature f10503-01)

The *VoLTE support determination enhancement* feature provides a capability on MME to check availability of STN-SR in UE subscription data and UE IMS APN subscription in determining IMS voice over PS indication to a UE in addition to checking the UE SRVCC capability and SRVCC feature activation in UE service agreement.

This feature provides provisioning to check availability of STN-SR and a separate provisioning to check UE IMS APN subscription.

Prior to this feature, IMS over PS indication was determined based on TAI provisioning of the `imsSupported` flag. In addition, the operator could place further restrictions on a given UE through service agreement profile provisioning (command `svcAgreementProfile`, parameter `imsOverPs`). MME also supported the UE radio capability match procedure.

With this feature, in addition to the above provisioning, MME can determine network IMS voice over PS support by

- checking STN-SR availability.

This functionality can be enabled using parameter `checkStnSrAvpAvailability` of the `plmn` command. If check STN-SR AVP availability is enabled and if HSS does not provide STN-SR, MME does not indicate support of IMS voice over PS to a UE in Attach Accept and TAU Accept messages and towards HSS in IDA if IDR comes with T-ADS bit in IDR-Flags. Also MME should indicate Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP as not supported towards HSS.

- checking UE IMS APN subscription.

This functionality can be enabled using parameter `checkImsApnSubscription` of the `plmn` command. If check IMS APN subscription is enabled and if HSS does not provide APN configuration AVP for IMS APN, MME does not indicate support of IMS voice over PS to a UE in Attach Accept and TAU Accept messages and towards HSS in IDA if IDR comes with T-ADS bit in IDR-Flags. Also MME should indicate Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP as not supported towards HSS.

6.5.7 SRVCC possible indication for emergency calls (Feature f11008-01)

The feature can be used to enable SRVCC for all UEs during their IMS emergency calls despite of the SRVCC PS to CS setting in service agreement profile for the UE.

When the feature is enabled, and the UE has indicated it supports SRVCC, but SRVCC PS to CS is not enabled in the service agreement profile for the UE, MME behaves as follows:

- When the normally attached UE initiates an emergency call, the MME informs the eNB that SRVCC is possible. The MME sends an S1AP UE Context Modification Request message to the eNB to enable SRVCC after the emergency PDN is successfully established. The S1AP UE Context Modification Request message contains only S1AP IDs and SRVCC Operation Possible IE as Possible.
- When the MME detects an emergency call deletion, the MME informs the eNB that SRVCC is not possible. The MME sends an S1AP UE Context Modification Request message to the eNB to inform that SRVCC is not possible after the emergency PDN is deleted. The S1AP UE Context Modification Request message contains only S1AP IDs and SRVCC Operation Not Possible IE as notPossible.

6.5.8 Customized setting of voice parameters towards HSS (Feature f11319-01)

With this feature, the MME provides SRVCC capability towards HSS according to specific requirements based on UE SRVCC capability and MME support for SRVCC for the UE (on service agreement profile level).

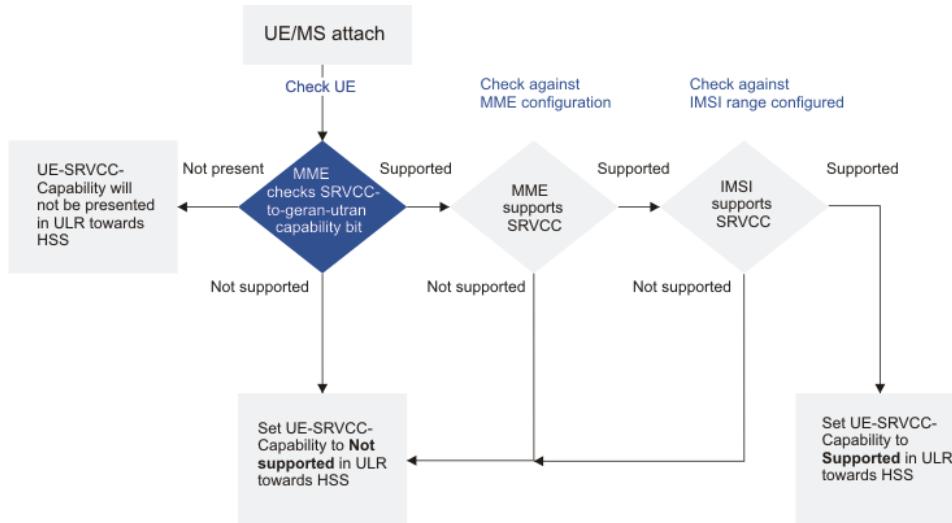
The MME provides Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions towards HSS according to specific requirements:

- tracking area's support for IMS voice over PS (separate activation parameter controls whether to include all TAIs MME globally, or all TAIs on the serving PLMN)
- voice over PS support for the UE
- checking or not checking the UE SRVCC capability (controlled by a parameter on service agreement profile level)

Functionality

The MME follows the logic shown in the figure to produce the SRVCC-capability AVP value towards the HSS:

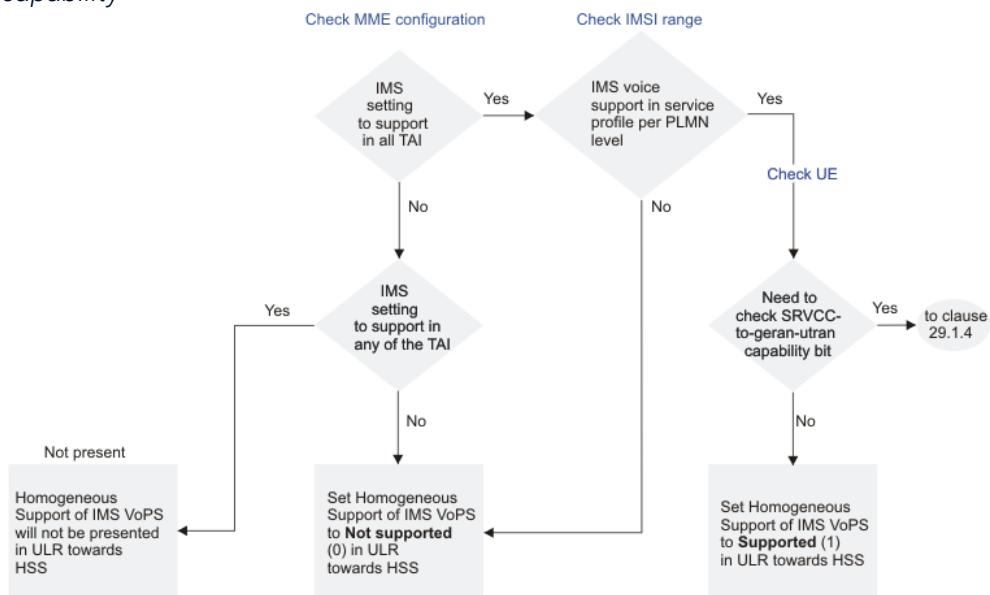
Figure 65: SRVCC-capability AVP value towards the HSS



- UE does not include MS network capability IE: UE-SRVCC-Capability AVP absent.
- UE does not support SRVCC to GERAN/UTRAN capability on MS network capability: the MME sends UE-SRVCC-Capability AVP as UE-SRVCC-NOT-SUPPORTED.
- UE supports SRVCC to GERAN/UTRAN capability on MS network capability:
 - The MME does not support SRVCC for the UE according to provisioning (UE PLMN/serving PLMN combination and/or IMSI range): MME sends UE-SRVCC-Capability AVP as UE-SRVCC-NOT-SUPPORTED.
 - The MME supports SRVCC for the UE according to provisioning (UE PLMN/serving PLMN combination and/or IMSI range): MME sends UE-SRVCC-Capability AVP as UE-SRVCC-SUPPORTED.

The MME follows the logic shown in the figure when providing Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP towards the HSS:

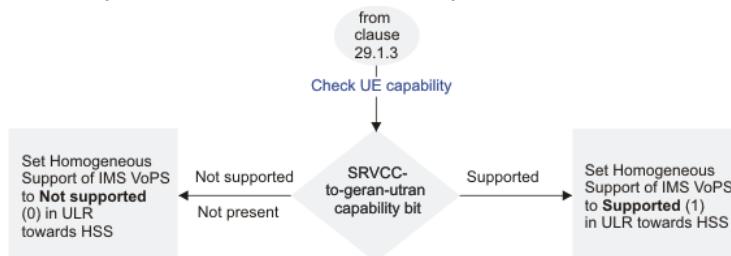
Figure 66: Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions IE based on system capability



The MME evaluates homogeneous IMS VoPS support. The MME takes into account the VoPS support of TAIs. The MME includes in the evaluation (according to the global parameter value) TAI of either the serving PLMN only, or all PLMNs MME globally (home PLMN and shared PLMNs) when evaluating whether all TAIs support VoPS (homogeneous support), none of the TAIs support VoPS (homogeneous non-support) or some TAIs support VoPS (homogeneous VoPS support IE absent or current TA supports VoPS).

- When some TAIs support VoPS, the Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be absent on S6a.
- When none of the TAIs support VoPS, the Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be indicated as NOT_SUPPORTED on S6a.
- When all TAIs support VoPS, the MME checks whether it supports voice for the UE on the MME provisioning:
 - If the MME does not support voice for the UE on UE PLMN/serving PLMN combination and/or IMSI range, Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be indicated as NOT_SUPPORTED on S6a.
 - If the MME supports voice for the UE on UE PLMN/serving PLMN combination and/or IMSI range, the MME checks the value of parameter `checkSrvccCapaForVopsHomogeneous` under `svcAgreementProfile` (may also be linked to UE PLMN/serving PLMN combination and/or IMSI range).
 - If `checkSrvccCapaForVopsHomogeneous` is disabled, Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be indicated as SUPPORTED on S6a.
 - If `checkSrvccCapaForVopsHomogeneous` is enabled, the MME follows additional logic as shown in the figure:

Figure 67: Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions IE based on IMSI prefix, UE capability, and MS network capability



If the UE does not include the MS network capability IE, or the UE does not support SRVCC to GERAN/UTRAN capability on MS network capability, Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be indicated as NOT_SUPPORTED on S6a.

If the UE supports SRVCC to GERAN/UTRAN capability on MS network capability, Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP will be indicated as SUPPORTED on S6a.

Provisioning

The MME supports:

- global parameter `homogeneousVopsSrvccCapa` to enable the feature
- global parameter `ueSrvccCapabilityHss` to control the value of the UE-SRVCC-Capability AVP the MME sends towards the HSS
- global parameter `homogeneousSupportTais` to define whether the MME includes voice over PS of home PLMN TAs or both home PLMN and shared PLMN TAs when evaluating homogeneous voice over PS support towards the HSS
- service agreement level parameter `checkSrvccCapaForVopsHomogeneous` to check or not to check the UE SRVCC capability for providing the homogeneous voice over PS support towards the HSS

6.5.9 Multi-SIM with VoLTE and SRVCC (Feature f10129-02)

This feature introduces an additional MSISDN parameter handling in MME.

Multi-SIM subscribers, besides having their own MSISDNs, share a common MSISDN which is the group-MSISDN that is used by the SAE-GW and PCRF for different applications, such as charging and legal interception. In such implementation, the HSS allows storing both MSISDN

identities per multi-SIM subscriber and the operator is given the flexibility to decide which, if not both, is propagated to the MME during the location update or subscriber update procedure. When both MSISDN (such as common MSISDN and own MSISDN) are configured, they are propagated to the MME in the MSISDN AVP and the additional MSISDN (A-MSISDN), respectively.

SRVCC feature also works for multi-SIM subscribers. When A-MSISDN AVP is downloaded to the MME via Diameter signaling, such as in Diameter Update Location Answer, it is used by the MME as the correlation MSISDN (C-MSISDN) during SRVCC.

To allow successful SRVCC for EPS multi-SIM subscribers in all possible configurations and implementations, the MME supports storing 2 x MSISDN per IMSI, propagated by the HSS during diameter procedures, such as, Location Update, in the MSISDN AVP and A-MSISDN AVP. The latter, when received, is commonly used to populate the C-MSISDN IE of the SRVCC PS to CS Request.

The A-MSISDN is also used on S1 handovers and IRAT handovers, on Forward Relocation Request message, towards another MME/SGSN as the C-MSISDN.

This feature is controlled with the global parameter `mmeAdditionalMsisdn`. If it is enabled, the MME:

- indicates support of A-MSISDN on ULR/IDA/DSA.
- takes the A-MSISDN into use if received on ULA>IDR/DSR.
- uses A-MSISDN as C-MSISDN on SRVCC PS to CS Request.
- uses A-MSISDN as C-MSISDN on Forward Relocation Request on the S3/S10/Gn interface, if it has been received from the HSS.

6.6 VoLTE access control

Features supporting selective VoLTE enablement.

6.6.1 Selective VoLTE enablement (Feature f10407-01)

The Selective VoLTE enablement feature provides the ability to deny UE access to defined tracking areas based on the configured combination of a UE's usage setting and voice domain preference (VDP). The feature prevents UEs from entering tracking areas where they cannot receive good service.

The feature is especially designed for LTE networks with different overlay frequencies under the same PLMN. Certain network frequencies areas can be defined as restricted for certain

types of UEs, and on another overlay frequency, the restricted areas can be indicated towards the E-UTRAN as forbidden to prohibit E-UTRAN from triggering any handovers to the restricted area.

For example, CS only, voice centric devices can be rejected from entering 800 MHz tracking areas with a configurable NAS return code, and when the same UEs access allowed 1800 MHz tracking areas, the 800 MHz areas are indicated as forbidden areas.

The feature can be enabled using global parameter `selectiveVoLteEnabled`.

MME allows configuring restriction profiles (VDP profiles) for UE's usage setting and voice domain preference combinations. This feature only includes the restriction option to completely deny the LTE access (for a given combination of UE's usage setting and VDP). By default, access is allowed. Each restriction profile is applicable to a set of tracking areas.

Options for UE's usage setting are

- Voice centric
- Data centric

Options for voice domain preference (VDP) are

- CS only
- CS preferred, IMS secondary
- IMS preferred, CS secondary
- IMS only

As also one option is that the values are not provided, different combinations include 9 possibilities. If either VDP only or UE's usage setting only is provided, but not both, this is considered as if neither is provided.

A restriction option to reject LTE access can be configured for each UE's usage setting and VDP combination option. The maximum number of restriction profile entries is 10. The combinations of restriction options for different kinds of UEs form profiles as shown in the table:

Table 51: Combinations of VDP and UE's usage setting (VDP profiles)

Voice domain preference	UE's usage setting	
	Data centric	Voice centric
CS only	dCsOnlyTreatment	vCsOnlyTreatment
CS preferred, IMS secondary	dCsPreferTreatment	vCsPreferTreatment
IMS preferred, CS secondary	dImsPreferTreatment	vImsPreferTreatment
IMS only	dImsOnlyTreatment	vImsOnlyTreatment

None (UE does not indicate both VDP and UE's usage setting): noneTreatment

MME is able to apply restriction profile entries on configured tracking areas.

In addition,

- MME provides the option to configure the NAS cause code used on attach/TAU rejection when LTE access is restricted. EMM cause #15 is the default cause code and used if no cause code is configured.
- MME provides an additional MME global provisioning option (`selectiveVoLteEmerAllowed`) whether to reject also the IMS emergency calls when LTE access is restricted.

EPS access restrictions apply to both EPS only registrations and combined CS/PS registration attempts. EPS access restriction applies to attach, intra-LTE and inter-RAT TAU, and X2-based/S1-based handover procedures for the provisioned tracking area/restriction profile combination. The handover procedures always use S1AP radio network cause Handover target not allowed for the handover rejection. In case of an inter-MME handover attempt, the target MME always uses Relocation failure as the GTP cause for the handover rejection.

The settings are applicable on the MME globally to all subscribers (both homers and roamers).

For each UE's usage setting and VDP combination, it is possible to provision which types of UEs are subject to forbidden TAI list sending:

Table 52: VDP and UE's usage setting combinations and forbidden TAI list sending

Voice domain preference	UE's usage setting	Forbidden TAI list sending (gParms)
CS only	Data Centric	<code>sendForbiddenTaiListDCsOnly</code>
CS preferred, IMS secondary	Data Centric	<code>sendForbiddenTaiListDCsPrefer</code>
IMS preferred, CS secondary	Data Centric	<code>sendForbiddenTaiListDImSPrefer</code>
IMS only	Data Centric	<code>sendForbiddenTaiListDImSOnly</code>
CS only	Voice Centric	<code>sendForbiddenTaiListVCsOnly</code>
CS preferred, IMS secondary	Voice Centric	<code>sendForbiddenTaiListVCsPrefer</code>
IMS preferred, CS secondary	Voice Centric	<code>sendForbiddenTaiListVImsPrefer</code>
IMS only	Voice Centric	<code>sendForbiddenTaiListVImsOnly</code>
-	-	<code>sendForbiddenTaiListNone</code>

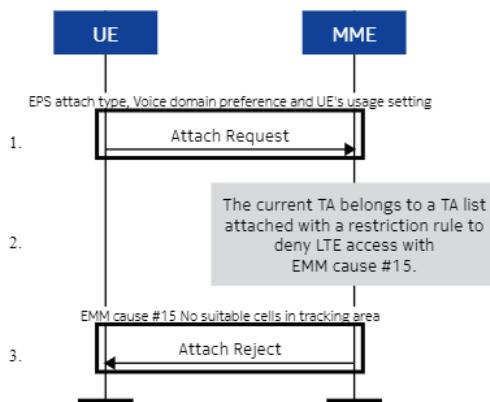
MME only includes the forbidden TAI list if the combination of UE's usage setting and voice domain preference is marked to be subject to forbidden TAI list sending, and the UE is currently accessing a separately provisioned tracking area linked with a forbidden TAI list.

The provisioned list of forbidden TAIs is sent for subjected UEs in the S1AP Handover Restriction List IE of the S1AP Initial Context Setup Request/Handover Request/Downlink NAS Transport messages.

It is possible to configure maximum 256 tracking areas on a forbidden TAI list. Up to 1000 forbidden TAI lists can be configured. The maximum number of TAs altogether on (potentially overlapping) forbidden TAI lists is 256000.

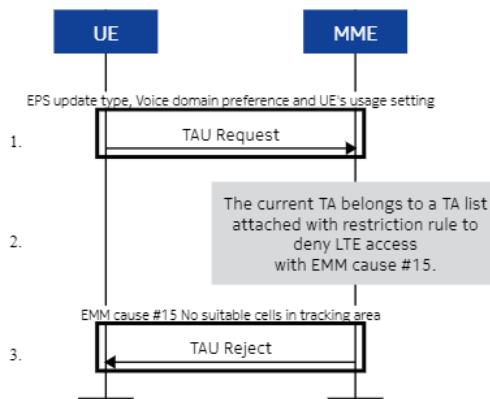
Example: Attach

Attach procedure when LTE is restricted for the TA and VDP/UE's usage setting combination (EPS attach type can be combined attach, old GUTI, old GUTI type, last visited TAI... and VDP/UE's usage setting can be voice centric, CS voice only, and so on):

Figure 68: Attach example

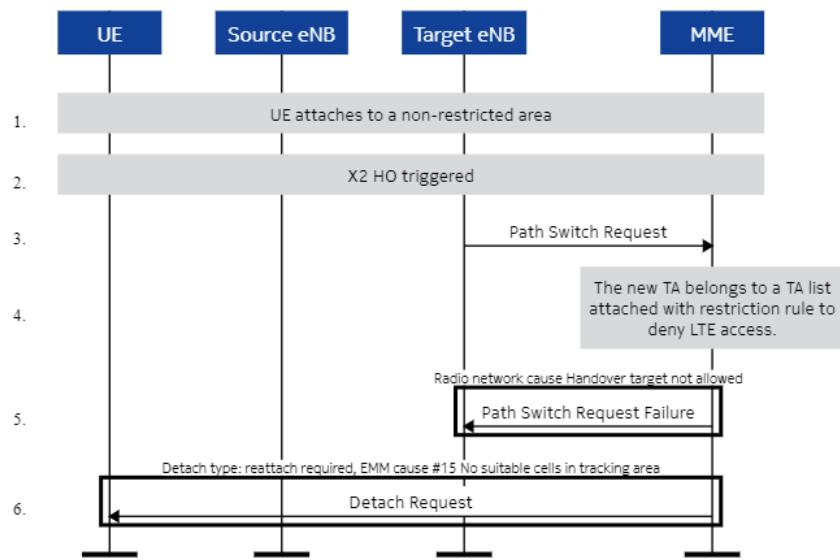
Example: Intra-LTE TAU

TAU procedure when LTE is restricted for the TA and VDP/UE's usage setting combination (EPS update type can be TA updating, old GUTI, old GUTI type, last visited TAI... and VDP/UE's usage setting can be voice centric, CS voice only, and so on):

Figure 69: Intra-LTE TAU example

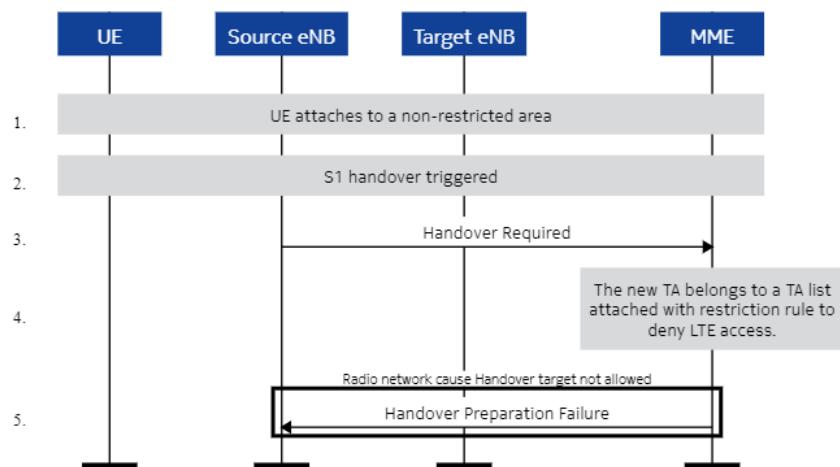
Example: X2-based handover

X2-based handover procedure when LTE is restricted for the TA and VDP/UE's usage setting combination:

Figure 70: X2-based handover example

Example: S1-based handover

S1-based handover procedure when LTE is restricted for the TA and VDP/UE's usage setting combination:

Figure 71: S1-based handover example

6.6.2 Selective VoLTE enablement enhancements (Feature f10407-02)

This feature provides further enhancements on top of feature Selective VoLTE

enablement (f10407-01). This feature enables partial access restrictions.

With this feature, the operator is able to restrict the CS service access of UEs indicating configured combination of UE's usage setting and voice domain preference (VDP) on specifically configured tracking areas. The MME allows EPS only registration but restricts the CS service access of the UE by limiting the CS service/SGs interface availability to 'SMS only', 'CS fallback not preferred' or 'CS domain not available'.

By restricting the CS service, the MME guides certain types of UEs to select GERAN/UTRAN access instead and disable its E-UTRAN capability. Thus, the operator is able to control the preferred type of radio access for different types of UEs.

The default setting is that both attach/TAU to EPS service, as well as combined attach/TAU to both CS and PS service is allowed. Any UE's PLMN-based restriction comes into effect if it is more restrictive than this feature's restriction.

6.6.3 Extending range of entryId in vdpRangeServices provisioning command (Feature f10407-03)

This feature increases the limits for the `vdpRangeServices` provisioning command to allow more voice domain preference (VDP) rules to be created.

In the provisioning command for `vdpRangeServices`, the `entryId` field is changed to have a range of 1 through 3072, instead of the former 1 through 1000. Also, the total number of records now allowed in `vdpRangeServices`, across all `uePlmnServicesNames`, is increased from 1024 to 3072.

6.6.4 MME support for VDP profile-based forbidden TAI inclusion separately per UE ranges (Feature f10407-04)

This feature allows the operator to more specifically define to which kind of UEs the forbidden TAI list, defined as part of the voice domain preference (VDP) range services, is sent to.

Previously, the implementation only allowed the operator to define via the global settings to which type of UEs the forbidden TAI lists were always sent, such as, to send "voice centric, CS voice only UEs". Furthermore, the forbidden TAI list was defined per IMSI/IMEI ranges as part of the VDP range services.

The previous implementation did not provide enough options for the operator to send

different lists for home/roaming UEs/MVNO users, and inside those definitions, to send the forbidden TAI list only to specific kinds of UEs, such as "voice centric, CS voice only UEs".

With this feature, the MME controls whether to send the forbidden TAI list to specific UEs in the VDP profile if one of the following situations are met:

- The operator is not able to derive the specific IMSIs/IMEIs, that are "voice centric, CS voice only UEs", into the IMSI/IMEI ranges.
- The IMSI/IMEI ranges are difficult to acquire and maintain.
- Both the previous two situations occur.

6.6.5 CSFB and VoLTE enhanced restrictions (Feature f10510-01)

The CSFB and VoLTE enhanced restrictions feature provides further enhancements to restrict CSFB and LTE usage on top of existing functionality provided by the Selective VoLTE enablement (f10407-01) and Selective VoLTE enablement enhancements (f10407-02) features. With this feature, the MME also supports the provisioning of IMSI and IMEISV ranges for the VoLTE/CSFB restrictions and the capability to detach misbehaving VoLTE UEs that either do not establish IMS PDN or perform IMS registration.

The features Selective VoLTE enablement (f10407-01) and Selective VoLTE enablement enhancements (f10407-02) provided MME support for restrictions based on the combination of UE usage type, voice domain preference (VDP), and tracking area.

This feature adds the following criteria that can be used for provisioning restrictions:

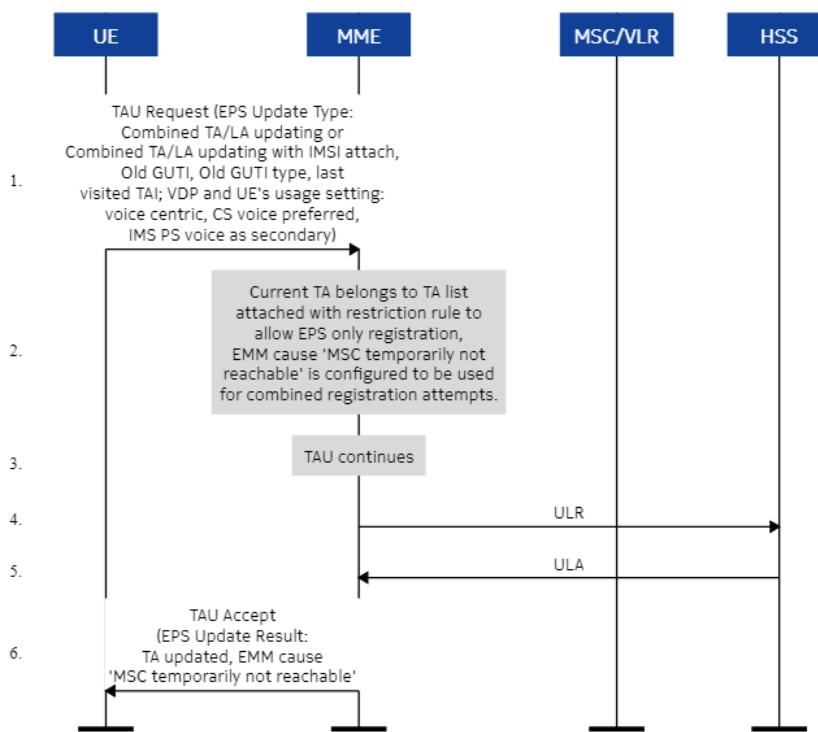
- IMEISV range
 - TAC+SVN, with both inclusive (applies if the UE's IMEISV matches the provisioned range) and exclusive (applies if the UE's IMEISV does not match the provisioned range)
- IMSI range (note that the full range equals a PLMN)
- UE IMEISV/IMSI ranges
 - additional override options for the existing UE usage type
 - VDP/TA combination, or additional criteria to apply the restrictions
- Separate provisioning restrictions for combined attaches and combined TAUs for treatment options
 - SMS_ONLY
 - CSFB_NOT_PREF
 - CS_D_NOT_AVAIL
- Restriction for EPS-only registration allowed with provisioned NAS cause code.
- IMS supervision

- With this capability, a provider can configure the MME to detach a misbehaving UE that keeps the IMS PDN connection without successful IMS registration or does not activate an IMS PDN connection. The IMS supervision treatment can be configured using a combination UE usage type, voice domain preference, tracking area, IMEISV range, and IMSI range. The relevant timers are `imsPdnActivation` and `imsRegistration`.

Example: EPS only attach

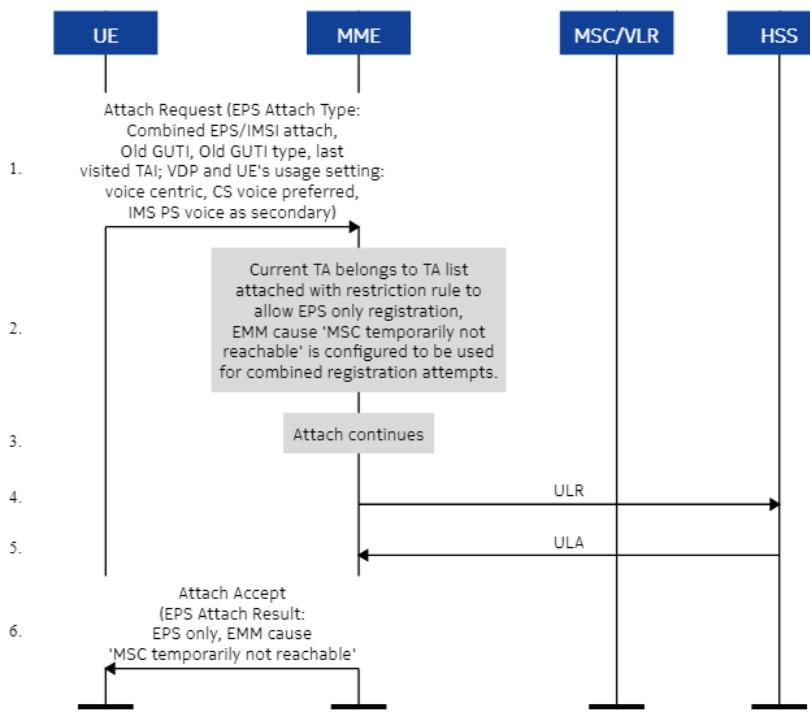
The following figure shows the TAU procedure when EPS only registration is allowed and the NAS cause is configured as "MSC temporarily not reachable".

Figure 72: TAU restricted to EPS only with configurable NAS code



The following figure shows the attach procedure when EPS-only registration is allowed and the NAS cause code is configured as "MSC temporarily not reachable".

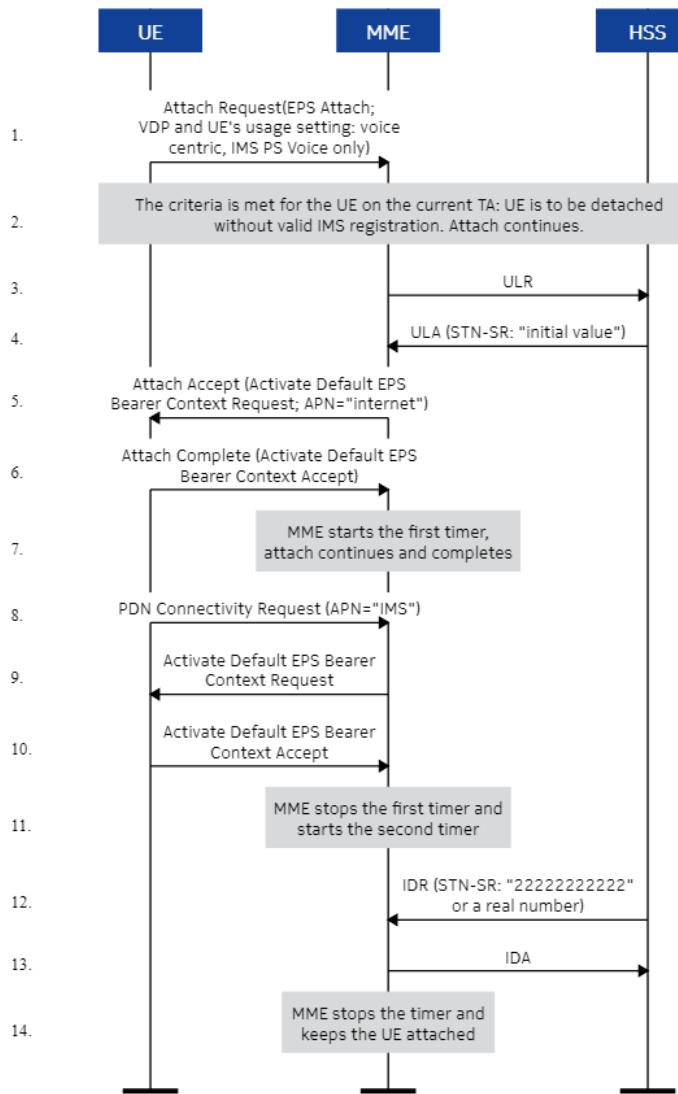
Figure 73: Attach restricted to EPS only with configurable NAS cause



Example: IMS supervision

The following figure shows the attach procedure when IMS supervision is provisioned for the UE. IMS PDN is not established during attach.

Figure 74: IMS supervision



6.6.6 CSFB sunsetting enhancement (f10510-02)

This feature provides two functionalities. First, as an enhancement to feature **CSFB and VoLTE enhanced restrictions** (f10510-01), the MME supports IMEISV sets/lists to be bound to a restriction rule. This feature also adds a possibility to override combined attach/TAU restrictions under specific conditions.

With this feature, the MME supports IMEISV sets/lists to be bound to a restriction rule created using the `vdpRangeServices`. The IMEISV list is defined by the number of IMEISV TAC SVs that are related to the restriction rule created with the `vdpRangeServices` command.

This feature also provides an override flag, `cmm vdpRangeServices`

`imsApnSubscrOverride`. By default, the flag is disabled. If the UE does not have IMS APN subscribed and if the MME is enabled for this feature, the MME takes the following actions:

- accepts any combined attach/TAU attempt from this UE (that is, the MME does not apply combined attach/TAU restriction for this UE, if such would be resulted based on other parameters of the restriction profile).
- sets IMS voice over PS session indicator (IMS VoPS) to “IMS voice over PS session in S1 mode not supported” on every Attach Accept/TAU Accept for this UE.

Related descriptions

- [CSFB and VoLTE enhanced restrictions \(Feature f10510-01\)](#)
- [Selective VoLTE enablement \(Feature f10407-01\)](#)
- [Selective VoLTE enablement enhancements \(Feature f10407-02\)](#)

6.7 IMS VoPS support

Features related homogeneous support of IMS VoPS indication to HSS.

6.7.1 Homogeneous support of IMS VoPS indication to HSS (Feature m11315-01)

With the *Homogeneous support of IMS VoPS indication to HSS* feature, the operators are able to provide voice service over the LTE access and indicate corresponding support to the IP multimedia subsystem (IMS) through the HSS.

This feature supports inclusion of the Homogeneous-Support-of-IMS-Voice-Over-PSSessions attribute-value pair (AVP) in Update Location Request to indicate to the HSS whether or not IMS voice over packet switching (PS) sessions (IMS VoPS) is supported homogeneously in all tracking areas (TAs) or routing areas (RAs) in the serving MME.

The value SUPPORTED indicates that there is support for IMS voice over PS sessions in all TAs or RAs. The value NOT_SUPPORTED indicates that there is no support for IMS voice over PS sessions in any of the TAs or RAs. The MME does not include the AVP if there is no homogeneous support of IMS voice over PS sessions, that is, some of the TAs in the MME serving support IMS voice over PS but not all TAs support it.

6.7.2 Homogeneous support of IMS VoPS indication to HSS for shared network (Feature m11315-02)

With the *Homogeneous support of IMS VoPS indication to HSS for shared network* feature an operator is able to provide voice service over the LTE access and indicate corresponding support to the IMS via the HSS also in network sharing environments.

This feature extends the support for homogeneous support of IP multimedia subsystem voice over packet switching sessions (IMS VoPSs) indication to shared network. The action taken by the MME depending on the provisioned support indication per tracking area (TA) in the home network (HPLMN) is now extended to provisioning associated with TAs in each of the serving (shared) public land mobile networks (PLMNs).

If the MME knows about the homogeneity of the support of IMS VoPSs in all TAs or routing areas (RAs) associated to that serving node (that is, it is supported in all the TAs or RAs or it is not supported in any of the TAs or RAs), it includes this indication to the HSS in the Homogeneous Support of IMS Voice over PS Sessions information element (IE).

- If Homogeneous Support of IMS Voice over PS Sessions in all provisioned tracking area identities (TAl)s in the serving PLMN is 0, the MME sends 0 to the HSS. However, if some are 1 and some are 0, the MME does not send this AVP to the HSS.
- If Homogeneous Support of IMS Voice over PS Sessions in all provisioned TAls in the serving PLMN is 1, the MME sends 1 to the HSS.

6.7.3 Enhanced homogeneous support of IMS VoPS indication to HSS (Feature m11315-03)

With implementation of the *Enhanced homogeneous support of IMS VoPS indication to HSS* feature, the MME bases the setting of the Homogeneous- Support-of-IMS-Voice-Over-PS-Sessions attribute-value pair (AVP) in ULR and also IMS-Voice-Over-PSSessions-Supported AVP setting in IDA based on the IMS voice over PS settings (IMS VoPS) at the public land mobile network (PLMN) level, global tracking area identity (TAI) level, and international mobile subscriber identity (IMSI) series and tracking area (TA) level for each UE of a PLMN. Operator is able to control the voice service and voice roaming per roaming partner (PLMN) and also control the voice service support per local network area (tracking area).

The MME basically checks IMS voice over PS settings at the PLMN level, global TAI level, and IMSI series and TA level to determine whether homogeneous support of VoPS is supported, not supported, or partially supported. If it is supported, the AVP is set to SUPPORTED. If it is

not supported in any TA, the AVP is set to NOT_SUPPORTED. If it is partially supported, the AVP is not included.

The MME checks the following IMS voice enabled provisioning to determine the setting of the Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP:

- MME tracking area
- IMS voice setting in service profile provisioned at the PLMN level
- IMS voice setting in service profile provisioned at the IMSI series and TA level.

Note that a UE can belong to multiple IMSI series and TA level provisioning. In this case, the MME has to examine all these to determine the homogenous support of IMS voice.

For example, a UE can belong to three IMSIs and TA provisionings. Assume that the IMSI range is the same but the tracking area code (TAC) provisioning is different:

- TACs from 200 to 210: IMS voice is enabled
- TACs from 355 to 375: IMS voice is disabled
- TACs from 515 to 520: IMS voice is enabled

The Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP is of type Enumerated.

The following values are defined:

- NOT_SUPPORTED (0): This value indicates that IMS voice over PS sessions is not supported, homogeneously, in any of the TAs or routing areas (RAs) associated to the serving node.
- SUPPORTED (1): This value indicates that IMS voice over PS sessions is supported, homogeneously, in all of the TAs or RAs associated to the serving node.

If this AVP is not present in the message, it indicates that there is no homogeneous support of IMS voice over PS sessions on all the TA/RAs of the serving node, or that the homogeneity of this support is unknown to the serving node.

The MME includes this in Update Location Request and Notify Request if there is a change to the IMS voice support.

The tables show how the AVP is set based on the provisioning.

Case 1: UE IMSI is not in any of the provisioned IMSI series

In this case, the MME checks the IMS voice provisioning of the TAI and IMS voice provisioning in the service profile assigned at the PLMN level.

Table 53: UE IMSI is not in any provisioned IMSI series

IMS voice setting of all TAIs Yes: supported in all TAIs No: not supported in any TAI Mixed: partial support	IMS voice support setting in service profile provisioned at PLMN level	Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP setting
No	Any value	NOT SUPPORTED
Yes	Yes	SUPPORTED
Yes	No	NOT SUPPORTED
Mixed	Yes	AVP is not included
Mixed	No	NOT SUPPORTED

Case 2: The UE IMSI is in one or more IMSI series and each IMSI series also has a TAI provisioning. The TAI provisioned are a subset or no TAIs are specified, that is, the provisioning applies to all TAs of the MME. If the UE is in multiple IMSI series that have different TAC provisioning, the MME has to look at all the provisioned data to determine the setting of the AVP. The IMSI series level checks result in the following values of the IMS support:

- Supported in some TAIs
IMSI series and TAC level provisioning indicate that the IMS voice is enabled for a subset of TAC served by the MME. There is no IMSI series and TAC level provisioning for which IMS voice is disabled.
- Supported in all TAIs
IMSI series and TAC level provisioning indicates that the IMS voice is enabled for IMSI series for all the TAC served by the MME.
- Not supported in some TAI
IMSI series and TAC level provisioning indicate that the IMS voice is disabled for a subset of TAC served by the MME. There is no IMSI series and TAC level provisioning for which the IMS voice is enabled.
- Not support in all TAIs
IMSI series and TAC level provisioning indicates that the IMS voice is disabled for an IMSI series for all the TAC served by the MME.
- Supported in some TAIs and not supported in other TAI (mixed)
IMSI series and TAC level provisioning indicate that the IMS voice is enabled for a subset of TAC served by the MME and disabled for another subset of TACs.

Table 54: UE IMSI is in a provisioned IMSI series

IMS voice support – result of IMS voice support setting in the service profile provisioned at multiple IMSI series and TA level	IMS voice setting of all MME TAs	IMS voice support setting in service profile provisioned at PLMN level	Homogeneous-Support-of-IMS-Voice- Over-PS-Sessions AVP setting
Any value	No	Any value	NOT SUPPORTED
Supported in some TAI	Yes	No	AVP is not included
	Yes	Yes	SUPPORTED
	Mixed	Any value	AVP is not included
Supported in all TAI	Yes	N/A	SUPPORTED
	Mixed	N/A	AVP is not included
Not supported in some TAI	Yes or Mixed	No	NOT SUPPORTED
	Yes or Mixed	Yes	AVP is not included
Not supported in all TAs	Yes or Mixed	N/A	NOT SUPPORTED
Supported in some TAI and not supported in other TAI	Yes or Mixed	Any value	AVP is not included

Note:

The TAI list in an IMSI series is assumed to be a partial list. The TAI list must be removed if the IMSI series applies to all the TAI in the serving area.

Related descriptions

- [Release 13 and Release 14 standards update for MME \(Feature f10002-01\)](#)

6.8 S1AP cause codes

Features enabling S1AP cause code provisioning.

6.8.1 MME provisioning for S1AP cause code to Normal release for double S1 and path switch (Feature f10907-01)

The **MME provisioning for S1AP cause code to Normal release for double S1 and path switch** feature provides the `nrCcDoubleS1PsAck` global parameter that is used to set the S1AP cause code to Normal release for certain scenarios. The feature also provides the global parameter `pdnDifferentApnOi` that specifies whether the MME sets up a second PDN connection with a different APN OI for an APN when the UE already has a PDN connection for the same APN.

If the `nrCcDoubleS1PsAck` parameter is set to Yes, the cause IE of S1AP UE Context Release Command is set to Normal release for the following scenarios:

- Double S1 events, that is, when the MME receives an Initial UE message while the UE S1 connection is up. For S1HO, the provisioning applies only to the UE Context Release Command message sent to the source eNB if the double S1 event occurs. If the parameter is set to No, the MME uses the cause value Radio connection with UE lost.
- The cause IE sent in E-RAB To Be Released IE of the Path Switch Request Ack message is set to Normal release in scenarios where bearers cannot be switched. If this parameter is set to No (the default), the MME uses the value Transport:Unspecified.

This feature also provides the global parameter `pdnDifferentApnOi`, which is used to enable or disable the MME to set up a second PDN connection with a different APN OI for APN when the UE already has a PDN connection for the same APN. By default the feature is enabled.

6.8.2 MME support for flexibility in configuring the S1AP cause codes (Feature f10902-02)

This feature allows the customers to change the S1AP cause codes for specifically defined scenarios.

This feature offers the provisioning of S1AP cause codes case by case in the MME for the cause IE in the UE Context Release Command and E-RAB Release Command messages. By default, the cause for each case is set to a value indicating the feature is disabled for this

case, for example, the MME follows the previous implementation. The provisioned cause codes are provided in the `s1apCauseCodeMappingProfile` command.

6.9 VoLTE QoS

Features enabling operator QoS class indicator (QCI) values.

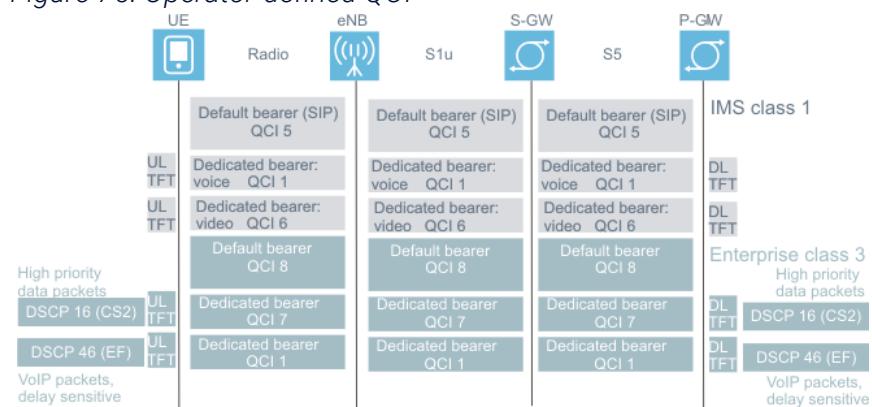
6.9.1 Operator defined QCI (Feature m10202-02)

The *Operator defined QCI* feature introduces support for specific operator QoS class indicator (QCI) values in addition to the standardized QCI. This is used for the user differentiation for guaranteed bit rate (GBR) and non-GBR traffic.

This allows classification of users between, for instance: gold, silver, bronze, and standard enterprise priority classes.

This feature creates placeholder QCIs, operator defined QCI1 through operator defined QCI6 that are provisioned with the actual QCI value that the operator wants supported. Up to 6 operator defined QCI values can be provisioned using any value in the range of 128-254. As an example, operator defined QCI1 can be provisioned with 131 when the operator wants the MME to support QCI 131.

Figure 75: Operator-defined QCI



This feature does not include support for:

- Provisioning of default quality of service (QoS) parameters for any of the operator defined QCIs
- Mapping of any of the operator defined QCIs to 2G/2G
- Mapping/override of QoS parameters for roammers
- UE-initiated requests, in other words, default bearer does not use custom/operator

defined QCI.

Before this feature, the MME supported a QCI range of 1 to 9 only. 3GPP TS 24.301 section 9.9.4.3 defines QCI as an 8-bit integer with QCI values divided as follows:

- 0: Reserved
- 1-9: Standard defined
- 10-127: Reserved
- 128-254: Operator specific
- 255: Reserved

This feature enhances the functionality by supporting the QCI range beyond the range 1-9.

Wherever the MME validity checks QCI, it first checks the table of provisioned operator specific QCIs and adds any provisioned values to the list of valid QCIs that are checked against. The MME gets QCI values from the network when requesting bearer setup. Handling of invalid QCI does not change from the current behavior.

Operators are able to provide special/specifically rated and proprietary services for customers.

Support is required throughout the rest of the network (the E-UTRAN, S-GW/P-GW).

Related descriptions

- [Enhanced operator defined QCI \(Feature f10167-01\)](#)
- [Operator defined QCI provisioning control \(Feature f10167-02\)](#)

6.9.2 3GPP specified new QCI values for mission critical and non-critical push to talk voice (Feature f10220-01)

The feature supports the new specified standardized QCI values which are used for unicast to meet the performance requirements for mission critical and push to talk (PTT) tasks.

A push to talk service provides one-to-one and one-to-many voice communication services. Users select the individuals or groups they wish to talk to. The session is connected in real time. Push to talk sessions are one-way communication (half-duplex): while one person speaks, the others only listen. Turns to speak are requested by pressing the talk key.

The feature complies with 3GPP TS 23.203, release 12.

The following QCI values need to be supported by the network:

- QCI = 65 (GBR): mission critical PPT voice
- QCI = 66 (GBR): non-mission critical PPT voice
- QCI = 69 (non-GBR): mission critical delay sensitive signaling
- QCI = 70 (non-GBR): mission critical data

The feature provides the same level of voice quality/performance for PTT+ application as for VoLTE. It eliminates the need for using QCI 1 if the operator wants to keep VoLTE bearers and PTT+ bearers on separate QCIs.

PTT service is part of a user's subscription and these QCI values can only be assigned upon request from the network side. MME validates/checks the received QCI values from the network during network-initiated bearer setup. Invalid QCI (for example, out of range QCI values) requests will be rejected.

The UE and any application running on the UE is not allowed to request these QCI values. If the UE requests any of the above specified QCI values, the request will be rejected by the MME with the cause code ESM Cause #59 - Unsupported QCI value. UE initiated modification or deactivation of bearers with these QCI values are accepted.

No provisioning is required to activate this feature.

6.9.3 Enhanced operator defined QCI (Feature f10167-01)

Feature *Enhanced operator defined QCI* introduces enhancement to the existing feature *Operator defined QCI* by supporting default bearers.

This feature enables use of enhanced operator defined QCI so that if operators want to assign QCIs other than 1-9, the MME will not reject session and mobility management procedures using those operator defined QCI values. QCI values can be provisioned using any value in the range of 128-254.

For 2G/3G to 4G TAU/handover procedures, PDP mapping will not map to operator defined QCI value, but to standards-based QCI 1-9 values. HSS-initiated QoS update during TAU after mobility may result in a QCI change to an operator defined value.

By default, this feature is disabled. It can be activated using the global parameter `supportDfltBearerOperDefQci`.

Related descriptions

- [Operator defined QCI \(Feature m10202-02\)](#)
- [Operator defined QCI provisioning control \(Feature f10167-02\)](#)

6.10 IMS emergency services

Features enabling IMS emergency services.

6.10.1 IMS emergency services (Feature m10106-01)

The **IMS emergency services feature provides the emergency bearer services to support IP multimedia subsystem (IMS) emergency sessions. The emergency bearer services are provided to normal attached UEs and depending on local regulations and operator's policy, to UEs that are in limited service state.**

This feature when receiving emergency services in limited service state does not require a subscription. Depending on local regulations and an operator's policy, the MME allows or rejects an emergency attach request for UEs in limited service state.

Based on the system settings, the MME can support emergency bearer services for the following types of UEs:

- Only valid UEs are allowed.

No limited service state UEs are supported in the network. Only normal UEs that have a valid subscription, are authenticated and authorized for the packet-switched (PS) service in the attached location are allowed to receive the emergency bearer service. It is not expected that a normal UE would do an emergency attach. Normal UEs should be attached to the network and then do a packet data network (PDN) Connection Request when an IMS emergency session is detected by the UE.

- Only UEs that are authenticated are allowed.

These UEs must have a valid international mobile subscriber identity (IMSI). These UEs are authenticated and can be in a limited service state because they are in a location that restricts them from the service. A UE that cannot be authenticated is rejected.

- IMSI required, authentication optional

These UEs must have an IMSI. If authentication fails, the UE is granted access and the unauthenticated IMSI retained in the network for recording purposes. The international mobile equipment identity (IMEI) is used in the network as the UE identifier. IMEI only UEs, for example, Universal Integrated Circuit Card (UICC) less UEs, are rejected in their attempts to receive the emergency bearer services.

- All UEs are allowed.

Along with authenticated UEs, this includes UEs with an IMSI that cannot be authenticated and UEs with only an IMEI. If an unauthenticated IMSI is provided by the UE, the unauthenticated IMSI is retained in the network for recording purposes. The IMEI is used

in the network to identify the UE.

To provide emergency bearer services, the MME is provisioned with the MME emergency configuration data that is applied to all emergency bearer services that are established by the MME on the UE request. This data contains the emergency access point name (APN) that is used to derive a PGW, or the data can also contain the statically configured P-GW for the emergency APN. The allocation retention priority (ARP) for the emergency bearers is also provisioned. The P-GW for emergency services is always located in the visited network (VPLMN).

In networks that support handover between E-UTRAN and high rate packet data (HRPD) accesses, the MME selects a P-GW that is statically configured in the MME emergency configuration data. The P-GW selection does not depend on the subscriber information in the HSS because an emergency call support is a local, not subscribed service. It is assumed that the same P-GW is configured in 3GPP and HRPD accesses.

An evolved packet system (EPS) security context is not set up for an unauthenticated UE that is emergency attached.

Once an IMS emergency call is in progress, the emergency call continuity is supported via single radio voice call continuity (SRVCC) when supported by the network and the UE.

Additionally, the source E-UTRAN and the source MME ignore any UE-related restrictions during handover evaluation when there are active emergency bearers. During tracking area update (TAU) procedures, including a TAU as part of a handover, the target MME ignores any mobility or access restrictions for the UE with emergency bearer services. Any non-emergency bearer services are deactivated by the target MME when not allowed by the subscription for the target location. Such UEs behave as emergency attached UEs in the target MME.

Call-back from a public safety answering point (PSAP) is supported for UEs that are not operating in the limited service state. However, the standards do not currently support priority paging for emergency bearer services.

UEs in ECM-CONNECTED mode with an active emergency bearer service are not released by the MME for rebalancing. The MME waits until the UE initiates a TAU or becomes inactive.

The MME supports an emergency attached mobile reachable timer specific for UEs that are emergency attached.

The MME records existence of an active emergency call in the UE context when there is an emergency bearer service established for the UE. Upon entering ECM-IDLE state the MME starts the mobile reachable timer for normally attached UEs and the emergency attached mobile reachable timer for the UEs that are emergency attached. At the expiry of the mobile

reachable timer or emergency attached mobile reachable timer the indication of an active emergency call in the UE context is removed.

The MME overload control procedure does not subject the emergency calls to the shedding algorithm under minor, major, or critical overload. If the critical overload condition persists for an extended period (a few seconds) then 100% of the non-emergency calls are subject to shedding and if the critical overload condition persists for an additional few more seconds, the emergency calls are also subject to 100% shedding.

If the MME starts running out of non-central processing unit (CPU) resources (for example, number of UE contexts it can store), the existing non-emergency and non-priority calls are dropped to make room for new priority and emergency calls. The existing priority calls and emergency calls are not dropped.

It is expected that the emergency APN, emergency quality of service (QoS) profile and emergency APN-aggregate maximum bit rate (AMBR) are always provisioned on the MME. If the P-GW identity is not provisioned on the MME, the MME uses straightforward name authority pointer (S-NAPTR) procedure to discover a P-GW. If the emergency P-GW identity is provisioned on the MME, the MME skips the S-NAPTR procedure for the P-GW discovery and uses the provisioned emergency P-GW identity.

If the emergency P-GW identity is provisioned as an IP address, that IP address is used for the emergency P-GW identity.

If the emergency P-GW identity is provisioned as a fully qualified domain name (FQDN), the MME launches A and AAAA domain name system (DNS) query to obtain P-GW IPv4 and IPv6 addresses. The MME gives preference to an IPv6 address if one is returned. Support for emergency bearer services is not expected to affect the system capacity or performance. However, under overload control conditions, the emergency bearer service request is given preference over non-emergency calls. This can cause a higher number of non-emergency calls to be shed under overload control conditions.

The feature fulfills regulatory requirements. Operators can make full voice over long-term evolution (VoLTE) offering also including the emergency service.

The MME support for the *IMS emergency services* feature has dependency on the *(Emergency) location based services* feature to meet the location reporting requirement for emergency services. The IMS emergency services feature also requires support from E-UTRAN, S-GW/P-GW, and IMS.

Related descriptions

- [\(Emergency\) location based services \(Feature m11000-01\)](#)

6.10.2 IMS emergency services enhancements (Feature m10106-02)

With the *IMS emergency services enhancements* feature the operator can control emergency users separately from normal users. Emergency users can be left idle for shorter or longer time than others on the network.

This feature provides the following requested enhancements to the *IMS emergency services* feature. It provides the following additional enhancements to the configuration data besides the enhancements listed in the *table 5.7.2-2 of 3GPP TS 23.401*:

- Separate configurable T3412 timer for emergency service only.
- Separate configurable mobile reachable timer in the MME for emergency attached UE only.

These two timers specific for emergency service can be included in the emergency configuration data so that the operator can manage it in a single place.

In addition,

- emergency bearers can be prevented from being transferred to the SGSN through Context Response as part of routing area update (RAU) procedure or Forward Relocation Request as part of the handover procedure.
- emergency bearers can be deactivated on the MME during inter-system RAU from the MME to SGSN.

6.10.3 Emergency dedicated bearer setup without piggybacking (Feature m11006-02)

The *Emergency dedicated bearer setup without piggybacking* feature allows the MME to support emergency dedicated bearer setup without piggybacking.

Currently the MME supports network initiated emergency dedicated bearer setup for only piggybacked dedicated bearer request for emergency calls.

This feature provides more options for IP multimedia subsystem (IMS) emergency voice service. The voice bearer for the emergency access point name (APN) can be established separately.

For this feature to work, the S-GW/P-GW support is required.

6.10.4 Configuration of E911 per TAI (Feature m10122-01)

The **Configuration of E911 per TAI** feature supports configuration of IP multimedia subsystem (IMS) E911 services support per tracking area identity (TAI) basis in addition to the support of IMS E911 service per MME-wide basis to help the deployment and testing of IMS E911 services one tracking area (TA) at a time.

The MME supports the UE emergency bearer services in S1 mode using the evolved packet system (EPS) Network Feature Support information element (IE) in Attach Accept and tracking area update (TAU) Accept message if an emergency profile is provisioned for the serving public land mobile network (PLMN) and if all the TAIs sent in the TAI List IE of the accept messages are provisioned to support emergency bearer services and there is an IMS voice over packet switching (PS) capability. No separate provisioning is required for roammers as the same provisioning applies to all the roammers. This provisioning must be supported for each shared PLMN if the MME is provisioned to support more than one shared PLMN.

The operator can restrict IMS emergency service introduction into specific areas for gradual deployment of emergency services.

6.10.5 Allow transfer of emergency bearers to SGSN (Feature m10106-03)

With the **Allow transfer of emergency bearers to SGSN** feature, an operator is able to control whether to provide emergency via packet switching (PS) or circuit switching (CS) and ensure that the LTE specific service (IMS emergency) is maintained only inside radio access that supports it.

The MME provides support for a global parameter that determines whether emergency bearers can be transferred to the SGSN.

- Value Yes allows the transfer of emergency bearers to the SGSN.
- Value No denies the transfer of emergency bearers to the SGSN.

By default, the emergency bearer transfer to the SGSN is denied.

6.10.6 E911 enhancements (Feature m10112-03)

The **E911 enhancements** feature provides an ability to send a SLg Location-Report-Request (SLR), also called LRR, with an indication of emergency call origination for a

subsequent set up of the emergency dedicated bearer.

If the feature is enabled, the MME sends the (LRR) EMERGENCY_CALL_ORIGINATION for emergency calls upon successful establishment of the following emergency default bearer of the emergency PDN session:

- successful completion of the emergency PDN connectivity request procedure (normal attached UE)
- successful completion of the emergency attach procedure and emergency PDN connectivity request procedure (limited/restricted service)

The MME does not send an EMERGENCY_CALL_ORIGINATION (LRR) for the first dedicated bearer once the active SOS APN session is established. After the default bearer of the emergency service APN and the voice dedicated bearer have been established, all subsequent requests for a dedicated EPS bearer for E911 calls on the same active emergency (SOS) APN always triggers an LRR (EMERGENCY- _CALL_ORIGINATION).

The LRR is not sent for failed default or dedicated bearer establishment requests (such as emergency attach reject).

E911 has only one GBR dedicated bearer with QCI=1 (voice bearer).

If the feature is enabled (global parameter

`s1rEmergencyInitiationDedicatedBearer`), the MME sends an LRR with an indication of emergency call release when the dedicated bearer of an emergency is released.

Whenever the MME detects the deletion of the dedicated bearer for the emergency PDN session, the MME sends the LRR (EMERGENCY_CALL_RELEASE), except when a bearer is being removed as the result of handover. The source MME still sends the LRR (EMERGENCY_CALL_HANDOVER) upon completion of both inter-RAT and intra-RAT handover events; and the target MME for an inter-LTE handover still sends the LRR (EMERGENCY_CALL_RELEASE) when the dedicated bearer is eventually removed (that is, the E911 voice call ends).

The MME does not send an additional LRR (EMERGENCY_CALL_RELEASE) when the emergency PDN session default bearer is deleted by P-GW after P-GW emergency PDN session inactivity timer expires, unless a dedicated bearer was never established on that emergency service PDN session. When the P-GW sends the Delete Bearer Request with the Default Bearer ID and the corresponding dedicated bearer has not been released yet, the MME sends the LRR (EMERGENCY_CALL_RELEASE) when the dedicated bearer is deleted because the emergency PDN session is about to be torn down.

The feature fulfills regulatory requirements. The location information is available for UEs making emergency calls.

This feature requires GMLC.

6.10.7 Non-standard treatment of serving node AVP in LRR (Feature f11308-01)

This feature allows the MME to always include the serving node AVP in LRR no matter there is an ongoing handover procedure for the IMS emergency call or not.

For SIMless UE emergency calls, the presence of serving node AVP in the LRR message is required by some customer GMLCs, even when there is no ongoing handover procedure. The AVP is optional. The MME always includes the serving node AVP. When there is not any ongoing handover procedure for the IMS emergency call, the MME name (mmecc*.mmegi*.mme.epc.mcc*.mnc*.3gppnetwork.org or epc.mcc*.mnc*.3gppnetwork.org) is used.

This feature can be enabled and disabled with gParm `servingNodeInLRR`. By default, it is disabled.

- When this feature is disabled, MME only includes the serving node AVP in LRR when there is an ongoing handover procedure for the IMS emergency call.
- When this feature is enabled, the serving node AVP is unconditionally included in LRR and is populated with the MME name when there is not an ongoing handover procedure of the IMS emergency call.

6.10.8 SIMless UEs to emergency attach independent of TAI (Feature m10141-01)

The *SIMless UEs to emergency attach independent of TAI* feature allows emergency services across all traffic areas (TAs) for SIMless UEs independent of any tracking area identity (TAI) restriction for general emergency service support.

This feature introduces a global parameter to allow all SIMless UEs to emergency attach independent of the current TAI.

For this feature to work, the *IMS emergency services* feature must be enabled.

6.10.9 Removing need for static IP and FQDN in emergency profile (Feature m10112-07)

Operators can use domain name system (DNS) configuration to discover an emergency P-GW. The *Removing need for static IP and FQDN in emergency profile* feature provides more possibilities for an emergency P-GW configuration.

This feature changes the provisioning of the emergency P-GW fully qualified domain name (FDQN) as an optional parameter. Provisioning of the access point name network identifier (APN-NI) of the emergency packet data network (PDN) is still mandatory. The MME does not change the current order of selecting the P-GW identity if all the three P-GW identities are provisioned (IP address, FQDN, and APN-NI).

DNS configuration must be updated.

6.10.10 IMS emergency services configuration enhancements (Feature m11003-01)

With the *IMS emergency services configuration enhancements* feature the IP multimedia subsystem (IMS) emergency service can be made available also for problematic UEs (those not reporting VoPS support).

This feature removes the restriction that IMS emergency services indication is only sent to the UE if IMS voice is supported.

This feature provides a global parameter to enable the feature.

- If the feature is activated, the MME allows IMS emergency services to be enabled without enabling the IMS voice.
- If the feature is disabled, the MME continues to support the restriction.

6.10.11 IMS emergency services configuration at the IMSI-NS level (Feature m10112-09)

With the *IMS emergency services configuration at the IMSI-NS level* feature the operator can control the IP multimedia subsystem (IMS) emergency service availability also per international mobile subscriber identity (IMSI) range. This feature helps in gradual deployment of IMS emergency services.

The MME supports provisioning to indicate to UE emergency bearer services in S1 mode

supported or not at the public land mobile network (PLMN) level (home, shared, and roaming partner networks), IMSI number series level, and at tracking area (TA) level.

Based on this provisioning and IMS voice provisioning, the MME sets the emergency bearer services indicator bit (emergency bearer services in S1 mode supported or emergency bearer services in S1 mode not supported) of the evolved packet system (EPS) Network Feature Support information element (IE) of the Attach Accept or tracking area update (TAU) Accept message sent to a UE.

- The UE uses this information to access the LTE network when initiating an emergency call.
- If IMS voice is not enabled, the bit is always set to emergency bearer services in S1 mode not supported.
- The MME only indicates changes to the IMS emergency services support on a subsequent Attach Request or TAU Request.
- If the emergency services are not allowed, the MME rejects any UE Attach Request for emergency services and also packet data network (PDN) Connectivity Request for emergency services with cause code #17 (network failure).

This feature provides configurable parameters to enable IMS emergency services support in service profile.

The feature supports the emergency provisioning parameter in the service profile to enable or disable emergency services at the public land mobile network (PLMN) level, IMSI series level, and TA level.

The following checks are needed to provide emergency services to a UE of a PLMN:

- The serving PLMN must be provisioned with an emergency profile.
- Emergency services must be enabled for the current TA of the PLMN and IMS voice capability must be enabled at the PLMN level or at the IMSI series level.
- The emergency parameter does not apply to the UE with international mobile equipment identity (IMEI) only. There are no changes to the CP behavior handling UEs with IMEI only.

In addition:

- If there is a service profile provisioned for an IMSI range and TAC that includes UE IMSI and current TAC, the MME must check if IMS voice and emergency services are enabled. If not, the MME checks the service profile provisioned for the UE PLMN to check that both IMS voice and emergency are enabled.
- Current requirements still apply for UEs with no roaming agreements and SIMless UEs.

This feature introduces a configurable global parameter to disable or enable IMS voice enabled check for IMS emergency support indication to the UE:

- If the global parameter is set to Yes and if provisioning indicates that IMS emergency is

enabled for the UE, the MME sends indication of support of IMS emergency service to the UE irrespective of the provisioning setting of the IMS voice support.

- If the global parameter is set to No and if the provisioning indicates that both IMS voice and IMS emergency services are enabled, the MME indicates to the UE support of IMS emergency service.
- The default for the global parameter is set to No to preserve current functionality when this feature is delivered. That is, the MME continues to support IMS emergency services indication based on the provisioning of both the IMS emergency service and IMS voice.

6.10.12 Enhancements for VoLTE emergency call deployment (Feature f11009-01)

Currently MME initiates the subscriber location request (SLR) procedure by sending LRR Location Event IE set to EMERGENCY_CALL_RELEASE whenever emergency bearer is released and an LRR for EMERGENCY_CALL_ORIGINATION has been sent. This feature extends this capability of sending SLR with EMERGENCY_CALL_RELEASE for abnormal release of emergency bearers.

The MME sends Subscription Location Report with EMERGENCY_CALL_RELEASE if the emergency bearers (dedicated or default) are released triggered either by UE, eNB or MME. The primary scenarios associated with this feature are abnormal release or deactivation scenarios.

This feature supports the global parameter `sendCallRelOnSlrEmerOrigFailure` to enable sending of SLR with emergency release to GMLC for conditions in which there is no response of a failed response from the GMLC after a Location Report has been sent.

The global parameter `slrEmergencyInitiationDedicatedBearer` of feature *E911 enhancements (m10112-03)* is not mandatory for correct operation of this feature. However, if the global parameter is enabled, MME sends LRR with emergency (release) for emergency dedicated bearer setup failure scenarios. If the parameter is disabled, MME does not send LRR (release) for dedicated bearer failure scenarios. Instead, the MME only sends LRR (release) for default bearer failure scenarios.

6.10.13 Emergency service enhancements (Feature f11017-01)

With this feature, if provisioned, the MME sends the emergency number list in attach and

TAU procedures, when the EPS network feature support IE indicates that emergency is not supported, but IMS voice over PS is supported. If disabled, the MME sends the serving PLMN's provisioned emergency number list during the attach or TAU procedure when the MME indicates that emergency is supported in EPS network feature support IE.

The feature is enabled through the `inclEmerNumListImsAllowed` global parameter.

When the feature is activated, the MME includes the UE's emergency number list during the attach and TAU procedure when the EPS network feature support with IMS voice over PS is sent and emergency call is not allowed. When the emergency number list is included, the MME uses the serving PLMN emergency profile information for the emergency number list. If the IMS voice over PS is not supported, the MME does not send the emergency number list.

Note:

The emergency number list will still be sent even if the MME indicates that the emergency is supported in the EPS network feature support list. This feature only impacts the emergency number list presence if it is to be sent due to the absence of the emergency support in the EPS network feature support list and the feature provisioning controls the IMS voice over PS criteria mentioned.

6.10.14 MME support for emergency call enhancements on LTE (Feature f11020-01)

This feature enhances the emergency feature by allowing the operator to provision P-GW-C+SMF for N1 capable UE for the emergency call for the MME.

An emergency P-GW-C+SMF is configured in the emergency configuration data in the MME in addition to an existing standalone emergency P-GW-C. The MME considers UE's support for the N1 interface based on the indication included in the UE network capability. The emergency P-GW-C+SMF is preferred, if it is provisioned during the emergency attach or standalone emergency PDN connectivity request procedure for N1 capable UE. Additionally, the MME sends the 5GS interworking indication towards the S-GW in Create Session Request message when P-GW-C+SMF is used.

6.11 Location services

Features supporting location-based services.

6.11.1 Homogeneous LCS enhancements: continuation of LCS session after S1 connection release (Feature m11000-02)

The **Homogeneous LCS enhancements: continuation of LCS session after S1 connection release** feature supports location services (LCS) when S1 connection was previously released because of data and signaling inactivity.

This feature enhances handling any ongoing location sessions of a UE when the S1 connection is released with the cause User inactivity by not aborting the location service session. Without this capability, location sessions fail when user inactivity exceeds the eNB inactivity timer value. The MME aborts an ongoing location session if the S1 connection release is because of any other cause than User inactivity.

This feature also supports paging of a UE if LPP PDU from the E-SMLC must be delivered and if the UE is in the ECM-IDLE state. The paging is only supported for the UE that has become ECM-IDLE state because of S1 connection release with the cause User inactivity.

6.11.2 Location report for UEs not supporting LTE positioning protocol (LPP) (Feature m11000-03)

With the **Location report for UEs not supporting LTE positioning protocol (LPP)** feature, operators can limit location reporting to LPP capable UEs to save signaling.

This feature supports a provisioning option to enable location reporting for UEs that only support the LTE positioning protocol. By default, this feature is disabled.

If the feature is enabled, the MME only initiates location reporting for UEs that indicate they are LPP capable.

If the feature is disabled, the MME initiates location reporting for all UEs irrespective of the UE's indication of LPP capability.

6.11.3 (Emergency) location based services (Feature m11000-01)

The **(Emergency) location based services** feature supports all the MME functions required for the control plane location services (LCS) in evolved packet system (EPS).

The MME supports location based services for the following purposes:

- IMS emergency services
- Coarse positioning
- HSS-triggered location request

The MME supports positioning of LTE devices, such as data-only devices. The MME obtains positioning information of these devices when requested by a GMLC using mobile terminated location request procedures. The MME supports positioning request for the following LCS client types:

- Emergency services

The emergency LCS is typically part of a service provided to assist subscribers who place emergency calls. In this service, the location of the UE caller and, if available, the positioning method used to obtain the location estimate are provided to the emergency service provider to assist them in their response. This service can be mandatory in some jurisdictions.

- Value added services

The commercial LCS (or value-added services) are typically associated with an application that provides a value-added service to the subscriber of the service, through knowledge of the UE location (and optionally, velocity) and if available, at the operator's discretion, the positioning method used to obtain the location estimate. This can be, for example, a directory of restaurants in the local area of the UE, together with directions for reaching them from the current UE location.

- PLMN operator services

The internal LCS (PLMN) is typically developed to make use of the location information of the UE for access network internal operations. This can include, for example, location assisted handover and traffic and coverage measurements. It can also include support for certain O&M related tasks and supplementary services.

- Lawful Intercept services

The Lawful Intercept LCS is typically part of a service provided to have an option to accept or deny the LCS client type for subscribers identified for lawful interception.

Support for value added services and PLMN operator services is provided by commercial location services. LCS for emergency services only requires NI-LR and MT-LR. MO-LR is not required.

If emergency services is enabled for the supporting tracking area, and if support for non-authenticated emergency mobiles is enabled, MT-LR and NI-LR for simless UEs, and UEs that have failed authentication is supported. An operator can provision these features on the tracking area identity and emergency profile MME provisioning.

The location of the UE caller and, if available, the positioning method used to obtain the location estimate is provided to the service provider.

Restrictions

The MME supports location services with the following restrictions:

- Only the immediate location request type is supported; delayed location is not supported.
- Authentication is not supported.
- Notification is not supported.
- Authorization is not supported.
- LCS billing and charging are not supported
- Non-dialable callback numbers are not supported.
- Network induced location request (NI-LR) is supported for emergency-attached UEs only.
- Mobile originated location request (MO-LR) is not supported.
- MSISDN is provided only if it is available from the HSS.
- Mobile terminating location request (MT-LR) query based upon MSISDN is not supported and will be ignored.
- Only the 15 digit IMEI format is supported.
- LPP APDUs between the E-SMLC and UE are limited to 7915 octets in length. Messages containing LPP APDUs larger than 7915 octets are dropped by the MME and LCSAP-Location-Abort message with cause value Misc is sent to the E-SMLC.
- The MME does not have any plans to support location based handover and traffic and coverage measurements.
- The MME does not support call independent supplementary services LCS procedures.

UE positioning methods in E-UTRAN

UE positioning methods refer to the technical solutions used to get an estimation of the target UE's geographical location. These techniques for UE positioning are supported in the UE and eNB with the assistance of E-SMLC. These methods are totally transparent to the MME. The following three positioning methods are specified by 3GPP TS 36.105 for E-UTRAN.

- Network-assisted global navigation satellite system (GNSS) methods
- Downlink positioning
- Enhanced cell ID method

See 3GPP TS 35.105 for a high-level description of these methods. Two modes of operation are possible for these methods: UE-based and UE-assisted. For the UE-based positioning,

the UE collects data and computes the position and sends it to the E-SMLC. In UE-assisted positioning operation, the UE collects location data and sends it to the E-SMLC for the computation of the geographical location.

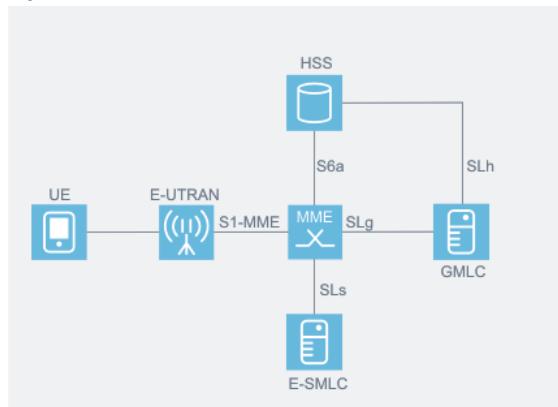
Indicating support for UE-based or assisted positioning

The MME populates the PS-LCS-Not-Supported-By-UE bit of ULR flags based upon the value of the UE LTE Positioning Protocol (LPP) capability (octet 7 bit 4) indicated in the UE network capability IE received from the UE.

Control plane EPS LCS reference architecture

The figure shows the EPS reference architecture for the support of LCS. The reference architecture does not include 2G and 3G reference architecture as the support of the LCS for 2G and 3G is beyond the scope of this feature. See 3GPP TS 22.071 and TS 23.271 for a complete description of LCS in EPS. The feature complies with 3GPP R9 standards.

Figure 76: EPS LCS reference architecture



To support control plane based LCS, the MME supports the following interfaces.

- **SLg** interface to gateway mobile location center (GMLC) to transport positioning requests and responses.
- **SLs** interface evolved packet core (EPC) serving mobile location center (E-SMLC) for obtaining UE's position.
- **S1-AP LPPa** transport messages. LCS positioning protocol (LPPa) is a protocol between eNB and E-SMLC used to obtain UE's position.
- Non-access stratum (NAS) messages Downlink Generic NAS Transport and Uplink Generic NAS Transport. The messages are used to transport transparent transport of LPP messages between a UE and E-SMLC.

Gateway mobile location center (GMLC)

GMLC is the first node to receive UE positioning requests from a LCS external client. An LCS client is a software or hardware entity that interacts with an LCS server (GMLC) for the purpose of obtaining location information for one or more mobile stations. LCS clients subscribe to LCS to obtain location information. LCS clients might interact with human users. The LCS client is responsible for formatting and presenting data and managing the user interface (dialog). The LCS client can reside in the UE. GMLC supports verification of identity of a client and client's subscription data. GMLC forwards a validated request to the MME over the SLg interface to obtain UE positioning data. GMLC has SLh interface to the HSS to obtain address of the serving MME to send client requests to the right MME serving a UE.

The GMLC obtains the address of the serving MME from the HSS to send client requests to the right MME serving a UE. The HSS contains the LCS subscription data and routing information.

EPC serving location mobile center (E-SMLC)

The E-SMLC manages the overall co-ordination and scheduling of resources required for the location of a UE that is attached to the E-UTRAN. It also calculates the final location and velocity estimate and estimates the achieved accuracy. The E-SMLC interacts with the UE to exchange location information applicable to UE-assisted and UE-based position methods and interacts with the E-UTRAN to exchange location information applicable to network-assisted and network-based position methods. The E-SMLC uses LTE positioning protocols (LPP and LPPa) to the UE and eNB respectively for the UE positioning. The positioning protocols are transparent to the MME.

The figures show the protocol layering between the UE and the E-SMLC and between eNB and E-SMLC.

Figure 77: Protocol layering for E-SMLC to UE signaling

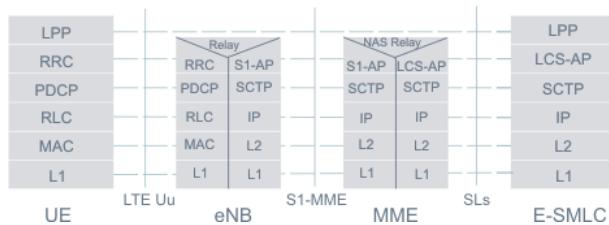
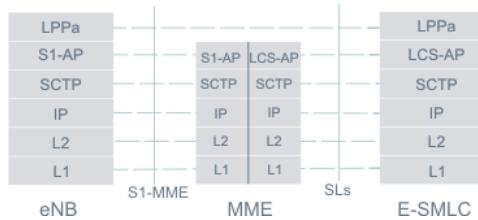


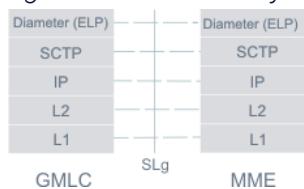
Figure 78: Protocol layering for E-SMLC and eNB



EPC LCS protocol (ELP) over SLg interface

The ELP defines procedures and coding of messages between the GMLC and MME. The protocol is specified in 3GPP TS 29.172. The ELP is a vendor-specific Diameter application. It reuses the basic mechanisms defined by the Diameter base protocol and it defines additional commands and attribute-value pairs (AVPs) to support SLg-specific procedures. The protocol stack used for the interface is shown in the figure.

Figure 79: Protocol layering between MME and GMLC



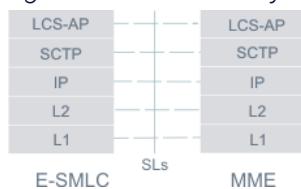
The MME's support of Diameter and SCTP comply with *RFC 3588* and *RFC 4960* respectively. For the SLg interface, the MME acts as client or server based on which node (the MME or GMLC) initiated a request. It is expected that semi-permanent SCTP associations are set up between the GMLC and MME. The GMLC establishes the SCTP association with the MME either at GMLC initialization time (the MME allows connections from a list of provisioned GMLC) or at the time the GMLC sends a positioning request to the MME. The GMLC can obtain the MME addressing information (MME fully qualified domain name, FQDN) from the HSS using the SLh interface. It is assumed that the MME always acts as the GMLC client and sets up the SCTP association with the provisioned GMLC.

The MME supports both the provider subscriber location procedure and subscriber location procedure and the associated messages as specified in 3GPP TS 29.172.

LCS application protocol (LCS-AP) over SLs interface

The LCS-AP is used between the MME and E-SMLC to support the LCS in the E-UTRAN. The figure shows the protocol stack associated with the SLs interface.

Figure 80: Protocol layering between E-SMLC and MME



The MME establishes semi-permanent connections with a set of E-SMLCs at the initialization time. The MME supports both local and remote multi-homing. An MME serving area can consist of several E-SMLCs and the MME provides an ability to configure tracking area identity (TAI) to the E-SMLC mapping to support an ability to select an E-SMLC for the UE positioning based on the UE's last seen TAI.

MME

The mobility management entity (MME) contains functionality responsible for the UE subscription authorization and managing positioning requests of the LCS. The MME is accessible to the GMLC through the SLg interface. The LCS functions of the MME are related to the LCS co-ordination, E-SMLC selection, location request, authorization and operation of the LCS services.

The MME can inform the HLR/HSS about the UE's LCS capabilities for EPS and can include the IP address of the GMLC associated with the MME in the Update Location Request message, during attach and inter-MME tracking area update (TAU) procedures.

The MME selects an available E-SMLC to serve the location request for a UE. The selection is based on network topology and should provide load balancing between E-SMLCs. Other criteria for E-SMLC selection can include LCS client type.

LCS options per PLMN

Introduced by feature *Location services enhancements - phase 2*, the LCS service options profile (`lcsOptionsProfile`) contains the attributes for a network. The profile consists of provisioning the following parameters:

- EPS state location info request flag (`epsStateLocInfoReq`)
 - QoS parameters to be used for UE location for HSS requested UE location
(`horizontalAccuracy`, `verticalAccuracy`, `verticalRequested`, `responseTime`)
 - Allow/disallow value-added location services (`valueAddedServices`)
 - Allow/disallow operator services (`operatorServices`)

Requirements

This feature requires the location services nodes (GMLC, E-SLMC) and other VoLTE IMS elements.

Related descriptions

- [Commercial location services](#)

6.11.3.1 Mobile terminating location request (MT-LR) procedure

The MT-LR procedure is used to manage external LCS client requests.

Steps in MT-LR:

- External LCS client requests location for a UE to GMLC.
- GMLC verifies LCS client subscription data to validate LCS client allowed to obtain UE position data.
- GMLC obtains the address of the serving MME from the HSS and sends the Provide-subscriber Location Request (PLR diameter command) message to the MME.
- The MME performs the following checks:
 - Optional check to see if the UE supports LPP
 - Tracking area has E-SMLCs with SLs links up associated with the tracking area
 - LCS client type global parameter associated with the PLR is enabled. Following are the supported client types (as indicated by their global parameter names):
 - `activateLcsClientTypeEmergencyServices`
 - `activateLcsClientTypeValueAddedServices`
 - `activateLcsClientTypePlmnOperatorServices`
 - `activateLcsClientTypeLawfulInterceptServices`
 - If the client type is value added services or PLMN operator services, and the MME is in overload, the MME will respond to a percentage of MT-LR requests with the cause indicated in the global parameter `mmeOverloadPlaResult`.
 - If a UE is ECM-CONNECTED, the MME uses the setting of the Retrieve cell ID global parameter (`retrieveCellId`) to determine whether to send S1AP Location Reporting Control to retrieve current cell ID and TAI for the UE. If parameter setting is Yes, Location Reporting Control /Location Report exchange with the eNB occurs prior to the MME contacting the E-SMLC for geographic information.
- The MME selects an E-SMLC based on the last visited TAI. If the primary E-SMLC endpoint

is not available, the CMM uses the secondary E-SMLC endpoint.

- The MME sends the location request to the selected E-SMLC.
- The E-SMLC initiates UE positioning. The positioning method is based on the position accuracy requested. E-SMLC uses the LPP and LPPa protocol to exchange location information with the UE and eNB respectively.
- The E-SMLC determines the UE location and sends the results to the MME.
- The MME responds with a Provide Subscriber Location Response - Diameter command Provide-Location-Answer (PLA) - to the GMLC from which the PLR was received. Routing of the PLA is based upon the GMLC from which the Provide-subscriber Location Request (PLR) was received.
- The MME saves location data in UE context.

6.11.3.2 Network-induced location request (NI-LR) for emergency calls

NI-LR applies only to emergency PDN attaches.

Support for NI-LR is as follows:

- The UE initiates emergency attach or emergency PDN attach. If the following are true, the MME initiates an NI-LR:
 - The supporting PLMN has an emergency profile configured, and `initiateLcsEmergency` on the associated PLMN provisioning (command `plmn`) is set to Send SLR to GMLC with estimated UE location
 - The supporting emergency profile (command `emergencyProfile`) indicated on the PLMN provisioning (`emergencyProfileName`) has the parameter `initiateLcsRequest` set to Send SLR to GMLC with estimated UE location.
- The following is only applicable when the MME is configured to use `Send SLR to GMLC with estimated UE location`:
 - The MME selects an E-SMLC based on the last visited TAI of the UE. If the primary E-SMLC endpoint is not available, the CMM uses the secondary E-SMLC endpoint.
 - The MME sends location request to the E-SMLC.
 - The MME uses the provisioned data for specifying the location accuracy to the E-SMLC.
 - The E-SMLC determines the UE location and sends it to the MME.
 - The MME sends the Subscriber Location Report (diameter command Location-Report-Request or LRR) to the GMLC provisioned on the emergency profile that is indicated on the PLMN provisioning.

- GMLC responds with Subscriber Location Report Ack (diameter command Location-Report-Answer or LRA).
- The MME saves location data in UE context.

If a UE attaches to an emergency APN, and NI-LR support is enabled, NI-LR updates are sent to the GMLC under the following conditions:

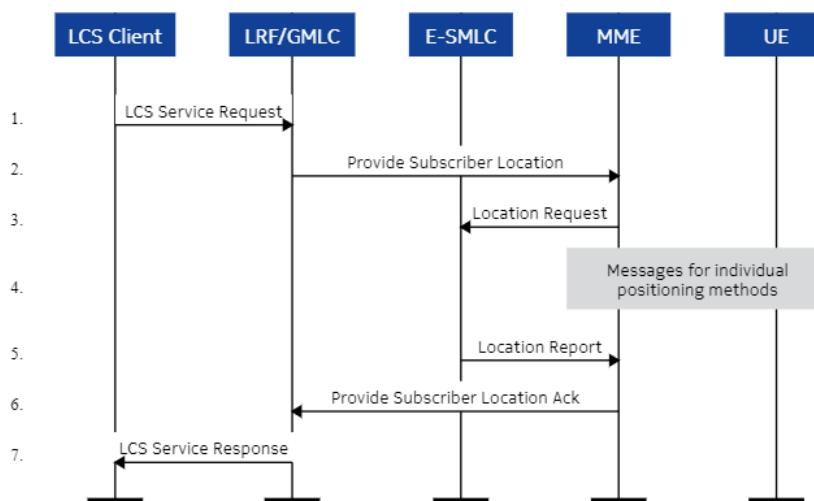
- Initial emergency attach or PDN connection
- S1 handover with MME relocation of an emergency session
- UE-initiated or network-initiated detach of an emergency session.

6.11.4 Customer specified emergency LCS handling (Feature f11007-01)

With this feature, MME supports MT-LR during emergency call or for clientType emergency, without contacting the E-SMLC.

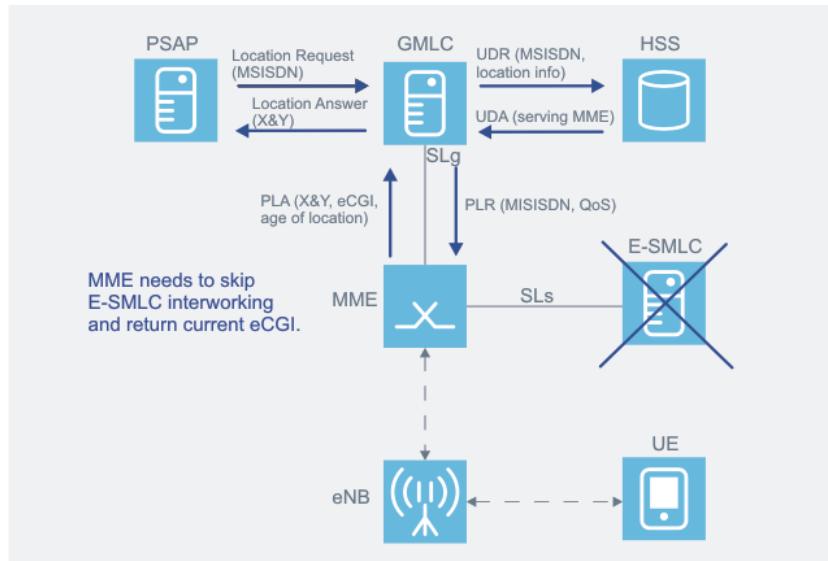
The 3GPP MT-LR procedure is carried out as follows:

Figure 81: 3GPP EPC MT-LR procedure



With this feature, MME skips the interworking with E-SMLC. Instead, the MME will report the current E-UTRAN Cell Global Identifier (eCGI) of the UE.

Figure 82: MT-LR without contacting E-SMLC



For getting current eCGI information of the UE, the UE may be in IDLE or CONNECTED mode:

- In IDLE mode, MME may send Paging message to the UE to establish radio contact and get current eCGI information.
- In CONNECTED mode, MME may perform S1AP location reporting control procedure to the eNB to get the latest eCGI.

If a UE is ECM-CONNECTED, the MME uses the setting of the global parameter

`retrieveCellId` (feature m11016-01 *Location services enhancements - phase 2*) to determine whether to send S1AP Location Reporting Control to retrieve current cell ID and TAI for the UE. If global parameter is set to value Yes, Location Reporting Control /Location Report exchange with the eNB occurs prior to the MME contacting the E-SMLC for geographic information. This function is generic to location services.

This feature can be activated using global parameter `emerMtLrNoEsmlc`.

When this feature is activated, it applies to mobile terminated location request (MT-LR) that either

- contains clientType=emergency or
- contains any clientType while an emergency call is ongoing.

Related descriptions

- [\(Emergency\) location based services \(Feature m11000-01\)](#)
- [Mobile terminating location request \(MT-LR\) procedure](#)
- [Location services enhancements - phase 1 \(Feature m11016-03\)](#)
- [Location services enhancements - phase 2 \(Feature m11016-01\)](#)

6.11.5 Configurable control emergency MT-LR eCGI timestamp (Feature f11007-02)

This feature introduces a configurable parameter as an enhancement to feature *Customer specified emergency LCS handling*. The operator can specify how up-to-date eCGI information in the MT-LR (Provide-Subscriber-Location-Ack) they want.

When feature *Customer specified emergency LCS handling* is enabled, the configurable timestamp of eCGI parameter (value range 0 - 180 s) controls the actions taken on receiving an MT-LR based on the eCGI timestamp of the UE:

- If the parameter is set to 0, when MME gets MT-LR from GMLC, MME either pages UE or sends Location-Reporting Control information to eNB to get current eCGI of the UE. MME reports eCGI to GMLC.
- If the parameter is set to a non-zero value, when MME gets MT-LR request, it will check the difference between the MME stored eCGI timestamp of the UE and the time of received MT-LR. If the time difference is less than the provisioned value, MME reports the stored eCGI information to GMLC. If the time difference is greater than the provisioned value, MME will request current eCGI either through paging or location report control, depending on the UE status.

6.11.6 MME support for configurable control with or without E-SMLC for any client type MT-LR (Feature f11016-01)

This feature allows the MME to report the current eCGI by contacting the eNB or by contacting E-SMLC, based on the provisioning for all MT-LR client types.

With this feature, the MME reports the current E-UTRAN Cell Global Identifier (ECGI) of the UE by contacting the eNB instead of the E-SMLC for all MT-LR client types, in addition to the previously-supported MT-LR emergency type. By default, the feature is disabled.

The MME adds support for controlling the following MT-LR client types:

- Value-added services
- PLMN operator services
- Lawful Intercept services

When the service for each MT-LR client type is activated, gParms are used to control whether the MME contacts the E-SMLC to obtain the UE's location or uses information from

the eNB. When this feature is enabled to set the MME to contact the eNB instead of the E-SMLC, the MME checks the difference between the MME-stored ECGI timestamp of the UE and the time that the MT-LR was received. If the time difference is less than the configured maximum time interval, the MME reports the stored ECGI information to GMLC. If the time difference is more than the maximum interval, the MME requests the UE's current ECIGI either by paging or by location report control, depending on the UE's status.

6.11.7 MME support for 4 ESMLCs per TA for emergency sessions (Feature f11011-01)

This feature increases the number of evolved serving mobile location centers (ESMLCs) per TA from 2 to 4 used for emergency services.

If the ESMLC selection is set to primary/secondary, the MME always selects ESMLC 1. If connection to ESMLC fails, the MME selects ESMLC 2. If connection to both ESMLC 1 and 2 fails, the MME selects ESMLC 3 and so on so forth.

6.11.8 MME support for NI-LR during MT-LR collision handling (Feature f11022-01)

This feature provides a provisionable option to report the network inducing location services activity to the GMLC while a mobile termination location service procedure is in progress.

When the CMM is processing a mobile terminated location service message (MT-LR procedure triggered by the MME receiving PLR message), the emergency related procedures are ongoing in parallel while it is reported to the GMLC.

When this feature is not enabled, the CMM queues the report to the GMLC until the MT-LR completes. The provisionable option sends immediately the emergency related procedures to the GMLC. The MT-LR complete continues in parallel.

7. Home eNodeB (HeNB)

A **Home eNodeB, or HeNB, is the 3GPP's term for a LTE femtocell or Small Cell. A HeNB performs the same function than an eNodeB, but is optimized for deployment for smaller coverage than macro eNodeB, such as indoor premises and public hotspots.**

The HeNB hosts the same functions as an eNB, however, instead of having an S1-MME interface directly with the MME, the HeNB Gateway (GW) can be deployed to limit the number of S1-MME interfaces between the HeNBs and the MME.

If an HeNB GW is deployed,

- the HeNB GW is responsible for discovery of an S-GW.
- the HeNB is only connected to a single HeNB GW at one time; it does not simultaneously connect to another HeNB GW, or another MME.
- the tracking area code (TAC) and public land mobile network (PLMN) ID used by the HeNB is also supported by the HeNB GW.
- selection of an MME at the time of the UE attachment is hosted by the HeNB GW instead of the HeNB.
- the S1-U interface from the HeNB can be terminated at the HeNB GW, or as a direct logical user-plane connection between the HeNB and S-GW.
- the HeNB GW appears to the MME as an eNB.
- the HeNB GW appears to the HeNB as an MME.

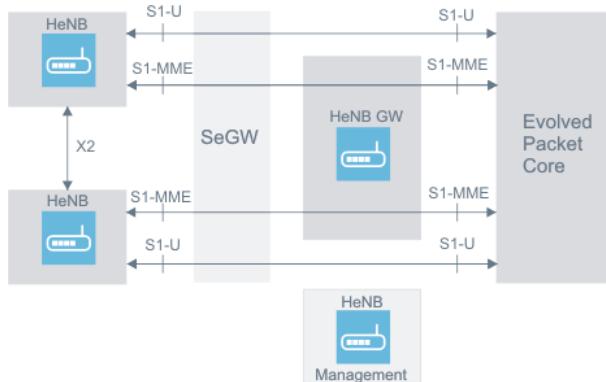
The S1 interface between the HeNB and the EPC is the same, regardless whether the HeNB is connected to the evolved packet core (EPC) through the HeNB GW.

7.1 MME support for Home eNB (Feature m14000-01)

The MME support for Home eNB feature provides all the key capabilities to support the Home eNB (HeNB). HeNBs are basically Femto Cells in the LTE.

See 3GPP TS 36.300 for detailed description of the HeNB, and HeNB gateway (GW) functions and reference architectures.

The figure shows a logical HeNB architecture.

Figure 83: HeNB architecture

The HeNB can be directly connected to the MME or through a HeNB GW. Note that the HeNB supports S5 if it supports the local IP access (LIPA) function.

The HeNB GW appears to the MME as an eNB and the HeNB GW appears to the HeNB as an MME. The S1 interface between the HeNB and the evolved packet core (EPC) is the same, regardless whether the HeNB is connected to the EPC via a HeNB GW or not.

Note that the *Support of multiple eNB with the same IP address* feature allows multiple S1-MME connections to use the same IP address. In particular, where there is a HeNB GW implemented, multiple S1-MME connections each defining a virtual GW can be established with the MME using a single IP address.

Support for 28 bit global HeNB ID

The *MME support for Home eNB* feature provides support for 28 bit global HeNB ID to distinguish between a macro eNB and Home eNB ID. When a HeNB connects directly to the MME, the HeNB sends 28 bit global HeNB in the Global eNB ID IE of the S1AP Setup Request message. The MME stores the global ID in UE context data for sending handover request and paging messages to the target eNB and also for coding of the target ID for type HeNB in the S10 Forward Request message.

The global eNB ID IE definition is shown in the following:

Table 55: Global eNB ID IE

IE/Group name	Presence	Range	IE type and reference	Semantics description
PLMN Identity	M		9.2.3.8	
CHOICE eNB ID	M			
>Macro eNB ID				
>>Macro eNB ID	M		BIT STRING (20)	Equal to the 20 leftmost bits of the Cell Identity ID contained in the E-UTRAN common gateway interface (CGI) information element (IE) (see 3GPP TS 36.300 section 9.2.1.38) of each cell served by the eNB
>Home eNB ID	M		BIT STRING (28)	Equal to the Cell Identity IE contained in the E-UTRAN CGI IE (see 3GPP TS 36.300 section 9.2.1.38) of the cell served by the eNB

Support for X2 handover in different combinations of HeNB connectivity

X2 handover is supported between

- HeNB and macro eNB directly connected to the same MME.
- HeNB connected to a HeNB GW and macro eNB to the same MME.
- HeNB directly connected to the MME and HeNB connected via HeNB GW to the same MME.
- two HeNBs connected to the same HeNB GW connected to the same MME.
- two HeNBs connected to different HeNB GW connected to the same MME.

Support for S1 handover in different combinations of HeNB connectivity

S1 handover is supported between

- HeNB and macro eNB directly connected to the MME with and without the MME relocation.
- HeNB connected to a HeNB GW and macro eNB with and without the MME relocation.

- HeNB directly connected to the MME and the HeNB connected via a HeNB GW with and without the MME relocation.
- two HeNBs connected to the same HeNB GW. The MME relocation is not supported in this case as it is assumed that all the HeNBs under the HeNB are connected to the same MME.
- two HeNBs connected to a different HeNB GW with and without the MME relocation.

Support for inter radio access technology (IRAT) handover with S4 SGSN and Gn/Gp SGSN interactions

If target ID received in S1AP Handover Required (or S10/S3/Gn Forward Relocation Request) message is an HeNB, the MME first determines whether the target HeNB is directly connected to the MME or not. If the HeNB is directly connected, the MME sends the S1AP Handover Request message to the HeNB. If the HeNB is not directly connected, the MME sends the S1AP Handover Request message to the HeNB GW with tracking area identity (TAI) matching the target TAI received in the S1AP Handover Required message (or in the S10/S3/Gn Forward Relocation Request message). The HeNB GW forwards the message to the target HeNB using the target eNB info in the Target to Source Container IE of the S1AP Handover Request message. The selection of the target HeNB GW based on the TAI imposes a restriction that TAI assigned to HeNB GW must be distinct to enable sending of the handover messages to one and only one HeNB GW.

For all the handover scenarios, the MME does closed subscriber group (CSG) access restrictions and can reject handover to the target eNB ID.

Closed subscriber group (CSG)

- CSGs are used to restrict a subscriber (UE) access to one or more cells of the public land mobile network (PLMN). The CSG access restriction uses a CSG identity that is assigned to a CSG HeNB. The MME imposes access restrictions based on the following information received from the HSS and eNB:
 - The CSG subscription data (CSG-Subscription-Data attribute-value pair (AVP)) of the UE subscription data received from the HSS. The CSG ID association with a PLMN is supported in Release 11. It is not supported by this feature. The MME considers whether CSG membership from the HSS is also applicable in the visited network (VPLMN) until the CSG membership in a PLMN is supported or not.
 - CSG ID and Cell Access Mode IEs in the following S1AP messages:
 - Initial UE Message
 - Handover Required
 - Path Switch Request

- CSG IDs supported by the HeNB are also sent in the S1 Setup message and changes to CSG ID list are sent in the eNB Configuration message. The MME uses the CSG ID list to filter paging messages if configurable CSG paging optimization in the MME is activated. The MME supports a maximum of 256 CSG IDs per eNB and 4 CSG IDs per subscriber. If configurable CSG paging optimization is activated in HeNB, the MME includes the UE valid and expired CSG ID in CSG ID list of the S1AP Paging message.

Cell access mode indicates to the MME whether the cell is a CSG cell or a hybrid cell. A CSG cell provides access only to members of the CSG ID supported by the CSG cell whereas a hybrid cell acts like a CSG cell for the members of CSG ID and at the same time provides access to all other UEs. A hybrid cell can provide preferential treatment to members of CSG. An open cell provides access to all the UEs.

Attach

If the initial Attach Request is received from a CSG cell, the MME uses CSG subscription data received from the HSS and CSG ID info received in the S1AP Initial UE Message to determine whether the UE subscribed to CSG of the cell and if subscribed, whether membership is expired or not. If the UE is not subscribed or membership has expired, the MME rejects the Attach Request with EMM cause Not authorized for this CSG (cause value #25) or provisioned cause code if the cause code is provisioned. For an emergency attach request, the MME does not do CSG restriction checks.

If the initial Attach Request is received from a hybrid cell, the MME sends CSG membership status to the eNB regardless of the CSG membership status in the Initial Context Setup Request message.

There are CSG restrictions on LIPA-enabled UEs, see the *Local IP access (LIPA)* feature.

Tracking area update (TAU)

If the UE initiates the TAU procedure at a CSG cell, the new MME checks whether the CSG ID and associated PLMN is contained in the CSG subscription and is not expired. If the CSG ID is not present or expired, the MME sends a TAU Reject message to the UE with evolved packet system mobility management (EMM) cause Not authorized for this CSG (cause value #25) or a provisioned cause value if a cause code is provisioned.

If the initial TAU Request is received from a hybrid cell and active flag is set, the MME sends CSG membership status to the eNB in Initial Context Setup Request message regardless of the CSG membership status.

Service request

If the UE initiates the service request procedure at a CSG cell, the MME checks whether the CSG ID and associated PLMN is contained in the CSG subscription and is not expired. If the CSG ID is not present or expired, the MME sends a Service Reject message to the UE with the EMM cause Not authorized for this CSG (cause value #25) or a provisioned cause value.

If a service request is received from a hybrid cell, the MME sends CSG membership status to the eNB in Initial Context Setup Request message regardless of the CSG membership status.

Paging optimization

The MME supports two global configuration flags for the CSG paging optimization: paging optimization in the MME and paging optimization in the HeNB.

If the CSG paging optimization in the MME is activated, the MME does not send paging message to CSG cells that are not in the UE's subscriber data. This paging optimization applies to all paging policies.

If the CSG paging optimization in HeNB is activated, the MME includes list of CSG IDs from the UE CSG subscription data in the paging message for all the macro eNBs including the HeNB GW. The MME includes both expired CSG IDs and valid CSG IDs in the CGS ID list.

The CSG ID list is never included for a directly connected HeNB because of security reasons.

See the *Local IP access (LIPA)* feature for the paging optimization used for traffic arriving on the LIPA PDN connection without mobility.

Paging optimization is not used for UEs with emergency bearers.

Paging optimization includes paging triggers because of the HSS, DDN, and SGs interface to the MSC/VLR.

Detach

If the MME receives a Detach Request through a CSG cell with the switch off parameter indicating that detach is not possible because of a switch off situation, and the CSG subscription for this CSG ID is absent or expired, the MME triggers an MME-initiated detach procedure as specified in the 3GPP TS23.401 clause 5.3.8.3. In this case, the MME sends the cause code #25 to the UE indicating that the UE is not authorized for this CSG.

X2 handover

The X2 handover is only possible between closed/hybrid HeNBs with the same CSG ID or if the target eNB is an open access eNB. However, the MME supports checks on the CSG ID received in the S1AP Path Switch Request message and takes action as follows:

- Case 1: The target cell is a CSG cell and the UE does not have any emergency bearer.
If the target CSG ID received in the Path Switch Request message is not in the UE's CSG subscription data or subscription has expired, the MME rejects the Path Switch Request by sending Path Switch Failure with an indication that the UE is not allowed to the CSG. If the UE has emergency bearers, the MME deactivates all other bearers except for the emergency bearer and sends Path Switch Ack messages with the emergency bearer included.
- Case 2: The target cell is a hybrid cell.
The MME does not do any access restriction but after sending the Path Switch Ack, the MME sends the S1AP UE Context Modification message if the UE membership status is changed.
- Case 3: An open access HeNB.
The MME does not do any checks.

S1 handover

In case of the S1 handover, it is the source MME that does CSG access controls. The source MME checks the UE's CSG subscription when the CSG ID is provided by the source eNB in the S1AP Handover Required message. If there is no subscription data for this CSG ID, the source MME rejects the handover by sending Handover Preparation Failure with cause value Invalid CSG ID. If the CSG subscription is expired, and the target cell is a CSG cell, the source MME rejects the handover by sending Handover Preparation Failure with cause value CSG subscription expiry. Additionally, the source MME includes the CSG ID in the Forward Relocation Request when the target cell is a CSG or hybrid cell. When the target cell is a hybrid cell, or if there are one or several emergency bearers and the target cell is a CSG cell, the CSG membership indication indicating whether the UE is a CSG member is also included in the Forward Relocation Request message. The target MME (or the source MME if there is no MME relocation) takes the following actions to support CSG:

- The target MME includes CSG ID IE and CSG Membership Indication IE in the S1AP Handover Request message if received in the Forward Relocation Request message.
- If the target eNB sends Handover Failure message with cause Invalid CSG ID, the MME sends Forward Relocation Response with cause Denied in radio access technology (RAT) to the source MME.
- The target MME includes user CSG information if the P-GW has requested and if the

configuration flag Support CSG change reporting is set in Create Session Request message or in Modify Bearer Request.

IRAT handover

This feature only supports the exchange of CSG related IEs on the S3 interface. The actions taken by the source and target MMEs are identical to the S1 handover except for the use of S10 messages. In this case, the S3 messages are used between the MME and SGSN. This feature proceeds with handover if the Gn interface is involved with the IRAT mobility (handover or TAU) in spite of lack of CSG related information.

This feature provides better LTE coverage.

7.2 20 bit Home eNB identifier (Feature m14003-01)

The 20 bit Home eNB identifier feature supports a use of 20 bit HeNB IDs of HeNB connected through gateway (GW). Basically, the MME supports routing of S1AP messages based on the tracking area identity (TAI) for target eNBs with 20 bit identifier that is not directly connected with the MME.

If the target ID received in an S1AP Handover Required (or S10/S3/Gn Forward Relocation Request) message is a 20 bit eNB ID, the MME first determines whether the target eNB is directly connected to the MME or not. If the eNB is directly connected, the MME sends the S1AP Handover Request message to the eNB. If the eNB is not directly connected, the MME sends the S1AP Handover Request message to the HeNB GW with TAI matching the target TAI received in the S1AP Handover Required message (or in the S10/S3/Gn Forward Relocation Request message).

The HeNB GW forwards the message to the target HeNB using the target eNB info in the Target to Source Container information element (IE) of the S1AP Handover Request message. The selection of the target HeNB GW based on the TAI imposes a restriction that TAI assigned to HeNB GW must be distinct to enable sending of the handover messages to one and only one HeNB GW. If there is no TAI matching the target TAI, the MME rejects the Handover Required message.

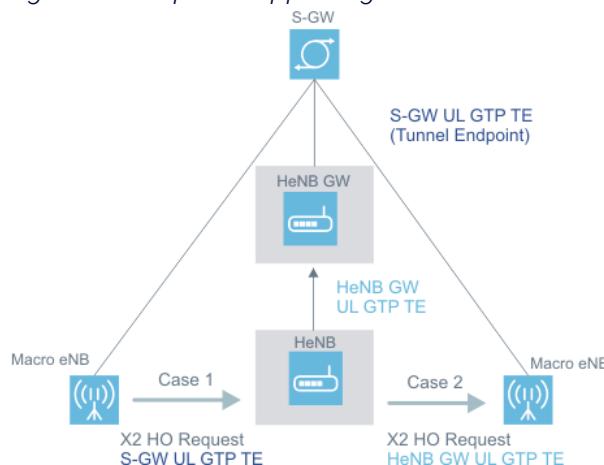
7.3 X2 HO between macro eNB/HeNB connected to a HeNB gateway (Feature m14002-01)

The X2 HO between macro eNB/HeNB connected to a HeNB gateway feature eliminates X2 handover failures between the macro eNB and Home eNB.

Before the implementation of this feature, the MME support of X2 handover between the macro eNB and the HeNB connected to a HeNB gateway (GW) is based on a proprietary solution because of a gap in 3GPP standards. However, these proprietary solutions cannot be used when operators buy an HeNB GW from one vendor and HeNBs from another vendor.

The figure shows the gaps in supporting X2 HO:

Figure 84: Gaps in supporting X2 handover



The macro eNB sends uplink (UL) data packets directly to the S-GW based on SGW UL GTP TE, or the HeNB sends UL data packets to the HeNB GW. The HeNB GW converts HeNB-GW UL GTP TE to SGW UL GTP TE, and forwards the data packets to the S-GW. There is an issue with UL GTP tunnel during Macro eNB->Indoor Metrocell X2 handover.

- Case 1: the HeNB must know HeNB-GW UL GTP TE
- Case 2: the macro eNB must know SGW UL GTP TE

This feature closes this gap to support X2 handover between the macro eNB and the HeNB connected to a HeNB by always including the UL tunnel IDs (E-RAB To Be Switched in Uplink List information element (IE)) in the S1AP Path Switch Request Acknowledge message.

Currently the IE is only included for X2 handover with the S-GW relocation.

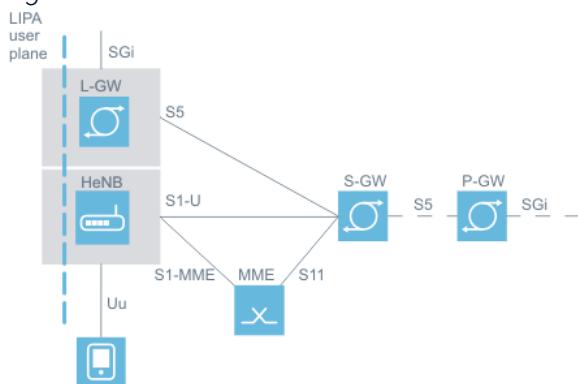
- Case 1: the HeNB GW uses the IE to set up mapping between the SGW UL GTP TE (Uplink GTP Tunnel Endpoint) and HeNB GW UL GTP TE to forward the S1-U traffic.
- Case 2: the macro eNB overwrites the UL GTP TE received from the HeNB GW with the UL GTP TE received in the S1AP Path Switch Request Acknowledge message.

7.4 Local IP access (LIPA) (Feature m14000-01)

The **Local IP access (LIPA)** feature allows the UE to directly access enterprise or residential networks without user plane data travelling through GWs.

The LIPA function enables an LTE UE connected through a HeNB to access other IP-capable entities (for example Internet) in the same residential or enterprise IP network without user plane mobile operators core network. The local IP access is achieved by using a local gateway (L-GW) collocated with the HeNB. The figure shows LIPA architecture.

Figure 85: LIPA architecture



Whether a UE is allowed or prohibited LIPA for an access point name (APN) at a cell is provided by LIPAPermission attribute-value pair (AVP) in APN Configuration AVP in UE subscription data and Service-Selection AVP of closed subscriber group (CSG) subscription data.

If a subscriber is roaming, the VPLMN-LIPA-Allowed AVP in UE subscriber data indicates to the MME to allow or prohibit LIPA in visited network (VPLMN) where the UE is attached. Additionally, the MME supports an option of overriding VPLMN LIPA allowed subscription data. This override is supported for each public land mobile network (PLMN) in the roaming agreement table.

The MME selection of a P-GW in core network or a local GW at the eNB is based on the eNB indication of LIPA support and user subscription data.

The eNB indicates to the MME that it supports LIPA by including GW Transport Layer Address information element (IE) in the S1AP Initial UE Message and S1AP Uplink non-access stratum (NAS) Transport message. This address is L-GW's S5 control plane address. If this indication is included in either of the messages, the MME verifies subscription data and CSG subscription data to allow the LIPA access.

If LIPA-Permission for an APN indicates LIPA-ONLY, the MME allows LIPA for that APN

through authorized CSG according to the CSG subscription data. If LIPA-Permission for an APN indicates LIPA-CONDITIONAL, the MME allows non-LIPA access if the eNB does not support LIPA access or for certain causes of L-GW create session failures. If the eNB supports LIPA, the MME allows LIPA through the authorized CSG cells according to the CSG subscription data. If the LIPA-Permission for an APN indicates LIPA-PROHIBITED, the MME does not allow LIPA access for the APN. If the LIPA-Permission AVP is not present for a specific APN, the MME does not allow LIPA access for the APN.

Once the MME selects a LIPA, the MME sends S11 Create Session Request message with P-GW S5/S8 Address for Control Plane IE set to the GW Transport Layer Address IE in the S1AP Initial UE Message and S1AP Uplink NAS Transport message. The S5/S8-U P-GW FTEID IE of the S11 Create Session Response is S5-U address of the L-GW and this address is sent in Initial Context Setup Request or in E-RAB Setup Request to eNB to establish direct user path to the L-GW.

Mobility of the LIPA connection is not supported. So, the LIPA packet data network (PDN) connection is released when the UE moves away from the eNB that is providing the LIPA. The LIPA PDN connection is released as follows for the handover:

- The eNB determines that the UE has a LIPA PDN by the presence of the Correlation ID in the UE evolved radio access bearer (E-RAB) context.
- The eNB requests the collocated L-GW to release the PDN connection using intra-node signaling.
- The L-GW then initiates release of PDN connection using the P-GW initiated bearer deactivation procedure as described in 3GPP TS 23.401 clause 5.4.4.1.

At the handover, the source MME checks whether the LIPA PDN connection has been released. If it has not been released:

- If the handover is a S1-based handover or an inter radio access technology (IRAT) handover, the source MME rejects the handover by sending S1AP Handover Preparation Failure message with cause value transport/unspecified.
- If the handover is an X2-based handover, the MME sends the Path Switch Failure message with the cause value transport/unspecified and detaches the UE with reattach required with cause #17 (network failure).

For the idle mode tracking area update (TAU) procedure, the source MME releases any LIPA PDN connections by sending the Delete Session Request if the UE has moved from the LIPA-enabled eNB. The MME considers that the UE moved to a different eNB if S1AP Initial UE Message does not contain the GW Transport Layer Address IE or the GW Transport Layer Address IE received in the S1AP Initial UE Message does not match the current GW Transport Layer Address. If the UE does not have any other PDN connection, the MME detaches the UE

with reattach required using cause # 40 (No EPS bearer context activated). In the case of MME relocation, the source MME sends international mobile subscriber identity (IMSI) not known in the S10 Context Response message.

7.5 LIPA enhancements (Feature f10927-02)

This feature supports MME switching UE LIPA-enabled PDN session(s) to L-GW when the UE in idle mode moves from Macro LTE coverage area into HeNB coverage area in the intra-MME TAU procedure. The MME deactivates the LIPA-enabled PDN session(s) to allow the PDN to be re-established on the L-GW. If the UE PDN connection is the last active PDN, the CMM detaches the UE with "re-attach required".

This enhances data traffic offload to local ISP rather than routing through operator core network as any data using the specified LIPA-enabled APN for LBO is offloaded. When a UE in idle mode moves)from a non-LIPA coverage area to a LIPA coverage area (HeNB coverage) in intra-MME TAU procedure and the UE has LIPA-enabled PDN connection(s) established, the MME deactivates LIPA-enabled PDN connection(s) to offload P-GW core network resources and re-establishes the PDN connection to a L-GW. If this is the last PDN connection, the MME detaches the UE with "re-attach required" to re-establish the LIPA-enabled PDN connection to a L-GW.

The feature is enabled by the global parameter `switchPdnToLipa`.

Note:

The MME determines UE presence in LIPA coverage area when it receives the GW Transport Layer Address IE in the initial UE message.

7.6 256 TAIs per eNB (Feature f10901-01)

The operator is able to introduce the femto eNB application where a large number of femto eNBs connects to the MME through a femto gateway.

In the framework that introduces eNB gateways for the femto cell concept support, the MME needs to support an extended number of tracking areas (TAs) for a number of eNBs.

For the eNBs that have the capability to support 256 tracking areas:

- If there is a single broadcast public land mobile network (PLMN) per each tracking area code (TAC), the MME supports a maximum number of 256 TACs per eNB, corresponding to 256 tracking area identities (TAIs).

- For multiple broadcast PLMNs per TAC, the supported number of TACs decreases accordingly, because the MME supports 256 TAIs (TAC and PLMN combination) in total.

7.7 Raising an alarm when a TAI is shared by two HeNB GWs (Feature f10903-01)

The *Raising an alarm when a TAI is shared by two HeNB GWs* feature supports raising an alarm when the MME attempts to send a handover request message to an indirectly connected HeNB using tracking area identity (TAI)-based routing of the message and the TAI is shared by two HeNB gateways (GWs)/eNBs.

The alarm helps operators to correct the situation.

Failure scenario

To initiate an S1HO, the source eNB sends a Handover Required message to the MME. That message contains the target Global eNB ID and the target Tracking Area Identity (TAI).

- If the target Global eNB ID is for a macro eNB (20-bit ID), there should be a direct S1 link to that eNB.
- If the target Global eNB ID is for a Home eNB (28-bit ID), there may be a direct S1 link to that HeNB, or (more likely) the connection may be indirect via a HeNB Gateway.
- If we have a direct S1 link to the target eNB (either macro eNB or HeNB), that S1 link is used (for example, to send Handover Request).

If the target eNB is a HeNB without a direct S1 link, the target TAI is used to index an internal table that maps TAIs to eNBs (or HeNB-GWs). (eNBs or HeNB-GWs sent the TAIs that they have been configured for to the MME when they initially set up their S1AP connection.) The TAI in this case should map to a unique HeNB-GW, as service providers should configure a unique TAI dedicated to each of their HeNB-GWs.

If there is more than one HeNB-GW or eNB using this TAI, the first one in the list is selected. It may or may not be the HeNB-GW actually desired, and the `mmeTAIENBMapping` alarm is raised to alert the service provider about the TAI/HeNB-GW misconfiguration.

Example: Investigating the error

Using the information in the alarm, the following command can be used to find the (H)eNB(-GW)s associated with the TAI of interest:

```
cmm taiEnbQuery list --taiMcc <tai> --taiMnc <mnc> --tac <tac>
```

Service providers would have to correct their TAI configurations on eNBs to correct this problem.

7.8 Non-standard HeNB GW selection (Feature f10905-01)

Non-standard HeNB GW selection feature is introduced to support routing of S1AP messages based on the 20 bit Macro eNB ID if the received HeNB ID type of the target ID is not directly connected with the MME.

Upon handing over from eNB to HeNB and MME configuration transfer messages, the TAI is not used. The eNB sends the Macro ID for a HeNB, and others send the HeNB ID, thus the MME uses the upper 20 bits of the Received ID to form a Macro ID and uses that to route to the HeNB GW. However, for inter-MME handover cases, the TAI is still used to select the target MME. The target MME uses the same mechanism to create the Macro ID.

MME provides global provisioning to enable and disable the *non-standard HeNB GW selection* feature. By default, this feature is disabled.

When the *non-standard HeNB GW selection* feature is enabled, the MME selection of target eNB is done as specified in the following:

- If the target eNB ID in the Handover Request message is 20 bit, MME selects target eNB from the directly connected eNB with the ID.
 - If the eNB is found, MME sends the Handover Request message.
 - If the eNB is not found, MME sends Handover Preparation Failure message.
- If the target eNB ID in the Handover Request message is 28 bit, MME selects target eNB from the directly connected eNB with the ID.
 - If the eNB is found, MME sends the Handover Request message.
 - If the eNB is not found, MME strips bottom 8 bits and selects target eNB from the directly connected eNB with the ID.
 - If the eNB is found, MME sends the Handover Request message.
 - If the eNB is not found, MME sends the Handover Request message to the first eNB found in the target TAI.
 - If the eNB is not found in either of these ways, MME sends Handover Preparation Failure message.

When this feature is disabled, the MME routes to a target eNB based on the TAI if no HeNB target ID (28 bit) is directly connected to the MME.

7.9 CMM support for release of active LIPA PDN connections (Feature f10927-01)

With this feature, the MME supports release of UE active local IP access (LIPA) PDN connections or ignores request for LIPA PDN connections when a subscriber is a lawful interception target.

The MME's behavior depending on the UE's ECM state at the time the UE is added at the LI target list is as follows:

- ECM CONNECTED case
 - If all PDN connections are LIPA, the MME will delete those bearers toward the S-GW/P-GW and will detach the UE with cause code 're-attach required'.
 - If some of the UE's PDNs are LIPA, the MME will delete the LIPA bearers toward the S-GW/P-GW and send e-RAB Release Command/NAS Deactivate EPS Bearer Context Request to the eNB/UE.
- ECM IDLE case
 - If all PDN connections are LIPA, the MME will delete those bearers toward the S-GW/P-GW and will implicitly detach the UE. Any subsequent procedure, apart from attach, will be rejected with the cause 'implicitly detached'.
 - If some of the UE's PDNs are LIPA, the MME will delete the LIPA bearers toward the S-GW/P-GW. No communication for the deleted bearers toward the UE is required (3GPP TS 23.401).

If for any reason an ECM IDLE UE that has become LI target still has active LIPA PDN connections at the time of Service or TAU Request, the MME will first delete those bearers toward the S-GW/P-GW and then process the Service/TAU Request.

If a UE that is LI target requests LIPA service

- during attach and the Initial UE Message containing the Attach Request includes the GW Transport Layer Address IE
- with NAS PDN Connectivity Request that includes the GW Transport Layer Address IE,

the MME ignores the IE in the message and proceeds with PDN connectivity/APN setup as per configured mode 1 or mode 2 selection (non-LIPA).

When a UE that is in the LI target list requests LIPA service for an APN with LIPA-ONLY LIPA-Permission, the MME rejects the Attach/Standalone PDN Connectivity Request with EMM CC #19 (ESM Failure) and ESM CC #34 (Service option temporarily out of order).

The MME pegs an existing LIPA PM count, **LIPA PDN CONNECTION RELEASES DUE TO MOBILITY**, when PDN connection is released due to UE becoming a LI target.

This feature is controlled by the global parameter `allowLIPAPDNWhenLITarget` (by default set to `No`).

7.10 MME support for restrict LIPA service for DCNR capable UE(s) (Feature f10927-03)

The MME restricts dual connectivity new radio (DCNR) capable UEs with the allowed DCNR service from the local IP access (LIPA) service.

Non-DCNR EUTRAN-NR dual connection (EN-DC) UEs are assigned via the L-GW, if allowed in the subscription, but DCNR UEs are assigned via P-GWs to ensure LIPA and EN-DC feature coexistence. This is done during attach and PDN connectivity request procedures. This function is controlled by the global parameter `dcnrOverrideLipa`.

For Gn-based or S10-based inter-node idle mode TAU with DCNR capable UEs, when the MME determines that the NR is not allowed for the UE as a secondary RAT and the HSS sends the UE subscription data to the MME, the MME releases the PDN. If this is the last PDN, the MME rejects the TAU message with "re-attach required". If this is not the last PDN, the MME responds with the TAU Accept message and the EPS Bearer Status indication for the released PDN. This applies to all DCNR users not just LIPA users, and this function is controlled by the global parameter `pdnReleaseNrSecRatRestriction`.

7.11 MME support for CSG ID enhancements (Feature f10906-03)

With this feature, the MME supports up to 10 CSG IDs from the subscription data. This change is reflected in all the messages in the CSG subscription data from the HSS like the ULA, IDR, or DSR.

8. Multimedia broadcast multicast services

Multimedia broadcast multicast services (MBMS) in the LTE is a broadcast service in which data is transmitted from a single source entity to multiple recipients.

Transmitting the same data to multiple recipients allows network resources to be shared. The MME provides a distribution of control messages associated with broadcast session start/update/stop through the Sm (GTPv2) interface to the MBMS gateway and the M3 (SCTP) interface to the multicast coordination entity (MCE) in the eNB nodes.

8.1 Multimedia broadcast/multicast service (MBMS or eMBMS) (Feature m11007-01)

With Multimedia broadcast/multicast service (MBMS or eMBMS) feature, content (for example, IP TV) can be broadcast over LTE access to multiple receivers or UEs in an MBMS service area. Network resources are used in an efficient manner as the same data is transmitted as broadcast to multiple receivers/UEs and not via traditional unicast bearers.

This feature supports Multimedia Broadcast/Multicast Service (MBMS or eMBMS) as defined in 3GPP TS 23.246.

To enable MBMS support for E-UTRAN, the MME:

- provides session control of MBMS bearers to the E-UTRAN access (including reliable delivery of Session Start/Session Stop/Session Update to E-UTRAN).
- determines the eNB nodes that are in the MBMS broadcast service area and transmits session control messages towards appropriate/multiple E-UTRAN nodes over the M3 interface.
- provides an Sm interface to the MBMS gateway (GW) function: it receives MBMS service control messages and the IP multicast address for MBMS data reception from the MBMS GW function over the Sm interface.



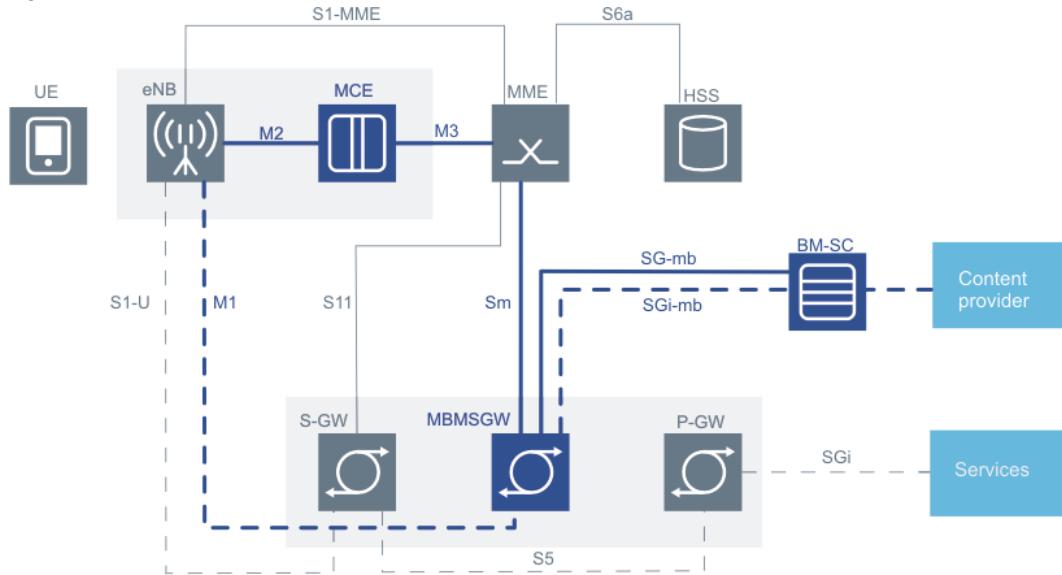
Note:

When a UE leaves or enters MBMS bearer coverage, the service continuity is handled by the service layer (in the UE and network).

Note:

Multicast is not applicable for E-UTRAN networks.

Figure 86: MBMS network architecture



Note:

The multicast coordination entity (MCE) is assumed to be within the E-UTRAN in the diagram.

It is the role of the MCE to initialize the M3 SCTP association with the MME. The MME sends MBMS M3AP message to only those MCEs that have initialized an M3 SCTP association. Thus, each MCE can, depending on SCTP association initialization, be M3- connected to one, two, or all the MMEs in an MME pool.

This feature is activated on the MME using an on/off switch on the provisioning interface.

There are three main events that can happen within an MBMS session:

- Session start
- Session update
- Session stop

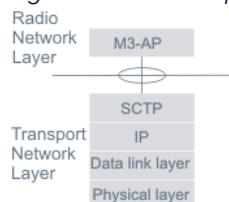
All three events are triggered by an SM message from the MBMS GW and result in the MME distributing messages out to the MCE(eNB).

M3 application protocol (M3AP) for MBMS

The E-UTRAN MBMS architecture consists of a set of MCE(eNB) nodes connected to the MME through the M3 interface. The M3 interface is specified at the boundary between the evolved packet core (EPC) and the E-UTRAN. From the M3 perspective, the E-UTRAN access point is an eNB, and the EPC access point is the control plane MME logical node. Bearer traffic for broadcasting routes directly from the MBMS GW to the MCE(eNB).

The M3AP messages between an eNB and the MME are transported over SCTP/IP.

Figure 87: M3AP protocol stack



The M3AP supports the signaling control functions:

- Session management for starting, stopping, and updating MBMS sessions
- Reset functionality to ensure a well-defined initialization on the M3 interface
- Error indication functionality to allow a proper error reporting and handling in cases where no failure messages are defined.

3GPP TS 36.444 defines the M3AP elementary procedures and the messages used in them. Elementary procedures are units of interaction between an eNB and the MME. They are intended to be used as building blocks to build up complete signaling sequences. An elementary procedure consists of an initiating message and possibly a response message.

Two types of elementary procedures, class 1 and class 2, are defined:

- Class 1: elementary procedures with response (success or failure or both)
- Class 2: elementary procedures without response

For a class 1 elementary procedure, the sender starts a timer after it sends the initiating message. If the sender does not receive a response message before the timer expires, the sender considers the elementary procedure as unsuccessful. For a class 2 elementary procedure, the sender considers the elementary procedure as always successful.

The SCTP association is initiated from the MCE(eNB).

The MME supports handling of unknown, unforeseen, or erroneous protocol data on the M3AP interface as specified in 3GPP TS 36.444 (36.413) section 10.

The MME supports the following elementary procedures for the M3AP interface.

Table 56: Class 1 elementary procedures (M3AP)

Elementary procedure	Initiating message	Successful outcome	Unsuccessful outcome
		Response message	Response message
MBMS session start	MBMS SESSION START REQUEST	MBMS SESSION START RESPONSE	MBMS SESSION START FAILURE
MBMB session stop	MBMB SESSION STOP REQUEST	MBMS SESSION STOP RESPONSE	
MBMB session update	MBMB SESSION UPDATE REQUEST	MBMS SESSION UPDATE RESPONSE	MBMS SESSION UPDATE FAILURE
Reset	RESET	RESET ACKNOWLEDGE	

Table 57: Class 2 elementary procedures

Elementary procedure	Message
Error indication	ERROR INDICATION

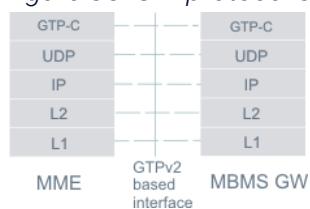
The procedures, messages, and information elements (IEs) are supported as specified in 3GPP TS 36.444.

Sm Interface for MBMS

The MBMS gateway is connected to the MME through the Sm interface.

The Sm application protocol supports the signaling/control functions. The signaling functions include session management: starting, stopping, and updating MBMS sessions.

The lower layers of the Sm protocol stack are shown in the figure.

Figure 88: Sm protocol stack lower layers

3GPP TS 29.274 defines the Sm elementary procedures and the messages used in these

procedures. An elementary procedure is a unit of interaction between an MBMS GW and the MME. These elementary procedures are intended to be used as building blocks to build up complete signaling sequences. An elementary procedure consists of an initiating message and possibly a response message. On this interface, the MBMS GW is always the initiating system sending the request message and the MME replies with the response message.

Up to 16 Sm interfaces are supported.

Note:

16 is based on up to 8 public land mobile networks (PLMN)s sharing the MME, each with a primary and backup MBMS GW.

The MME listens for Sm messages on User Datagram Protocol (UDP) port 2123 and responds to the source port in the triggering message.

The MME supports:

- Sm link management (for example, echo) as specified in 3GPP TS 29.274 section 7.1.
- reliable delivery of Sm messages as specified in 3GPP TS 29.274 section 7.6.
- handling of unknown, unforeseen, or erroneous protocol data on the Sm interface as specified in 3GPP TS 29.274 section 7.7.

In addition, these errors and the errored message are logged in the MME signaling log.

The following elementary procedures are supported for the Sm interface.

Table 58: Class 1 elementary procedures (Sm)

Elementary procedure	Initiating message	Successful outcome	Unsuccessful outcome
		Response message	Response message
MBMS session start	MBMS SESSION START REQUEST	MBMS SESSION START RESPONSE	MBMS SESSION START RESPONSE (error cause value)
MBMB session stop	MBMB SESSION STOP REQUEST	MBMS SESSION STOP RESPONSE	
MBMB session update	MBMB SESSION UPDATE REQUEST	MBMS SESSION UPDATE RESPONSE	MBMS SESSION UPDATE RESPONSE (error cause value)

The MME supports:

- receipt of the Sm MBMS Session Start Request message with a mandatory, conditional, and optional IE as specified in *3GPP TS 29.274 section 7.13.1*.
- sending the Sm MBMS Session Start Response message with a mandatory, conditional (excepting those for Sn), and optional IE as specified in *3GPP TS 29.274 section 7.13.2*.
- receipt of the Sm MBMS Session Update Request message with a mandatory, conditional, and optional IE as specified in *3GPP TS 29.274 section 7.13.3*.
- sending the Sm MBMS Session Update Response message with a mandatory, conditional (excepting those for Sn), and optional IE as specified in *3GPP TS 29.274 section 7.13.4*.
- receipt of the Sm MBMS Session Stop Request message with a conditional and optional IE as specified in *3GPP TS 29.274 section 7.13.5*.
- TMGI as an optional IE.
- sending the Sm MBMS Session Stop Response message with a mandatory and optional IE as specified in *3GPP TS 29.274 section 7.13.6*.

On receipt of any Sm MBMS message when the MBMS feature is off for the PLMN identified in the TMGI IE, the MME silently discards the message and records the event and message contents in the signaling log.

Session start procedure

The MME supports the MBMS session start procedure for the E-UTRAN as described in *3GPP TS 23.246 section 8.3.2*.

The MME sends the M3 MBMS Session Start Request to all MCE(eNB)s with an active M3 SCTP association.

Table 59: Sm to M3 information element mapping for session start procedure

IE in incoming Sm MBMS Session Start Request	IE in outgoing M3 MBMS Session Start Request
Not in IE, locally derived in MME	MME MBMS M3AP ID
TMGI	TMGI
MBMB Session ID (conditional)	MBMS Session ID (optional – include if available)
QoS Profile – QCI and GBR	MBMS E-RAB QoS Parameters
MBMS Session Duration	MBMS Session Duration
MBMS Service Area	MBMS Service Area
Provisioned Value – minTimeToMBMSdataTransfer	Minimum Time to MBMS Data Transfer
MBMS IP Multicast Distribution	Transport network layer (TNL) Information

The MME responds to the MBMS GW with the Sm MBMS Session Start Response without waiting for responses from the MCE(eNB)s. The Cause IE for the successful case is set to Request accepted.

The Recovery IE is included if this is the first contact with this MBMS GW.

The MME stores dynamic data associated with each broadcast session. This data is referred to as the MBMS bearer context in standards.

The MME supports the Sm MBMS session start procedure error cases where the message is received at the MME but cannot be handled or parsed by the MME. The MME responds to the MBMS GW with Sm MBMS Session Start Response with cause values as follows:

- System failure, if the MME is unable to handle the procedure because of system or interface state or operational issues (including all M3 links unavailable)
- No resources available, if the MME is in overload and this MBMS message is being dropped
- Mandatory IE incorrect
- Mandatory IE missing
- Invalid message format

The MME logs the received request and sent response Sm messages in error cases in the signaling log.

On receipt of M3 MBMS Session Start Response from the MCE(eNB)(s) to which the MBMS

Session Start Request was sent, the MME updates the MBMS bearer context with the MCE MBMS M3AP ID for each MCE(eNB) responding with successful status.

If one or more MCE(eNB)s fail to positively acknowledge the MBMS Session Start Request (responds with an MBMS Session Start Failure, Error Indication or the response times out), the MME removes these MCE(eNB)s from the MBMS bearer context for this broadcast.

In addition, the MME records the MCE(eNB) ID and contents of the failure or error indication or time-out event in the signaling log.

Session stop procedure

The MME supports the MBMS session stop procedure for the E-UTRAN as described in 3GPP TS 23.246 section 8.5.2.

On receipt of a non-error case Sm MBMS Session Stop Request from the MBMS GW.

- The MME populates and sends an M3 MBMS Session Stop Request with the MME MBMS M3AP ID and MCE MBMS M3AP ID information elements to each MCE(eNB) that is part of the broadcast per the MBMS bearer context.
- The MME responds to the MBMS GW with the Sm MBMS Session Stop Response with cause Request accepted.
- On receipt of the M3 Session Stop Response (or time-out for that response), the MME releases the MBMS bearer context for this broadcast.

The MME supports the Sm MBMS session stop procedure error cases where the message is received at the MME but cannot be handled or parsed or the MBMS session is not found by the MME. The MME responds to the MBMS GW with Sm MBMS Session Stop Response with cause values as follows:

- System failure (this includes the case where the broadcast service area does not map to any connected eNBs)
- Context not found, if Flow Identifier is not found in MBMS bearer context
- No resources available, if the MME is in overload and this MBMS message is being dropped
- Mandatory IE incorrect
- Mandatory IE missing
- (Needed) Conditional IE missing (MBMS Flow ID is missing)
- Invalid message format

The MME logs the received request and sent response messages in error cases in the signaling log.

If one or more MCE(eNB)s fail to positively acknowledge the MBMS Session Stop Request (the response times out), the MME still removes the MBMS bearer context for that eNB and records the MCE(eNB) response time-out in the signaling log.

Session update procedure

MBMS session update procedure for the E-UTRAN is supported as described in *3GPP TS 23.246 section 8.8.4*.

The MME finds the MBMS bearer context through F-TEID (if available) or TMGI and MBMS Session ID (if available).

The MME sends the M3 MBMS Session Update Request to all MCE(eNB)s with an active M3 SCTP association.

The MME uses the following Sm IE to M3 IE mapping.

Table 60: Sm IE to M3 IE mapping

IE in incoming Sm MBMS Session Update Request	IE in outgoing M3 MBMS Session Update Request
Locally in MBMS Bearer Context	MME MBMS M3AP ID
Locally in MBMS Bearer Context	MCE MBMS M3AP ID
TMGI	TMGI
MBMB Session ID (conditional)	MBMS Session ID (optional – include if available)
Quality of service (QoS) Profile – QoS class indicator (QCI) and guaranteed bit rate (GBR)	MBMS evolved radio access bearer (E-RAB) QoS Parameters

The MME responds to the MBMS GW with the Sm MBMS Session Update Response without waiting for responses from the MCE(eNB)s. The Cause IE for the successful case is set to Request accepted.

The MME supports the Sm MBMS session update procedure error cases where the message is received at the MME but cannot be handled or parsed or the MBMS session is not found by the MME. The MME responds to the MBMS GW with Sm MBMS Session Update Response with cause values as follows:

- System failure (this includes the cases where the MME is in such a state or condition that it cannot process the update or the broadcast service area does not map to any connected eNBs)

- Context not found, if session is not found in MBMS bearer context
- No resources available, if the MME is in overload and this MBMS message is being dropped
- Mandatory IE incorrect
- Mandatory IE missing
- (Needed) Conditional IE missing (Sender F-TEID and MBMS Session ID are missing)
- Invalid message format

The MME logs the received request and sent response messages in error cases in the signaling log.

Reset procedure

In the event of failure at the MME which results in the loss of some or all MBMS bearer contexts, the MME sends a M3 Reset message to those MCE(eNB)s for which the information is lost with the following cause values.

- Hardware failure: board failure that results in lost MBMS bearer context
- O&M intervention: O&M action that results in lost MBMS bearer context
- Unspecified failure: all other cases

The MME sets the reset type to

- Reset all, if all MCE(eNB)s are being reset because of loss of all MBMS data
- MME MBMS M3AP ID and MCE MBMS M3AP ID, if only specific broadcasts/MCE(eNB)s are affected.

The MME deletes the MBMS bearer context associated with the reset links/broadcast session.

In the event of receipt of M3 Reset from an MCE(eNB), the MME removes that MCE(eNB) from the MBMS bearer context for the indicated session or all sessions for that MCE/eNB if reset type is Reset all.

The MME responds with an M3 Reset Acknowledge with the MME MBMS M3AP ID and MCE MBMS M3AP ID if a specific broadcast session was identified in the Reset message.

The MBMS bearer context information survives normal maintenance activities and board switchovers.

The MME periodically cleans up MBMS bearer context for which the MBMS session duration has expired but was not cleaned up due to missing MBMS Session Stop handling.

3GPP CRs applied to MBMS functionality

- *CR – 0025 (36.444)*: Correction of MCCH update synchronization mechanism
- *CR#1114 (29.274)*: Absolute time for MBMS data transfer start and stop
- *CR – 0269 (23.246)*: MBMS data transfer time
- *CR-0268 partial support*: Service area filtering complies with Rel 9 (3GPP TS 23.246) MBMS corrections (for example, ARP usage, GBR for MBMS bearer service). This CR introduces changes to the usage of allocation retention priority (ARP) in Release 10. This has no MME impact since the MME simply forwards ARP values it receives from the MBMS GW. The CR also introduces service area filtering. This is a new functionality agreed from 3GPP Release 11 onwards. The MME complying with Release 9 broadcasts the MBMS signaling towards all MCEs, each MCE being in charge of service area filtering. From Release 11 onwards, the MME performing service area filtering sends the MBMS messages only to the MCEs serving the corresponding service area. In addition, the CR also introduces changes to *section 8.3.2 MBMS Session Start Procedure for E-UTRAN and UTRAN for EPS call flow items 4 and 6* that has impact on the MME along with *section 8.8.4 items 4 and 6* which the MME is supporting.
- *CR – 0988 (29.274)*: Recovery IE in MBMS Session Stop Response message
- *CR – 1047 (29.274)*: C-TEID in MBMS IP Multicast Distribution IE
- *CR-0268 (23.246)*: MBMS corrections (for example, ARP usage, GBR for MBMS bearer service). This feature covers the part of the CR related to service area filtering, a functionality agreed from 3GPP Release 11 onwards.
- The MME complies with Release 9, and broadcasts the MBMS signaling towards all MCEs, each MCE being in charge of service area filtering.
- From Release 11 onwards, an MME performing service area filtering sends the MBMS messages only to the MCEs serving the corresponding service area.
- In addition, the CR also introduces changes to the *section 8.3.2 MBMS Session Start Procedure for E-UTRAN and UTRAN*. The list of downstream nodes of BM-SC and the list of MBMS control plane nodes (MMEs and SGSNs) of MBMS GW are achieved in the following ways:
 - The list of MBMS control plane nodes for MBMS GW is sent from the BM-SC to the MBMS GW in the Session Start Request.
 - Normally, the MBMS GW contained in the List of downstream nodes for BM-SC is the default MBMS GW (or two for resilience).

Additional MBMS functionality:

- The MME supports filtering the distribution of MBMS session /control signaling based on the MBMS service area when connected to multiple MCEs to avoid overflowing E-UTRAN nodes with unnecessary signaling.

- The MME stores the session attributes and the identifier of the eNBs/RNCs as the List of downstream nodes parameter in its MBMS bearer context and responds to the MBMS GW. The MME returns a MBMS Session/Start Response to the MBMS-GW as soon as the session request is accepted by one E-UTRAN node.

Requirements

This feature requires support in the UE and the E-UTRAN/eNB (including MCE). The MBMS GW and the BM-SC are required.

Related descriptions

- MME support for MBMS

8.2 MBMS restoration (Feature m11007-04)

The **MBMS restoration feature ensures re-establishment of the evolved multimedia broadcast/multicast service (eMBMS) service even in case of complete evolved packet core (EPC) nodes failure (multicast coordination entity (MCE); MME; BM-SC, MBMS gateway (GW)) for eMBMS service.**

MBMS Restoration specification 3GPP TS 23.007 has introduced several Release 12 CRs related to restoration of MBMS. This feature provides support for Release 11 and 12 MBMS restoration procedures.

- 0220r1: MME/SGSN behavior upon MBMS GW restart
- 0221r1: eMBMS service restoration upon MCE failure or M3 application protocol (M3AP) path failure
- 0222r1: eMBMS service restoration upon MME/SGSN restart
- 0223r2: Sm path failure handling
- 0228: Trigger for re-establishing MBMS sessions upon an M3AP path recovery
- 0231r2: SGmb path failure
- 0232r: Contents of MBMS Session Start Request when re-establishing MBMS sessions
- 0246r1: MBMS Session Start Request received for an ongoing MBMS bearer service
- 0250r1: Release of resources at old MME/SGSN during transient Sm path failure
- 0259: M3AP path recovery
- 0266r2: Non-transient SGmb path failure

The MME also supports the structure of MBMS service area identifier (SAI) as specified in

3GPP TS 23.003 section 15.3 (MBMS SAI decimal number between 0 and 65 535).

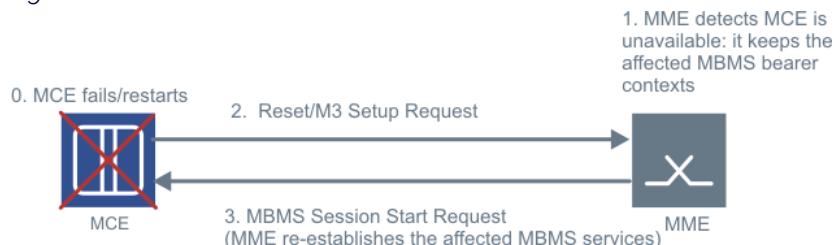
The MME also supports 3GPP TS 23.246 transmit session control messages towards the necessary E-UTRAN nodes to ensure the distribution of content from ongoing MBMS sessions,

- if the MCE sets up (or restarts) an M3AP connection with the MME by applying the MCE failure procedure specified in 3GPP TS 23.007.
- if the MCE modifies the list of MBMS service areas it serves by triggering the MCE configuration update procedure.

MCE failure/restart

The MME that recognizes unavailability of an MCE (for example, no more Stream Control Transmission Protocol (SCTP) association in service) or receives a Reset or a M3 Setup Request message from an MCE, maintains the related MBMS bearer contexts but locally deletes the MCE-related information (M3-related resources) for all MBMS service associations or those indicated in the Reset message.

Figure 89: MCE failure/restart



Upon a receipt of a Reset or M3 Setup Request message from the MCE, the MME re-establishes the MBMS bearer services affected by the MCE failure by initiating MBMS session start procedure towards the MCE.

In the MBMS Session Start Request:

- The MME sets a new MBMS session re-establishment indication flag to signal that this message is used to re-establish an MBMS session if (and only if) the MME has received recently an MBMS session re-establishment indication from the MBMS GW.
- The MME sets the estimated session duration to the remaining duration of the session.
- The MME can change the relative start time to speed the restoration process (centralized MCE architecture).

The MCE is able to accept an absolute start time in the past.

In case of a partial MCE failure, the MCE releases MBMS services affected by the failure

either immediately or after a pre-configured period if the corresponding MBMS bearer services are not re-established through any MME.

For further details, see *3GPP TS 23.007 sub clause 15A.3 3GPP CR#: 0220*.

M3AP path failure/recovery

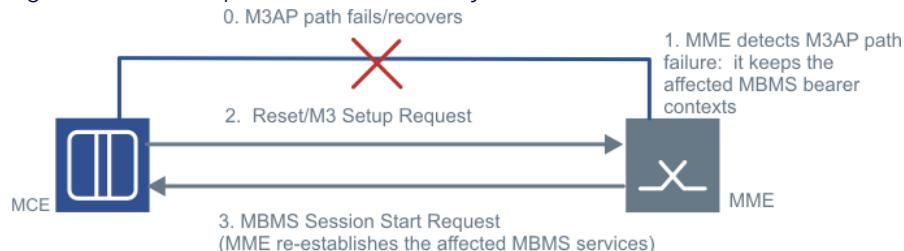
Upon the detection of an M3AP path failure (that is, no more SCTP association in service):

- The MCE releases all the MBMS services affected by the M3AP failure locally and towards E-UTRAN either immediately or after a pre-configured time if the corresponding MBMS bearer services are not re-established through any MME. In the latter case, the MCE accepts MBMS Session Start Request received from the same MME without the re-establishment flag for an ongoing MBMS session during that period.
- The MME maintains the related MBMS bearer contexts but locally deletes the MCE-related information (M3-related resources) for all MBMS service associations.

Upon the recovery of the M3AP path, the MCE initiates a reset or M3 setup request procedure towards the related MME.

Upon the receipt of a Reset or M3 Setup Request message, the MME re-establishes the MBMS bearer services affected by the MCE failure by an initiating MBMS session start procedure towards the MCE.

Figure 90: M3AP path failure/recovery



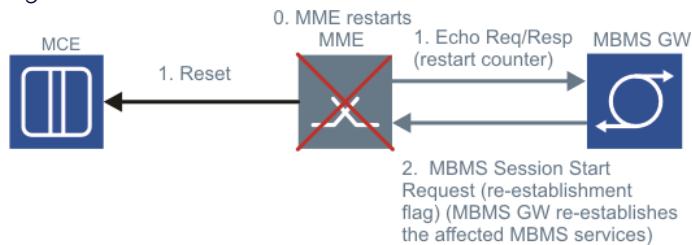
The same rules apply for encoding the MBMS Session Start Request as MCE failure/restart.

The MCE is able to accept an absolute start time in the past.

For further details, see *3GPP TS 23.007 sub clause 15A.4 3GPP CR#:0266*.

MME restart

The MME can send an M3 Reset message to MCEs (if the restart event has resulted in loss of some or all M3 transactions reference information).

Figure 91: MME restart

The MCE deactivates all the related MBMS bearer contexts locally and towards E-UTRAN either immediately or after a pre-configured time if the corresponding MBMS bearer contexts are not re-established through an MME. In the latter case, the MCE accepts MBMS Session Start Request received from the same MME without the re-establishment flag for an ongoing MBMS session during that period.

When the MBMS GW detects a restart in the MME (incremented MME restart counter), the MBMS GW re-establishes the active MBMS bearer services affected by the MME restart by initiating MBMS session start procedure towards the restarted MME (or an alternative MME in the same MME pool).

In the MBMS Session Start Request:

- The MBMS GW sets a new MBMS session re-establishment indication flag to signal that this message is used to re-establish an MBMS session.
- The MBMS GW sets the estimated session duration to the remaining duration of the session.
- The MBMS GW can change the relative start time to speed the restoration process (centralized MCE architecture).

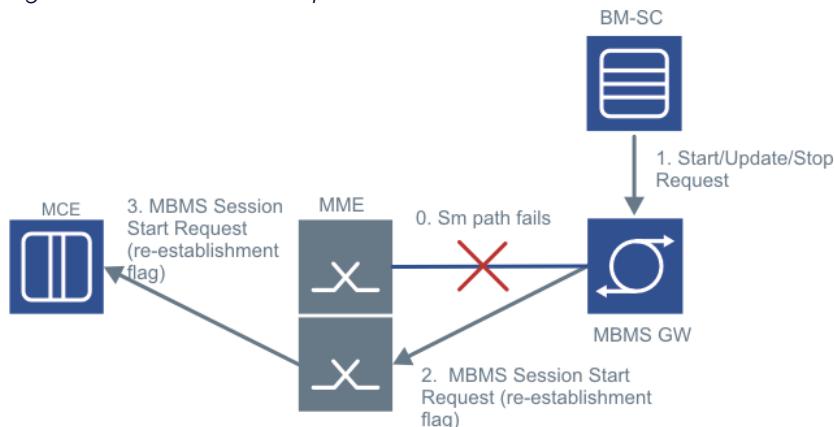
For further details, see 3GPP TS 23.007 sub clause 14.1.1.

Transient Sm path failure

The MBMS GW is provisioned with the (sub)list of MMEs of the MME pool supporting the MBMS.

Upon detecting a Sm path failure, the MME and MBMS GW maintain the affected MBMS bearer contexts.

Figure 92: Transient Sm path failure



- The MBMS GW sends new MBMS Session Start Request (from BM-SC) to different MMEs.
- Upon receipt of MBMS Session Update/Stop Requests from BM-SC, MBMS GW moves the control of the MBMS session to a new MME (by sending an MBMS Session Start Request) and then sends the Update/Stop Request through the new controlling MME.

The same rules apply for encoding the MBMS Session Start Request as for the MME restart.

The MCE accepts a MBMS Session Start Request received for an ongoing MBMS session (same TMGI) from a different MME than the MME that currently controls the MBMS session if the message includes the MBMS session re-establishment indication flag.

The MCE replaces the M3-related resources for this MBMS service associated to the previous MME by those associated to the new MME and considers that the MBMS session is now being controlled by the new MME.

For further details, see 3GPP TS 23.007 sub clause 20.2.3.1, 20.2.4 3GPP CR#:0231.

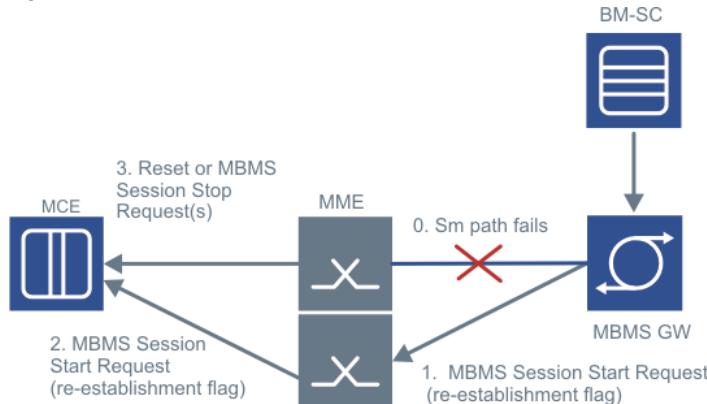
Non-transient Sm path failure

Upon detecting a non transient Sm path failure, the MME behaves as if MBMS GW had restarted and deactivates sessions locally and in MCEs.

The MBMS GW considers that the MME has released MBMS sessions. No Stop Requests are sent towards the old MME.

The MBMS GW can move the control of all the affected active MBMS sessions to another MME in the same MME pool (if any other MME is reachable by the MBMS GW) by initiating a new MBMS Session Start Request(s) to alternative MME(s).

Figure 93: Non-transient Sm path failure



The maximum path failure duration timer should be configured with a shorter value in the MBMS GW than in the MME (shorter by at least the period between 2 GTP-C Echo Requests) to avoid interrupting active MBMS sessions upon a non-transient Sm path failure. The Reset or MBMS Session Stop from old MME arrives after the new MBMS Session Start from the new MME and does not affect the MBMS sessions.

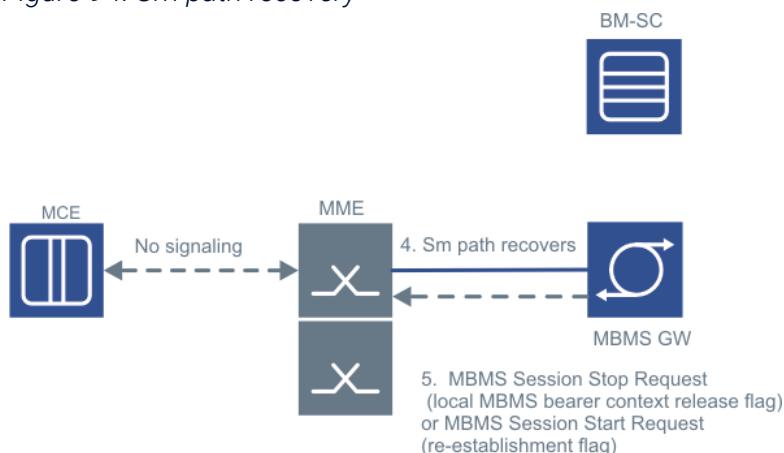
The same rules apply for encoding the MBMS Session Start Request as for the MME restart.

For further details, see 3GPP TS 23.007 sub clause 20.2.3.1, 20.2.4 3GPP CR#: 0250.

Sm path recovery

The MBMS GW determines whether the Sm path failure has been transient from the MME perspective. The MBMS GW is provisioned with the maximum path failure timer of the MME.

Figure 94: Sm path recovery



If the Sm path failure is transient from the MME perspective, and if the MBMS GW has already moved the control of the MBMS session to an alternative MME, the MBMS GW sends an MBMS Session Stop Request message to the MME previously controlling the MBMS.

session with a Local MBMS bearer context release indication to instruct the MME to release its MBMS bearer context locally, without sending any message to the MCE(s).

If, however, the MBMS GW has not yet moved the control of the MBMS session to an alternative MME (for example, if the MBMS restoration procedures are not supported in the network):

- If the Sm path failure is transient from the perspective of the MBMS GW, the MBMS GW considers that MBMS session is still controlled by the related MME and proceeds as if there had been no Sm path failure.
- If the Sm path failure is non-transient from the perspective of the MBMS GW, the MBMS GW sends a MBMS Session Start Request to the MME for the session.

For further details, see *3GPP TS 23.007 subclause 20.2.3.1, 20.2.4 3GPP CR#: 0231*.

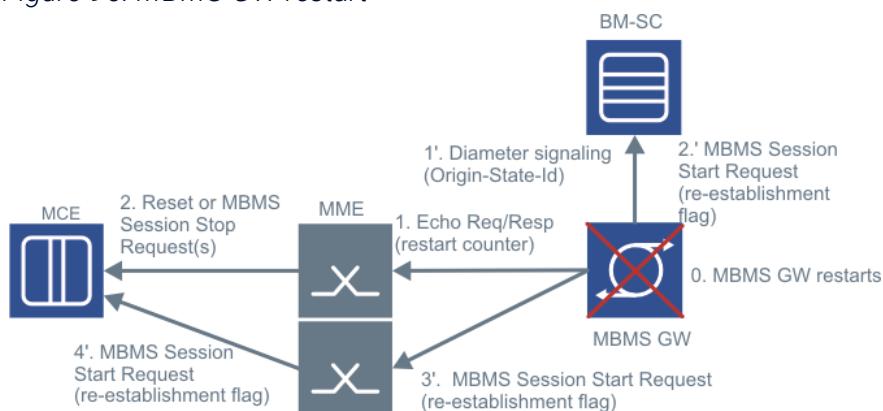
MBMS GW restart

Bearer contexts in the MBMS GW affected by the failure are lost. SGmb Diameter sessions affected by the restart are also lost.

Upon detecting the MBMS GW restart (incremented MBMS GW restart counter), the MME deactivates all related MBMS bearer contexts locally and in the (E-)UTRAN.

The MME initiates a M3AP reset procedure, or an MBMS session stop procedure per affected MBMS service towards the MCE(s).

Figure 95: MBMS GW restart



Upon detecting the MBMS GW restart, the BM-SC maintains the related MBMS bearer contexts and re-establishes the active MBMS bearer services affected by the restart towards the restarted MBMS GW (or an alternative MBMS GW). The MBMS GW re-establishes the session through the same or a different MME.

The eNB leaves the former M1 IP multicast group and joins the new one if the M1 resources

are modified (for example, session re-established through a different MBMS GW).

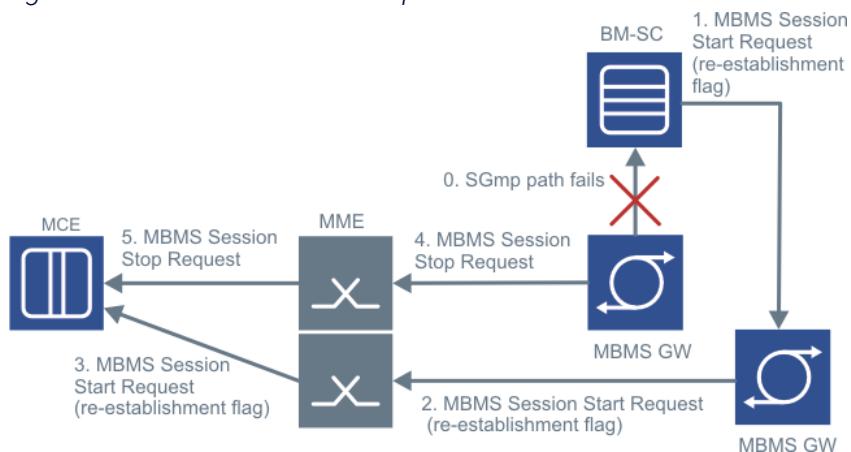
For further details, see *3GPP TS 23.007 subclause 17A.1 3GPP CR#: 0239*.

Non transient SGmb path failure

Upon detecting a non-transient SGmb path failure, the MBMS GW deactivates all the related MBMS bearer contexts locally and sends MBMS Session Stop Requests towards all MMEs in which the MBMS bearer services are active.

The BM-SC considers all related MBMS bearer contexts as terminated in the MBMS GW.

Figure 96: Non-transient SGmb path failure



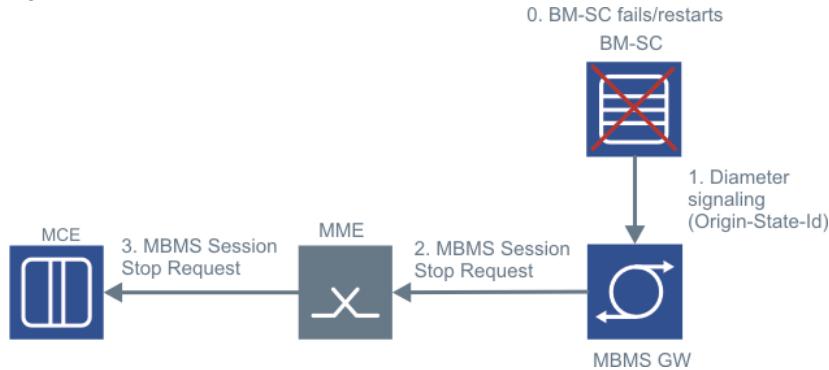
The BM-SC then re-establishes the active MBMS bearer services affected by the SGmb path failure by initiating MBMS session start procedure(s) towards an alternative MBMS GW (if available) or towards the same MBMS GW (once the SGmb path is recovered).

For further details, see *3GPP TS 23.007 subclauses 20.2.3.3/20.2.6.1 3GPP CR#:0266*.

BM-SC failure/restart

Upon detecting a BM-SC restart, the MBMS GW deactivates all the related MBMS bearer contexts locally and sends MBMS Session Stop Requests towards all MMEs in which the MBMS bearer services are active.

Figure 97: BM-SC failure/restart



For further details, see 3GPP TS 23.007 subclauses 17A.1.3 / 17D.1 3GPP CR#: 0237.

MBMS flags for MBMS restoration procedures

The MBMS session re-establishment indication flag (CR#:0404) signals that an MBMS Session Start Request is used to re-establish an MBMS session, over the SGmb, Sm, and M3AP interfaces.

- The MCE accepts an MBMS Session Start received for an already existing MBMS session from the same or another MME if it includes the MBMS session re-establishment indication.
- The MCE rejects an MBMS Session Start Request received without the flag for an ongoing session (this can be because of some misconfiguration at the BM-SC, for example), except if it supports the option to maintain MBMS sessions during a pre-configured time after an MCE, M3AP, or MME failure and the message is received from the same MME during that period.
- This flag ensures that the MCE always accepts the MBMS session start request from the new MME (in transient situations where both MMEs have the same MBMS bearer context) and this whatever the order of the MBMS Session Start Request the MCE receives from both MMEs.

Local MBMS bearer context release indication flag signals that an MBMS Session Stop Request is used to release an MBMS bearer context locally in the MME or MBMS GW or both, that is, without the need for the MME to propagate the request to the MCE(s) over the Sm and SGmb interfaces.

- After having moved an MBMS session across MMEs, during a transient Sm path failure, the MBMS GW releases the MBMS bearer context in the old MME after the recovery of a transient Sm path failure. In that case, the old MME does not need to release the MBMS session in the MCE(s).
- Likewise, after having moved an MBMS session across MBMS GWs, during a nontransient

SGmb path failure, the BM-SC releases the MBMS bearer context in the old MBMS GW and old MMEs if the SGmb path recovers before this is seen as a nontransient failure by the old MBMS GW. The old MME does not need to release the MBMS session in the MCE(s).

- This is an optimization to avoid sending useless Stop Requests on the M3AP interface that would anyway be rejected by the MCE (because control has already taken over by another MME).

This feature requires the GW, BM-SC, and MCE support for the same function.

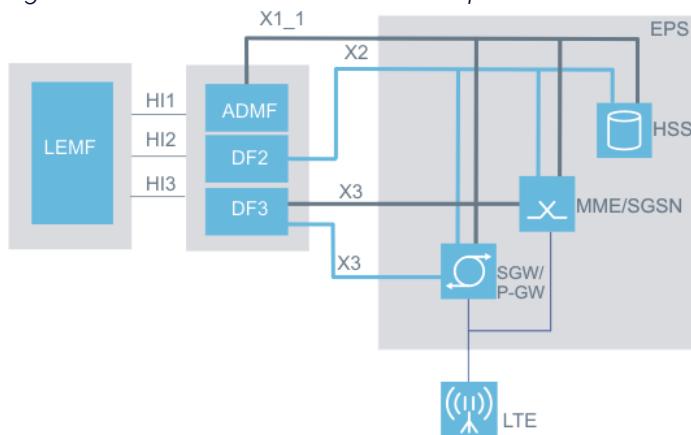
9. MME/SGSN support for lawful interception

In the evolved packet system, MME-only and MME/SGSN deployments of CMM support IP layer interception of content of communication (CC) data. The LI solution for EPS generates intercept related information (IRI) records from control plane messages.

The networking architecture for lawful interception is shown in the figure with the MME/SGSN's administrative interface to the administration function (ADMF) over X1_1, and to the delivery function 2 (DF2) distribution function over X2.

The DF3 network element handles the content of communication (CC) messages over X3. The X3 interface is supported only for LIPv2 specification for SGSN.

Figure 98: MME/SGSN lawful interception architecture



The following table summarizes the LI functions and their corresponding VM/link usage.

Table 61: LI functions and VM/link usage

LI function	VM entity	Link used
Administration	ADMF/LIC	X1_1
Event reports	DF2/LIB	X2
Content of communication	DF3/LIB	X3

Handover interfaces

Communication between the network operator and the LEA is performed using the

handover interface (HI). The HI interface is implemented as part of the regional mediation function and is provided by the administration function (ADMF) and delivery function (DF). The lawful interception standards provide for HI1, HI2, and HI3 handover interfaces.

- HI1 interface represents the interface between the law enforcement monitoring facility (LEMF) and the lawful interception administration function (ADMF) in the service provider's network.
- HI2 interface represents the interface between the lawful interception agency (LEA) and the delivery function responsible for distributing the intercept related information (IRI) to the relevant LEA.
- HI3 interface represents the interface between the LEA and the delivery function responsible for distributing the content of communication (CC) to the relevant LEA.

Lawful interception administration function

The lawful interception administration function varies among service providers and is used for activation, deactivation, and interrogation of lawful interception. The ADMF:

- Interfaces with all the LEAs that require interception in the intercepting network.
- Keeps the intercept activities of individual LEAs separate.
- Interfaces to the intercepting network.

When the LIPv2 interface specification is used, this ADMF is commonly referred to as the lawful interception controller (LIC).

Lawful interception delivery function

The delivery function (DF) is the portion of the LIG responsible for the collection of messages from the lawful interception extension (LIE) network elements and the delivery of this content to the LEAs. A DF2 network element handles the delivery of IRI messages and a DF3 network element handles the delivery of content of communication (CC) messages.

When the LIPv2 interface specification is used, this DF is commonly referred to as the lawful interception browser (LIB).

Encryption

- LI surveillance target records are automatically encrypted on the lawful interception handling service (LIHS).
- The LIPsec encryption mechanism is supported for use with the LIPv2 interface specification.



Note:
CMM supports LIPsec only on the X1_1 interface.

- IPsec is supported on the LIHS, PAPS, and IPPS to protect the X1_1, X2, X3_2G, and X3_3G interfaces.
- Libreswan 3.25 is used to support IPsec on the X1_1, X2, X3_2G, and X3_3G interfaces.

The following IPsec attributes are supported:

- Internet key exchange (IKE) key exchange version 1 and version 2.
- Encryption methods aes, aes128, aes256, 3des.
- Hash functions sha1, sha2_256, sha2_384, sha2_512 and md5.
- Perfect forward secrecy (PFS) groups modp1024, modp1536, and modp2048.

Capacity

With LIPv2, the maximum number of connections is:

- 5 connections to LIC per node, thus maximum 5 X1_1 connections in the SGSN/MME.
- 10 LIBs/LIC, thus maximum 50 LIBs with 5 LICs per node.

With ASN.1, the maximum number of connections is:

- Up to 5 X1_1 transmission control protocol (TCP) connections to an ADMF for administering target identities. If an X1_1 link between the MME/ADMF goes down, an alarm is raised.
- Up to 6 primary X2 TCP connections to an LIG (DF2) for processing IRI messages. If an X2 link between the MME/LIG goes down, an alarm is raised.

General LI capacity:

- Total stored targets are 150 000 (AMF/MME/SGSN or AMF/MME or AMF or MME).
- Up to 1000 UEs with LI surveillance active is supported per CPPS.

With X2 interface, for 2G/3G subscribers, up to 8 PDP contexts are included in IRI event reports.

Related descriptions

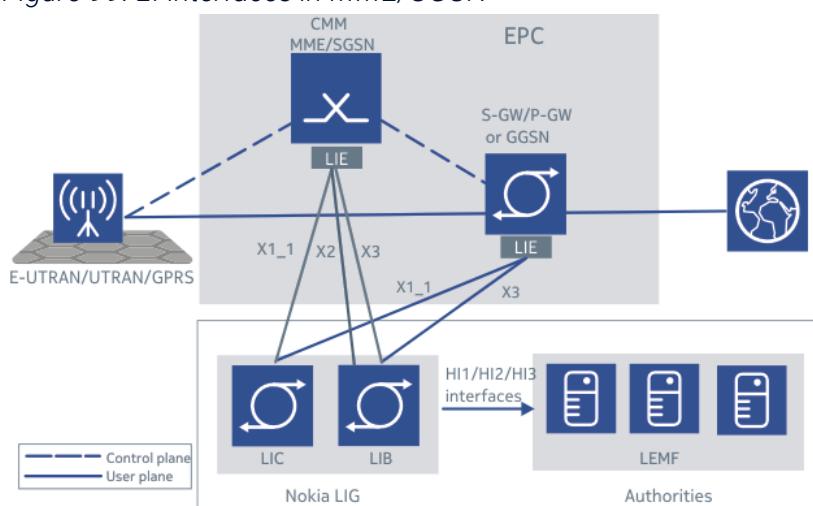
- [Configuring MME/SGSN LI](#)

9.1 Lawful interception (LIPv2 based)

The **Lawful interception (LIPv2 based)** feature includes the lawful interception gateway (LIG) and lawful interception extensions (LIE) in various network elements. When a LIG supporting the LIPv2 is used, the ADMF is commonly referred to as the **lawful interception controller (LIC)** and the DF2/DF3 is commonly referred to as the **lawful interception browser (LIB)**.

A solution for lawful interception can be built for the CMM through direct integration to a Lawful Interception Management System (LIMS) or Unified Lawful Interception Suite (1357 ULIS) with the X1, X2 and X3 interfaces, for example, Utimaco or Thales, for which Nokia currently offers pre-integrated solutions (LIG function in the figure).

Figure 99: LI interfaces in MME/SGSN



The LIE in the CMM is part of the lawful interception (LI) solution. The CMM supports direct interfacing with the X1_1, X2 and X3 interfaces to the LIG. The LIE in the CMM acts as instructed by the LIG, doing the actual interception, and sending the intercepted data and the content of communication to the LIG. Interception can be activated using international mobile subscriber identity (IMSI), international mobile equipment identity (IMEI), or mobile station international ISDN number (MSISDN). The CMM supports LI protocol version 2 (LIPv2) as one LI configuration option. The X1_1, X2 and X3 interfaces use TCP/IP as the transport protocol.

X1_1 interface design

The X1_1 interface is the sole means for administration of the surveillance target list. It stores the target list.

Local and remote addresses for the X1_1 interface can be either IPv4 or IPv6. In case of two X1_1 links, both links must have either IPv4 or IPv6 IP address type.

Individual X1_1 links can have the lawful interception extension (LIE) set to true or false.

The LIP message frame is used to delimit message boundaries on the X1_1 and X2 interfaces. The LIP message frame includes the message length and uses a specific byte pattern to indicate the end of the message frame.

X2 interface design

Local and remote addresses for the X2 interface must be IPv4 on the MME/SGSN configuration. On the MME configuration, the X2 interface can be IPv6.

X2 links are dynamically created by the CMM in response to administration requests received over the X1_1 interface when the LIPv2 interface specification is used.

X3 interface design

Local and remote addresses for the X3 interface must be IPv4.

X3 is used to populate the communication content (CC) to the delivery function 3 (DF3). The interface in CMM terminates in IPPS for 3G user plane data and PAPS for 2G user plane data.

9.2 LCS client type lawful interception (Feature f10308-01)

This feature supports GMLC location request for lawful intercept. The feature provides a provisioning option to accept or deny the LCS client type lawful intercept.

MME accepts LCS client type lawful interception services in Provide Subscriber Location Request message received from the GMCL.

The feature does not require any other provisioning checks.

10. Public safety services

Public safety services provide high priority service treatment for government-authorized personnel, emergency management officials, and other authorized users. Accurate UE location can be provided to security personnel.

10.1 Enhanced multimedia priority services (MPS) (Feature m11009-01)

Commercial users and public safety end users can get priority for IMS service.

This feature allows certain subscribers (service users as per 3GPP TS 22.153) priority access to system resources in situations such as during congestion, creating the ability to deliver or complete sessions of a high priority nature. Service users are government-authorized personnel, emergency management officials, or other authorized users. The MPS supports priority sessions on an end-to-end priority basis.

This feature supports both the UE-initiated and network-initiated priority access. There are 15 priority access levels that can be assigned to a user. Operators can use a parameter to specify the allocation and retention priority (ARP) high priority levels that are allowed high priority access treatment locally at the MME during overload conditions at the MME.

This feature is supported for all the shared public land mobile networks (PLMNs). The MME provides a provisioning option to activate multimedia priority services per shared PLMN basis. A UE does not get priority treatment if the MPS is not activated for the serving PLMN of the UE. The MME allows separate provisioning of ARP values for each PLMN.

The MME uses the following to determine whether a UE bearer has been granted high priority access treatment during MME overload conditions:

- The highPriorityAccess indication in the RRC Establishment Cause parameter of the initial UE message sent to the MME by the eNB and the presence of MPS-priority attribute-value pair (AVP) with MPS-EPS-Priority bit or MPS-CS-Priority or both in the UE subscriber data. The highPriorityAccess indication in the radio resource controller (RRC) Establishment Cause is set by the UE based on the access classes stored in its UMTS subscriber identity module (USIM). The MME uses these indications for initial determination of priority treatment for received initial UE messages.
- The value of the ARP priority level field (part of the quality of service (QoS) sent by the HSS/policy and charging rules function (PCRF)) is used to determine whether a UE bearer gets high priority treatment during overload conditions. It is compared to the locally

provisioned ARP High Priority Level parameter to see if this UE is granted high priority treatment at this MME.

- The ARP priority level field received in the S11 Downlink Data Notification message is compared to locally provisioned ARP value to determine whether paging for the UE is granted high priority treatment during MME overload conditions.
- For paging message received on the SGs interface with priority indication, the MME provides preferential treatment to this message. The subsequent circuit-switched fallback (CSFB) procedure also gets preferential treatment compared to other normal procedures if the UE is marked as a high priority user. If the UE needs to be paged, the MME sets priority indication on the paging request to the eNB. The MME also sets priority indication, that is, CSFB High Priority, in S1AP message to the eNB, so that the eNB can initiate the CSFB procedure with priority.
- For an UE extended service request, the MME determines that the CSFB request needs priority handling based on the MPS CS Priority stored in UE's evolved packet system (EPS) subscription. The MME provides preferential treatment to this request. It also sets priority indication, that is, CSFB High Priority, in S1AP message to eNB to initiate CSFB procedure with priority. This applies to both 1xRTT calls and 3GPP CSFB calls.

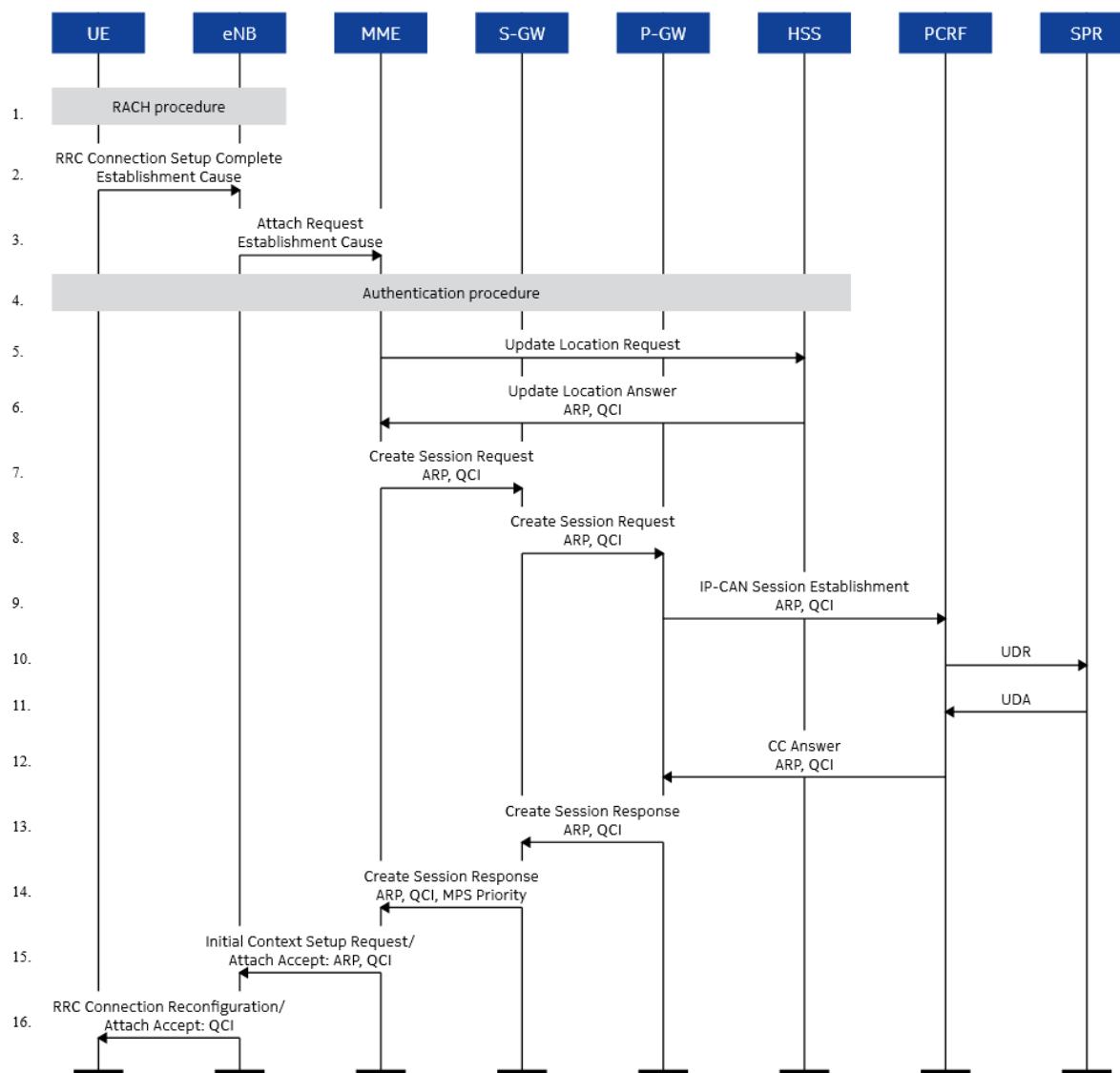
The MME uses the initial UE RRC Establishment Cause value of highPriorityAccess and the MPS-EPS-Priority indication (based on either MPS-CS-Priority bit or MPS-EPS-Priority bit) as an indication that the UE should receive high priority access treatment initially. Once the MME has the ARP value for the UE, the ARP priority level value is also used to determine whether the UE should receive high priority access treatment. The figure shows how the MME gets these high priority indications.

Roamers are given high priority access as defined locally in the visited MME based on the per PLMN provisioning to provide priority access or not. Also, the MME determines high priority access for the following handovers:

- inter-MME S1 handover with or without S-GW relocation
- intra-MME S1 handover with or without S-GW relocation
- X2 handover
- Inter radio access technology (IRAT) handover
- Single radio voice call continuity (SRVCC)

The best effort is provided to establish and maintain sessions for UEs identified as high priority access through any proactive or deliberate action taken to avoid or relieve overload on the MME.

Figure 100: Use of ARP during initial attach (call flow)



In the diagram,

- Based on the received Establishment Cause (high priority access and subscription data), the MME considers the UE high priority.
- The HSS retrieves subscriber data, including EPS-Subscribed-QoS profile (ARP, QoS class indicator (QCI), messages per second (MPS) priority).
- The MME receives ARP and QCI from the HSS in Update Location Answer and saves the values in the UE context.
- The SPR retrieves subscriber information to evaluate the received User-Data-Request message (UDR).
- The PCRF can modify ARP and QCI. The PCRF instructs the P-GW to set up a default bearer and dedicated IP multimedia subsystem (IMS) signaling bearer, each with their own ARP and QCI.

- The MME saves the ARP and QCI received in Create Session Response for each bearer in the UE context and sends the ARP and QCI values to the eNB.

The radio/UE IMS must support this feature.

10.2 Advance priority for eMPS (Feature f11303-01)

This feature ensures priority treatment for two eMPS user types: advance priority users and non-advance priority users. Both get priority treatment and are the last to be pre-empted or throttled in case of MME overload.

Advance priority users can be detected earlier during the call since for these users the MPS-EPS-Priority bit is set on the HSS subscription, and also the default APN configuration has ARP priority level (PL) value 1 to indicate priority.

Non-advance priority users have normal subscription and can only be detected as eMPS priority users when the ARP indicates the MME-provisioned priority ARP once it is modified or established from the S-PW/P-GW side on Update Bearer Request or Create Bearer Request (or also indicated on Downlink Data Notification).

This feature includes, when possible, an extra priority setting for signaling messages to detect an eMPS user prior to sending the message: S6a DRMP value 0 and GTPv2 Message Priority value 0.

When the MME can verify that the user deserves priority treatment as eMPS user prior to sending the S6a message, the MME indicates DRMP 0 for an eMPS user in a request message: Update-Location-Request (ULR), Authentication-Information-Request (AIR), Purge-UE-Request (PUR), and Notification-Request (NOR).

- During the attach, MME is only able to set DRMP 0 for advance priority users if the MME already holds the UE subscription data. For non-advance priority users it is not possible to send DRMP 0 during the attach procedure on S6a messages.
- On inter-MME TAUs, DRMP 0 can only be sent for connected mode TAU when the priority call is ongoing.
- MME does not include the DRMP AVP in S6a answer messages.
- MME internally treats an S6a message with priority when the MME either receives DRMP 0 in the request message from HSS or itself otherwise detects an eMPS user.

MME applies GTP message level priority according to 3GPP Rel 14 CR C4-165264 for eMPS users.

- MME indicates Message Priority value 0 for outgoing S10 and S11 initial or triggered

messages when the MME detects eMPS user.

- MME internally applies highest priority for an incoming S11 messages (initial or triggered) when the MME either receives Message Priority 0 value from the S-GW on the GTP header, or detects eMPS user/session.

Both eMPS types are treated with higher priority than emergency calls.

This feature is disabled by default. It can be enabled using global parameter `empsAdvancePriority`.

10.3 MME support for eMPS priority on RRC establishment cause only (Feature f12126-01)

With this feature, the MME treats an incoming signal with priority purely based on the received high priority RRC establishment cause.

The MME indicates priority on initial signaling towards the HSS after the UE has indicated the high priority RRC establishment cause.

If a UE establishes a connection to the network with the RRC establishment cause indicating that the priority does not have the MPS subscription, the MME does not continue treating the UE with priority after detecting no corresponding priority on the network side.

This feature is not applicable for CloT UEs.

Note:

The MME treats the UE with priority later based on whether the S-GW/P-GW establishes a priority ARP bearer, or modifies the ARP of an existing bearer to a priority value.

10.4 Overlapping position requests for a single UE (Feature m10112-10)

With the *Overlapping position requests for a single UE* feature, simultaneous mobile terminated location request (MT-LR) procedures can be used for the same or a different source.

The MME supports overlapping GMLC position requests for a single UE. This capability is needed for emergency services to obtain a low accuracy early estimate to the PSAP while

high accuracy position is in progress.

When the feature is enabled (global parameter `gmlcOverlappingLocationRequests`), the MME allows up to three ongoing positioning towards the E-SMLC: the original request and two additional requests. The positioning requests can be from the same GMLC or different GMLCs.

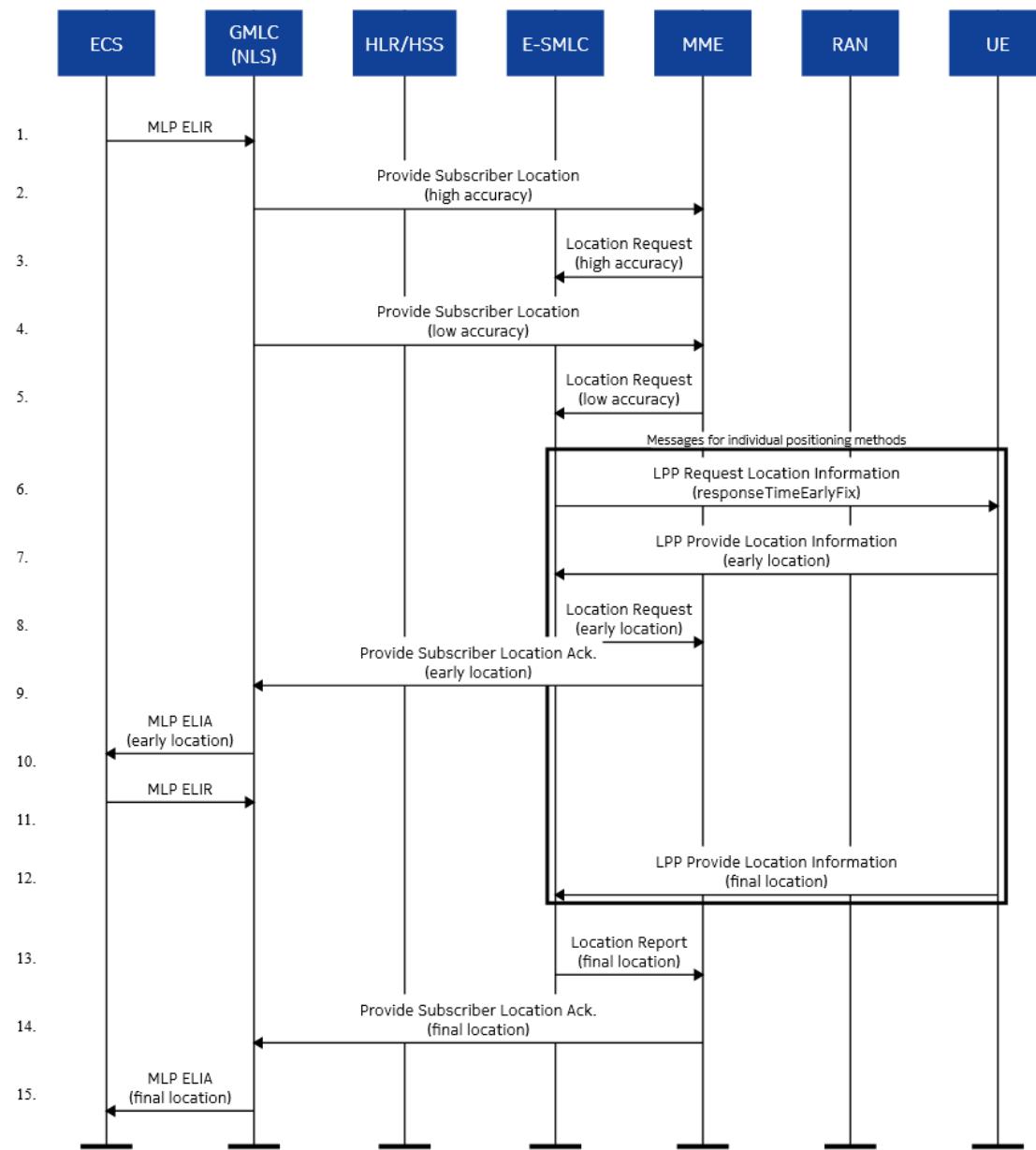
 **Note:**

All overlap positioning request must complete within 90 seconds of the first overlap request, otherwise the 90-second guard timer will expire and any new request is rejected (or last known location returned, if requested and available).

If the location type sent by GMLC is not Current or the last known location, the MME rejects the fourth position request with cause Unable to comply. If location type is Current or last known location, the MME sends the last known UE location, if available.

The figure shows how the MME needs to support overlapping control plane transactions for a single subscriber.

Figure 101: Interim location to PSAP, control plane call flow



10.5 Heightened accuracy location support for SLs/SLg interface (Feature f11001-01)

The MME supports more accurate location information of devices making calls from an indoor location by providing Civic Address, Barometric Pressure, and Additional-Positioning-Data information.

To support indoor positioning capability, this feature introduces parameter extensions on messaging over the SLs and SLg interfaces to enhance the location accuracy of a UE. The

information elements (IEs) that are included in the LCS-AP Location Response message are:

- Civic Address
- Barometric Pressure
- Additional-Positioning-Data

The MME sends information of these IEs to the GMLC in corresponding IEs in the Provide Location Answer Command and Location Report Request Command messages.

11. CMAS/ETWS

The MME supports sending of warning messages to UEs in a particular area as a result of receipt of warning messages from Cell Broadcasting Center (CBC) and forwarding these messages through the eNB.

The base commercial mobile alert system (CMAS) feature was based on Rel 10 standards including 3GPP TS 29.168 and 3GPP TS 36.413.

11.1 Warning message delivery (Feature m11005-01)

The *Warning message delivery* feature provides an ability to send warning messages to a UE in a particular area. The MME receives warning messages from Cell Broadcasting Center (CBC) and forwards these messages to the eNB.

The CBC solution was created for the special requirement of an Earthquake and Tsunami warning system (ETWS) created for Japan, introduced in Rel 8. It utilizes the existing S1-MME control plane interface between the UE and MME, through the eNB. The SBc interface between the CBC and MME is used for warning message delivery and control functions. In the LTE/4G, the SBc interface is based on Stream Control Transmission Protocol (SCTP). There are two main commercial mobile alert system (CMAS) procedures, write-replace warning procedure and stop warning message procedure.

Write-replace warning procedure

The write-replace warning procedure involves the exchange of Write-Replace Warning Request and Write-Replace Warning Response messages. The CBC directs the MME to forward requests to the eNB, the eNB responds to the MME, and in turn, the MME responds to the CBC.

- A Write-Replace Warning Message is received at the MME and sent to the SBc process running on the IP director services (IPDS)/Load Balancer.
- The message is decoded and validated. If all tracking area identities (TAIs) are not served by the MME, the message is rejected by sending a Write-Replace Warning Response message with the appropriate cause Tracking area not valid.
- If any other error occurs, the Write-Replace Warning Response message is returned to the CBC with the appropriate cause Unrecognized message, Missing mandatory element, Warning broadcast not operational, Unspecified Error, Transfer syntax error, Message not compatible with receiver state, or Abstract syntax error.

- If all checks pass, the Write-Replace Warning Response message, with the cause Message accepted, is sent to the CBC.
- The TAI list is converted to an eNB list and encoded and sent in a Write-Replace Warning Request to each eNB in the list. The MME starts a timer for each sent message.

Stop warning message procedure

The stop warning procedure involves the exchange of the Stop Warning Request and Stop Warning Response messages. The CBC directs the MME to forward requests to the eNB, and the eNB responds to the MME, which then responds to the CBC.

- A Stop Warning Message is received at the MME and sent to the SBc process running on the IPDS/Load Balancer.
- The message is decoded and validated. If all TAIs are not served by the MME, the message is rejected by sending a Stop Warning Response sent to the CBC with the appropriate cause.
- If any other error occurs, the Stop Warning Response message is returned to the CBC with the appropriate cause Unrecognized message, Missing mandatory element, Warning broadcast not operational, Unspecified Error, Transfer syntax error, Message not compatible with receiver state, or Abstract syntax error.
- If all checks pass, the message is forwarded to the CBC with the cause Message accepted.
- The MME creates a list of all eNB contained the associated TAIs and sends a Kill Request message to each eNB in the list.
- When the Kill Request messages are sent to the eNBs, the MME starts a timer for each message

Additional capabilities

If the S1-MME interface to an eNB targeted for S1AP Write-replace Warning Request message is down, the MME stores all the messages with message IDs 4370 to 4374 until it initiates the warning message cancel procedure or a configurable timer has expired. If the MME has stored pending warning messages, it sends the S1AP Write-Replace Warning Request message as soon as the S1-MME connection is restored.

- The MME provides an ability to time the response to the S1AP Write-Replace Warning Request message and retransmit the request.
- The MME starts the configurable Write-Replace Warning Response timer. This timer should be configured to be larger than the SCTP retransmission timer.
- If no response is received from an eNB, the MME retransmits the request as specified by the configurable Warning Retransmissions parameter.

- The response timer is cleared once the MME triggers the warning cancel procedure and stops any retransmission of messages.
- The MME also generates an alarm, of configurable severity, if the MME does not receive Write-Replace Warning Response message from an eNB.

The MME provides an ability to continue to send or resume sending CMAS alerts with message IDs in the range 4370 to 4374 for the following failures:

- IPDS or Network Element Cluster Controller (NECC) VM switchover
- CPPS VM failure

In a failover or switchover, messages are check-pointed to the standby IPDS. When a failover or switchover occurs, all pending messages are resent and have their timers restarted.

The MME provides an ability to log all alert message requests and responses to and from the CBC and eNB. The log contains the content of messages received and sent and timestamp of reception or transmission.

- The MME provides a global parameter to start/stop logging and to specify which alert messages should be logged.
- By default, the MME logs all alert messages exchanged between the MME and CBC and between the MME and eNB.
- Messages are logged to `WarnSys.log`.

The MME supports an access control list of valid peer IP addresses for the SBc link. The MME accepts CMAS alert requests on the transport layer only from the provisioned CBC IP addresses on the access control list.

Alarms are generated for the following conditions:

- Loss of SCTP association with a CBC server
- Any software or hardware failures that would result in inability to receive messages from CBC
- Failure to send messages to an eNB
- Failure to receive a response from an eNB to a Write-Replace Warning Request message
- Failure to send S1AP Kill Request message

The MME also can activate/deactivate generation of alarms and severity of the alarms for the following events:

- Failure to send a Write-Replace Warning Request message to an eNB
- Failure to receive a Write-Replace Warning Response message from an eNB
- Failure to send S1AP Kill Request message

New alarms are added on a per S1-MME/SBc basis. Transmission failure alarms are cleared when the next successful message is sent/received.

Alarm activation and severity control for failure to send a Write-Replace Warning Request, Kill Request message, or failure to receive a Write-Replace Warning Response message from an eNB is included in the global parameters. The domain for these alarms is OFF, WARNING, MINOR, MAJOR, and CRITICAL.

The feature fulfills national regulations. Warning messages can save lives of people in crisis situation.

This feature requires support from the E-UTRAN. Operators need to deploy CBC also for the LTE access support.

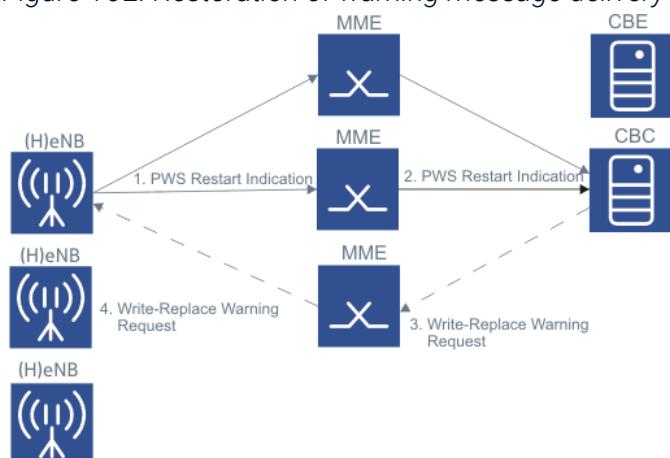
11.2 Restoration of warning message delivery upon eNB restart (Feature m11005-09)

Operators are able to control warning message deliveries via the Cell Broadcasting Center (CBC) even in case of eNB restarts.

This feature supports public warning system (PWS) restoration procedure as specified in 3GPP upon failure or restart of an eNB.

When an eNB has lost its warning message data (for example, after restarting), the eNB sends a PWS Restart Indication message to the CBC through the MME to request the CBC to reload its warning message data, if any. The CBC initiates write-replace writing request (WRWR) procedures to reload the applicable warning message data to the eNB. The figure shows the message sequence of the procedure.

Figure 102: Restoration of warning message delivery upon eNB restart



1. After the eNB has restarted, it deletes all its warning message data. If the warning message service is operational in one or more cells of the eNB, the eNB sends a PWS Restart Indication message that includes the identity of the eNB, the identity of the restarted cells, and the tracking area identities (TAIs) and enterprise application integrations (EAIs) with which the restarted cells are configured, to the CBC to request the CBC to reload its warning message data, if applicable. The eNB should send the PWS Restart Indication message via two MMEs of the MME pool, if possible, to ensure that the CBC receives the message even if one MME cannot propagate it to the CBC (for example, because of an SBc path failure).
2. The MME copies the parameters received from the eNB into the PWS Restart Indication message to the CBC.
3. The CBC reloads the warning message data to the eNB by initiating Write-Replace Warning procedures with the following additions:
 - CBC copies the Restarted-Cell-List, or the Tracking Area ID List or the Emergency Area ID List to populate the Warning Area List information element (IE) of the Write-Replace Warning Request message
 - CBC copies the Global eNB ID into the Write-Replace Warning Request message
4. If a Global eNB ID IE is present in the Write-Replace Warning Request message, the MME forwards the message only towards the eNB identified by the Global eNB ID if this IE is supported by the MME.

Note that there is no change to the current behavior of the MME to store message with IDs 4370 to 4374 if the S1-MME to the eNB is down and send the Write-Replace Warning Request message as soon as the S1-MME connection is restored. It is possible for the eNB to receive two Write-Replace Warning Requests for the same message. The eNB supports the intelligence to recognize this and to ignore the second commercial mobile alert system (CMAS) message.

Support is required from the E-UTRAN and CBC.

11.3 Provisioning restriction for warning area list sent to eNB (Feature f11101-01)

The *Provisioning restriction for warning area list sent to eNB* feature supports provisioning option to specify the maximum number of E-CGI (E-UTRAN Cell Global Identifier) warning areas list.

The E-CGI warning area list is sent to the eNB in the S1AP Write Replace Warning Request or S1AP Kill Request messages. When this feature is enabled, if the CBC sends a SBc Write

Replace Warning Request or SBc Stop Warning Request message with an E-CGI warning area list that exceeds the provisioned warning area max number, the MME does not include the Warning Area List IE in the S1AP message sent to the eNB. The provisioned warning area max number is used only when the E-CGI warning area list is sent to an eNB and the provisioning restriction feature is activated. By default, this feature is disabled.

Figure 103: Provisioning restriction for warning area list in SBc Write Replace Warning Request message

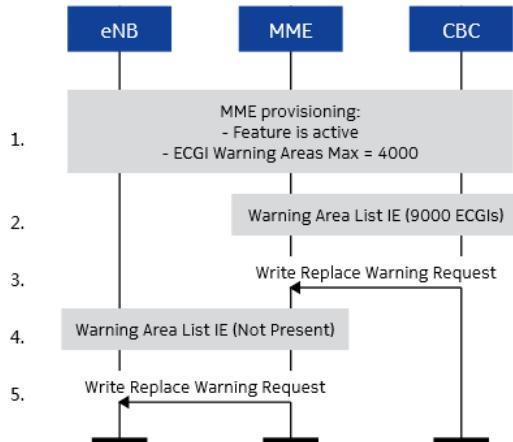
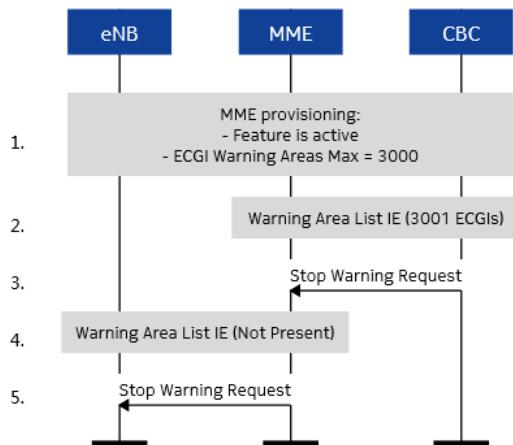
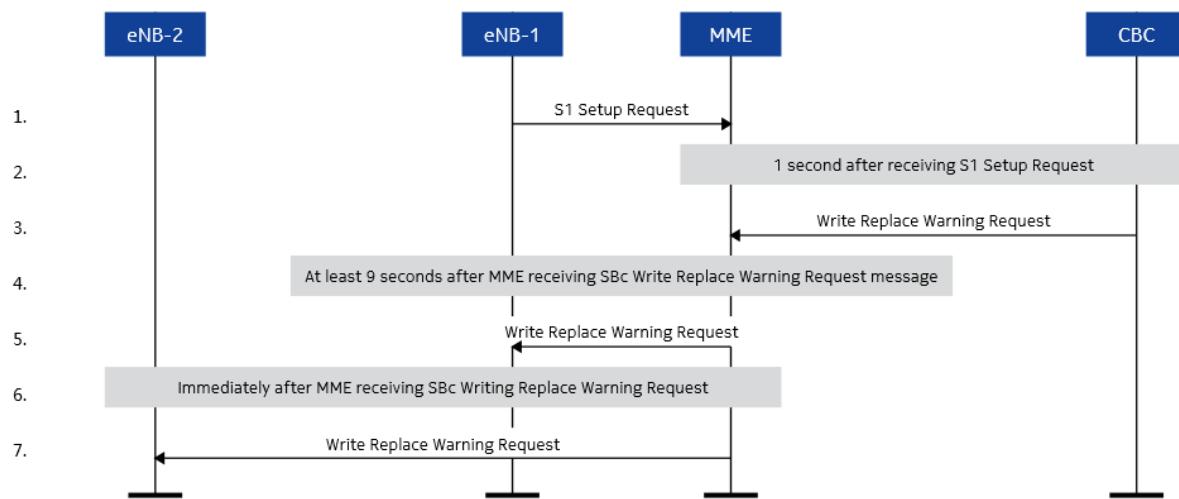


Figure 104: Provisioning restriction for warning area list in SBc Stop Warning Request message



When this feature is enabled, if an eNB sends a S1 Setup Request message when the MME is sending a S1AP Write Replace Warning Request or S1AP Kill Request message, the MME waits 10 seconds before sending the S1AP Write Replace Warning Request or S1AP Kill Request message to the eNB.

Figure 105: Provisioning restriction for warning area list when a race condition occurs



11.4 TAI alarm if TAI is not recognized in CMAS messages from SBc (Feature f11102-01)

If the TAIs received from the SBc Write Replace Warning Request or SBc Stop Warning Request message are not provisioned by the MME, alarm 40881 LSS_cmasTAIinvalid is raised to inform the operator that either the CBC is incorrectly populating the SBc messages or the MME is missing the TAI provisioning.

When the MME receives an invalid TAI, the MME responds to the CBC with cause value "Tracking area not valid" and raises an alarm indicating that unrecognized TAI is received from the CBC. The alarm information contains TAI and SBC identity. The MME only raises the alarm for the first invalid TAI received and reports no more than 10 alarms at a given time.

11.5 MME support for new Warning Area Coordinates IE (Feature f11105-01)

The MME supports the new Warning Area Coordinates IE in the Write-Replace Warning Request message.

The Warning Area Coordinates IE contains the alert area coordinates of a warning message. MME upon receiving the Warning Area Coordinates IE from the SBc interface (from CBC) in Write-Replace Warning Request message transfers it to eNB by copying the data into the S1AP Write-Replace Warning Request message to request the start or overwrite of the broadcast of a warning message.

11.6 CMAS enhancements for Write Replace Warning message (Feature f11106-01)

This feature supports the modified version of 29.168 ASN.1. The SBc Write Replace Warning message and SBc Stop Warning message support the criticality of ignore when the global parameter `useModifiedSbcAsn1` is set to Yes. By default, this feature is disabled.

12. Commercial location services

The location services features make it possible to locate a UE in E-UTRAN.

Related descriptions

- (Emergency) location based services (Feature m11000-01)

12.1 Coarse positioning (Feature m10112-02)

The **Coarse positioning** feature supports quick location of devices such as tablets.

This feature supports positioning of LTE devices like data only devices. The MME obtains positioning information of these devices when requested by a GMLC that is, using mobile-terminated location request procedures. Note that these devices cannot support any positioning capabilities. Thus, these devices never send a positioning request and neither does the MME initiate UE position requests. In addition, the MME is not required to obtain user (UE) permission to obtain positioning information. Location services (LCS) client types that can request position data can be either value added services or public land mobile network (PLMN) operator services. Hence, the feature supports positioning request with an LCS client type set to either value added services or PLMN services from the GMLC.

This feature introduces additional provisioning to accept or reject positioning requests from the following LCS clients in addition to the LCS feature activation:

- Emergency services
- Value added services
- PLMN operator services

The *Coarse positioning* feature requires the *Location services* feature.

Related descriptions

- (Emergency) location based services (Feature m11000-01)

12.2 Expanded LPP container maximum size (Feature m11018-01)

The **Expanded LPP container maximum size** feature supports large packet size to transfer location data between the E-SMLC and UE.

With implementation of this feature the MME supports LPP protocol data unit (PDU) size up to 7915 octets.

If the maximum LPP PDU size received from the E-SMLC exceeds the maximum size (7915 octets), the MME drops the message and sends the LCS-AP Location Abort Request message to the E-SMLC with the location services (LCS) cause set to Misc-Cause. In this case, the MME also logs a message indicating that a message was dropped with adequate details (timestamp of the log message, size of the message, reason for dropping the message, for example).

The MME sends and receives the LPP message using the Downlink Generic NAS Transport message and Uplink Generic NAS Transport respectively. The Generic message container information element (IE) contains the LPP message. In this case, the Generic message container type is set to LTE Positioning Protocol (LPP) message container.

Non-access stratum (NAS) messages (Downlink Generic NAS Transport message and Uplink Generic NAS Transport) used for LPP messages also contain an Additional Information IE that has a length of 3-n. The contents of the Additional Information are the Correlation ID received over the SLs interface. The Correlation ID is defined in *3GPP TS 29.171* section 7.4.28 as 4 octets, while *3GPP TS 24.301* defines a value in the maximum supported length 7.

This feature does not change the currently supported size of the LPPa PDU (2000 octets).

The MME also drops messages from the E-SMLC if the LPPa PDU size exceeds the supported size and sends LCS-AP Abort message to the E-SMLC with LCS cause set to Misc-Cause.

This feature requires location services features.

Related descriptions

- [\(Emergency\) location based services \(Feature m11000-01\)](#)

12.3 HSS-initiated location request

This capability can be used to restrict any UE position requests from a home HSS for a roaming UE.

If configured, the MME processes the following flags received in the IDR message from the HSS:

- EPS User State Request
- EPS Location Information Request
- Current Location Request

- EPS location information in IDA, if requested in the IDR

This capability is enabled or disabled in the LCS options profile (`lcsOptionsProfile`) per PLMN.

The EPS state location info request flag (`epsStateLocInfoReq` parameter) specifies how the MME handles the HSS request for EPS State/Location information in the IDR message. If the MME is configured for either `ECGI and TAI Only` or `UE Geolocation`, the MME indicates support for User State and Location Retrieval to the HSS by setting the State/Location Information Retrieval bit in the Supported-Features AVP.

- If the MME is provisioned for ECGI and TAI support, the MME sends only the ECGI and TAI information along with an age of when the information was collected. IDRs requesting EPS Location without Current Location are unaffected by overload processing, because the MME always has an ECGI and TAI to return for any attached UE. If the current location is requested and the UE is
 - ECM-IDLE: the MME pages the UE to get the latest ECGI and TAI information.
 - ECM-CONNECTED: the MME returns the information currently stored for the UE in the MME's UE context. If the retrieve cell ID (`retrieveCellId`) parameter is enabled, the MME sends S1AP Location Reporting Control to retrieve current cell ID and TAI for the UE.

The cell ID and TAI returned are stored in MME's UE context and sent to the HSS. The MME does not run LCSAP procedures to obtain UE location.

- If the MME is provisioned for UE geolocation, and when the HSS sends an IDR requesting EPS Location Information and Current Location, and the MME is not in overload, the MME runs the LCSAP procedures to obtain UE location and sends the obtained UE geolocation in the Insert-Subscription Data Answer (IDA) message along with the most recent ECGI and TAI. The MME performs the LCSAP procedure only if `epsStateLocInfoReq` has value `UE Geolocation` and current location is requested. If the MME is in overload, the MME will respond to a percentage of IDRs requesting EPS Location and Current Location with just ECGI and TAI without geographical information.
- If the MME is set to not supported, and the User State, EPS Location, or Current Location flags are indicated in an IDR, the IDR is rejected with DIAMETER-_UNABLE_TO_COMPLY (5012) in an IDA message.
- The IDA message supports only the ellipsoid point with uncertainty circle shape. If the MME receives an LCS-AP Location Response message with a different shape or if failure occurs while retrieving data for the UE, the MME sends the IDA message with only the available ECGI and TAI information.

The function of the User State flag is also controlled by the `epsStateLocInfoReq` global parameter

**Note:**

LCS location procedures can take a long time to complete. Ensure that all diameter timers on the HSS (or any Diameter transport equipment, such as a DRA) are configured appropriately to allow for lengthy responses from the MME if LCS is requested.

Related descriptions

- [\(Emergency\) location based services \(Feature m11000-01\)](#)

12.4 Location services enhancements - phase 1 (Feature m11016-03)

The *Location services enhancements - phase 1* feature supports the UE positioning available through the HSS.

This feature provides the capability of sending of the UE state and positioning information to the HSS in Insert Subscriber Data/Answer (IDR/IDA) messages. The feature only supports a global parameter to enable/disable the capability. This feature uses pre-defined values for location services (LCS) quality of service parameters to be used for the HSS requested UE position:

- Horizontal Accuracy set to 20
- Response Time set to low delay
- Vertical Accuracy set to 20
- Verticality set to 5

This feature uses the currently supported GMLC and E-SMLC provisioning.

This feature does not support the following:

- UE privacy checks
- Session-related UE position requests
- PM counts
- Bulk provisioning of E-SMLC for tracking area (TA)
- Overload control on LCS requests in case of the MME overload
- Alarms and provisioning of additional GMLC and E-SMLC per client type

This feature requires location services features.

Related descriptions

- (Emergency) location based services (Feature m11000-01)

12.5 Location services enhancements - phase 2 (Feature m11016-01)

The *Location services enhancements - phase 1* feature provides initial support for the evolved packet system (EPS) User State, EPS Location Information, and Current Location attribute-value pair (AVP). The *Location services enhancements - phase 2* feature builds on the *phase 1* feature and adds additional provisioning capability for those AVPs.

This feature adds functions to value added location services supported by the MME.

This feature does not affect and has no new requirements for the network initiated location request (NI-LR).

This feature builds on top of all the existing features. The additional functions supported are:

- EPS location information in Insert Subscriber Data (IDA) if requested in Insert Subscriber Data Request (IDR).
 - This support can be enabled or disabled per public land mobile network (PLMN) through the LCS options profile.
 - This capability can be used to restrict any UE position requests from a home HSS for a roaming UE.
- Provisioning of an LCS options profile per PLMN. The profile consists of provisioning parameters for the following:
 - Quality of service (QoS) parameters to be used for the UE location for the HSS requested UE location
 - Allow/disallow value-added location services
 - Allow/disallow operator services
- Provisioning of the MME handling of the HSS-requested UE status and location. The MME supports three options:
 - Do not support EPS status/location information retrieval.
 - Only send E-UTRAN cell global identifier (ECGI) and tracking area identity (TAI) to the HSS.
 - Obtain the UE geo-location using LCS-AP procedures and send it along with the ECGI and TAI.
- Provisioning of four additional GMLCs.
- Provisioning of dedicated E-SMLC for IP multimedia subsystem (IMS) emergency services, value-added services, and operator services.

- For value-added services and operator services, the MME supports up to six E-SMLCs per tracking area (TA).
- These E-SMLCs can be provisioned to support a primary/secondary or a load sharing configuration.
- For HSS-initiated UE position requests, the MME uses the E-SMLC provisioned for the value-added services to determine the UE's position.

This feature does not support the UE notification to get UE's permission to proceed with UE location requests.

This feature also adds support for triggering S1AP-LOCATION-REPORTINGCONTROL/LOCATION-REPORT for Current Location.

This feature requires the *Location services enhancements - phase 1* feature.

Related descriptions

- [Location services enhancements - phase 1 \(Feature m11016-03\)](#)

12.6 Including age of location in Provide Subscriber Location Response for failure cases (Feature f10405-01)

When the feature is enabled, the MME includes the ECGI E-UTRAN cell global identifier (ECGI) of most recent eNBs and age of location estimate in Provide Location Answer message, even if the result-code AVP of the message is set to not success and no location information is provided in the Provide Location Answer message.

The age of location estimate is set to the last UE activity timestamp in the UE context. Here last UE activity timestamp represents the last ECGI update timestamp as the MME receives the ECGI in the S1AP Initial UE message and also in the Uplink NAS Transport message.

This feature covers following two scenarios:

- Mobile-terminated location request:
The feature supports the mobile-terminated location request procedure where the Provide Location Answer message is for a current or last known location where the UE is known but no previous latitude/longitude information is available.
- Network-induced location request:
When the Location Report Request message is sent for emergency and no location estimate is provided, the MME includes ECGI. The MME will include the age of location estimate for the feature. The inclusion of age of location applies to all emergency calls for the Location Report Request message related location events including emergency

origination.

12.7 MSISDN in SLg Provide Subscriber Location Request Message (Feature f11004-01)

This feature supports MSISDN as UE identity in the SLg Provide Subscriber Location Request (PSLR).

Currently, MME only supports UE identities IMSI and IMEI. The feature requires HSS to send correct MSISDN of the UE to MME in Update Location Answer. GMLC does not include IMSI if MSISDN is included in the Provide Subscriber Location Request message. This feature enables public safety systems to use MSISDN to obtain UE location in emergency services.

13. M2M, Internet of things support (IoT)

IoT-scale networks require improved indoor coverage, support for massive number of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption, and (optimized) network architecture.

- Devices: low bandwidth, complexity, cost, power consumption

Table 62: Devices

	Release 8	Release 8	Release 12	Release 13	Release 13
	Cat. 4	Cat. 1	Cat. 0	"Cat. 1.4MHz"	"Cat. 299kHz"
Downlink peak rate	150 Mbps	10 Mbps	1 Mbps	1 Mbps	200 kbps
Uplink peak rate	50 Mbps	5 Mbps	1 Mbps	1Mbps	144 kbps
Number of antennas	2	2	1	1	1
Duplex mode	Full duplex	Full duplex	Half duplex	Half duplex	Half duplex
UE receive bandwidth	20 MHz	20 MHz	20 MHz	1.4 MHz	200 kHz
UE transmit bandwidth	23 dBm	23 dBm	23 dBm	20 dBm	23 dBm
Modem complexity	100%	80%	40%	20%	<15%

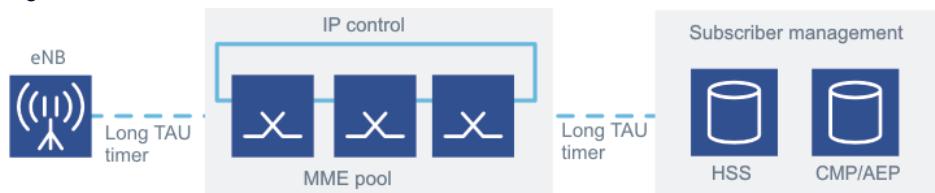
- Radio access network (RAN): reuse of the LTE antenna, the radio head with new baseband unit to support the narrow band radio frequency (RF) and increase in number of sessions
- Core:
 - Support for RAN paging efficiency (last cell for CAT-M devices)
 - More efficient IoT core network architectures
 - Streamline of the control and data delivery to reduce signaling load

13.1 Periodic TAU timer override at attach (Feature m10214-01)

The **Periodic TAU timer override at attach** feature provides an MME capability to override the local provisioned T3412 timer if Subscribed-Periodic-RAU-TAU-Timer as defined in 3GPP TS 29.272 is present and received as part of the subscription data/profile from the HSS and is subsequently passed on to devices.

This feature improves UE reachability and allows the support for customized T3412 timer per international mobile subscriber identity (IMSI) or device profile. This capability can also be used to reduce the frequency of tracking area update (TAU) procedure for machine type communications.

Figure 106: Periodic TAU timer override at attach



The MME receives a long periodic TAU timer from the HSS and sends it to an Internet of Things (IoT)/ machine-to-machine (M2M) device during attach or TAU. To reduce signaling from stationary IoT/M2M devices, a long periodic TAU timer is stored as part of subscription data in the HSS.

For IoT devices with low mobility, having an extended periodic routing area update (RAU)/TAU timer in the subscription data, significantly reduces signaling traffic and power consumption in the IoT/M2M devices.

Three provisioning options are supported for `T3412src` flag:

- MME provisioned T3412 timer
- Subscription T3412 timer
- Maximum T3412 timer (maximum of 1 and 2)

The flag is on UE PLMN service level. If option 2 is selected and data is not received from the HSS, option 1 value is used. The default value is the MME provisioned T3412 timer.

For emergency calls the provisioned emergency T3412 timer (`esrvct3412Timer`) takes precedence.

Extended RAU/TAU timers reduce overall signaling transactions second per device and reduce the UE power consumption.

For this feature to work, the HSS must be able to provide the T3412 override timer value in the subscription data.

13.2 UE power saving mode (PSM) (Feature m10923-01)

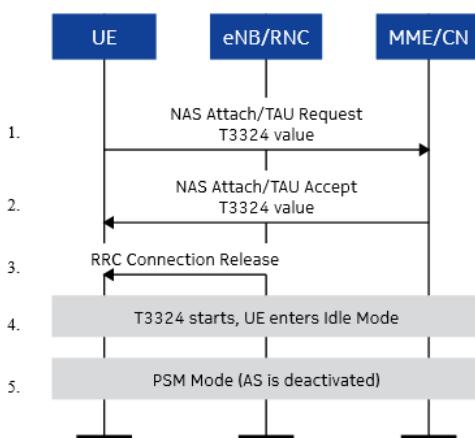
The *UE power saving mode (PSM)* feature allows deployment of low power, long battery life devices. The power saving mode makes Internet of Things (IoT) devices sleep and thus enables longer battery lifetime.

The purpose of the PSM is to allow the device to reduce its power consumption.

When a UE is in the PSM, the device is registered to the network and in EMM-IDLE mode (in S1 mode).

Access stratum (AS) is deactivated in the UE upon entering the PSM. The UE can deactivate the PSM at any time for any mobile-originating service (data or signaling).

Figure 107: UE power savings mode



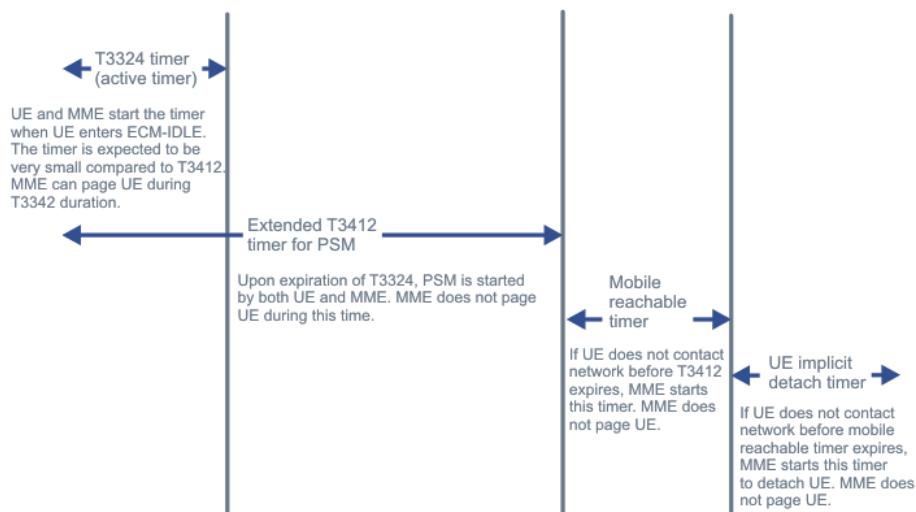
1. The UE supporting the PSM includes the T3324 value information element (IE) in Attach/tracking area update (TAU) Request to request the PSM.
2. If the PSM request is accepted, the MME sends the T3324 timer (active timer) value in the Attach/TAU Accept message.
3. The radio resource controller (RRC) connection is released.
4. When a UE transitions from ECM-CONNECTED to ECM-IDLE state, it starts the T3324 timer. The MME can page the UE before the expiration of the timer.
5. Upon expiry of T3324 timer, the UE enters the PSM (EMM-IDLE): the UE releases its AS functions and goes to the sleep mode to save power. Once the UE enters the PSM, the MME does not send any data to the UE.

While the UE starts the received T3324 timer, the MME starts the mobile reachable timer set to the provisioned T3324 timer value. Both timers T3412 and T3324 are started when the UE enters the ECM-IDLE state. After the T3324 timer expires and until the T3412 timer expires (while the UE is in sleep mode):

- The MME does not page the UE.
- The T3412 timer is stopped on any UE-initiated mobility management procedure.
- If the timer expires, the MME implicitly detaches the UE using the current scheme of detaching a UE:
 - If the T3412 timer expires, the MME starts the mobile reachability timer.
 - If the mobile reachability timer expires, the MME starts the implicit detach timer.
 - If the implicit detach timer expires, the MME detaches the UE and starts the purge timer. The MME purges the UE upon the expiration of the purge timer.

The figure shows the timers used in the PSM procedure. Note that it does not show the actual relative sizes of the timers.

Figure 108: T3324, T3412, mobile reachable timer and UE implicit detach timer



The MME provides provisioning capability to select the UE-sent T3324 timer value or a locally provisioned T3324 timer value to be sent to the UE in Attach/TAU Accept messages.

The MME provides provisioning ability to select the UE-sent T3412 timer, a locally provisioned T3412 timer (the timer value is the TM3412 extended timer value) for the PSM, or an HSS provided timer value.

Note:

The ueWakeUpTimestamp field and the ueWakeUpReason field are used for internal event processing and they are not 3GPP-standard-defined field. Therefore, these fields are not confused with UE wakeup following the PSM.

Related descriptions

- [Extended Idle Mode DRX \(eDRX\) \(Feature f11603-01\)](#)
- [Configuration of eDRX and PSM parameters per APN and IMSI series \(Features f11721-01 and f11603-05\)](#)

13.3 Coverage enhancement paging (Feature m11604-01)

The Coverage enhancement paging feature reduces congestion and increases capacity at the eNB by reducing resources required for paging broadcast. Paging is optimized for low cost, low complexity Internet of Things (IoT) devices in indoor coverage.

This feature introduces support for the Cell identifier and coverage enhancement level information element (IE) within the UE Context Release Complete message sent to the MME. When the MME triggers paging of a UE after the reception of the UE Context Release with a Cell identifier and coverage enhancement level IE, the MME includes the cell identifier and coverage enhancement level information in the Paging messages sent to the eNBs for that UE.

This feature also supports the configuration of a paging policy to be used by the MME when coverage enhancement information is available for a UE.

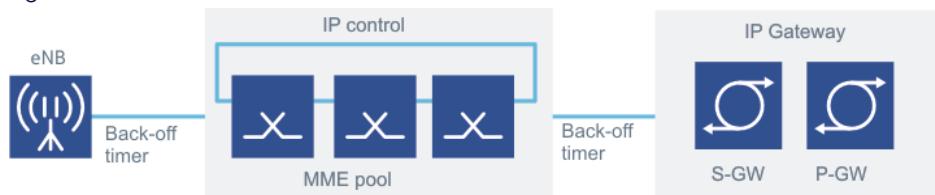
- The eNB sends Cell identifier and coverage enhancement IE in S1AP UE Context Release Complete message for the UE.
- The MME stores the IE and sends the coverage enhancement level in the subsequent paging message.

13.4 Back-off timer for overload control (Feature m10709-02)

In case of overload, the MME can guide Internet of Things/machine-to-machine (IoT/M2M) devices to stop signaling for a certain time by sending a mobility management (MM) back-off timer.

To protect the MME from overload, mobility management requests are rejected and an MM back-off timer (T3346) is included to guide IoT/M2M devices to stop MM signaling.

Figure 109: Back-off timer for overload control



This feature is applicable to

- selective/all IoT services
- selective/all eNBs in a geographic location

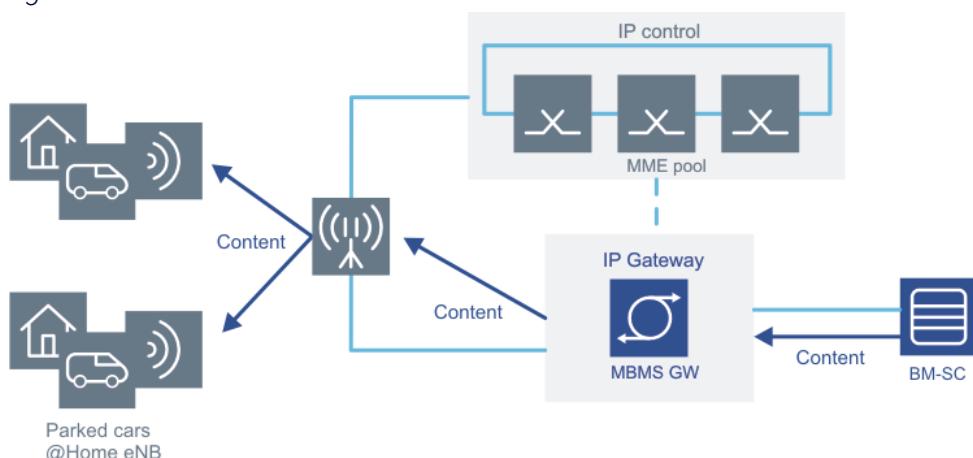
This feature reduces network impact of a signaling overload scenario. In case of overload, higher priority requests are accepted over lower priority ones. Signaling is reduced from low priority M2M devices.

13.5 MME support for MBMS

Providing content (for example, live content for digital signage, firmware/software updates) in an efficient manner to Internet of Things/machine to machine (IoT/M2M) devices in a service area, the MME and multimedia broadcast/multicast service gateway (MBMS GW) support the MBMS session management to reserve and release capacity for content delivery.

Content is forwarded by the MBMS GW to eNBs in a service area.

Figure 110: EMBS



For further details, see the *Multimedia broadcast multicast services (MBMS)* feature.

This feature allows better utilization of radio access network (RAN) and transport resources. Network resources are used in an efficient manner as the same data is transmitted as broadcast to multiple receivers/UEs and not through traditional unicast bearers.

Related descriptions

- [Multimedia broadcast/multicast service \(MBMS or eMBMS\) \(Feature m11007-01\)](#)

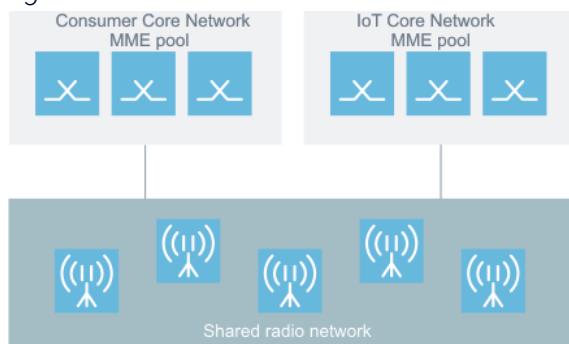
13.6 Multi operator core network (MOCN) (Feature m10902-01)

The *Multi operator core network (MOCN)* feature allows deployment of a separate core for Internet of Things (IoT) devices.

Before other 3GPP network slicing technologies (like Decore), the MOCN allows deployment of a separate core for IoT devices. This requires a separate public land mobile network (PLMN) to be deployed for IoT devices.

For more information, see the *Network sharing feature*.

Figure 111: MOCN



This feature requires the eNB support for MOCN.

13.7 IMSI - ISDN range MME assisted move - UE load balancing (Feature m10713-01)

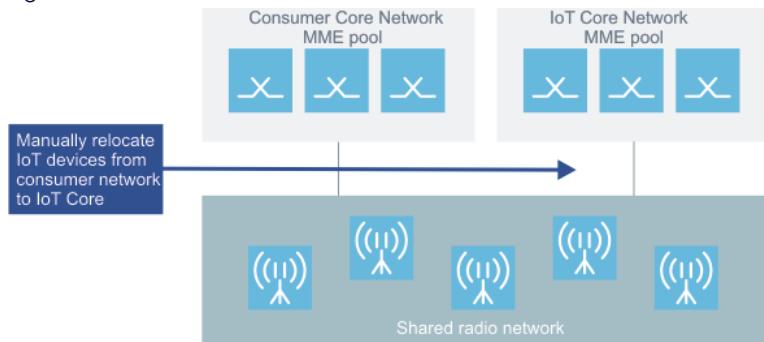
The *IMSI - ISDN range MME assisted move - UE load balancing* feature allows deployment of a separate core for Internet of Things (IoT) devices.

Because of backhaul connectivity issues some IoT devices might register with the consumer

network MME.

The UE load balancing (UELB) feature allows IoT devices registered on the consumer core network MME to be relocated to the IoT core network MME manually.

Figure 112: Subscriber relocation to IoT core network



This feature requires the eNB support for MOCN.

13.8 Extended Idle Mode DRX (eDRX) (Feature f11603-01)

This feature introduces MME support for *Extended Idle Mode DRX (eDRX)*, which is used to reduce UE power consumption.

UE power consumption reduction is achieved by allowing UEs to only listen to the paging channel for relatively short predetermined paging opportunity time windows. The UE's paging channel receiver can be powered down at all other times.

The UE negotiates the eDRX paging opportunity parameters with the MME during the attach and TAU procedures. The eDRX cycle length and eDRX paging time window (PTW) length parameters are determined during this negotiation. Using these parameters, the MME can determine when a UE with eDRX enabled will be reachable (that is, listening to the paging channel).

This feature also includes support for

- delayed processing of SGs Page Requests for SMS delivery
- delayed processing of Provide Subscriber Location Requests from a GMLC when a UE is not reachable because the UE is currently outside of its eDRX paging opportunity window.

This feature supports eDRX deployment option 1 as defined in 3GPP TS 23.272.

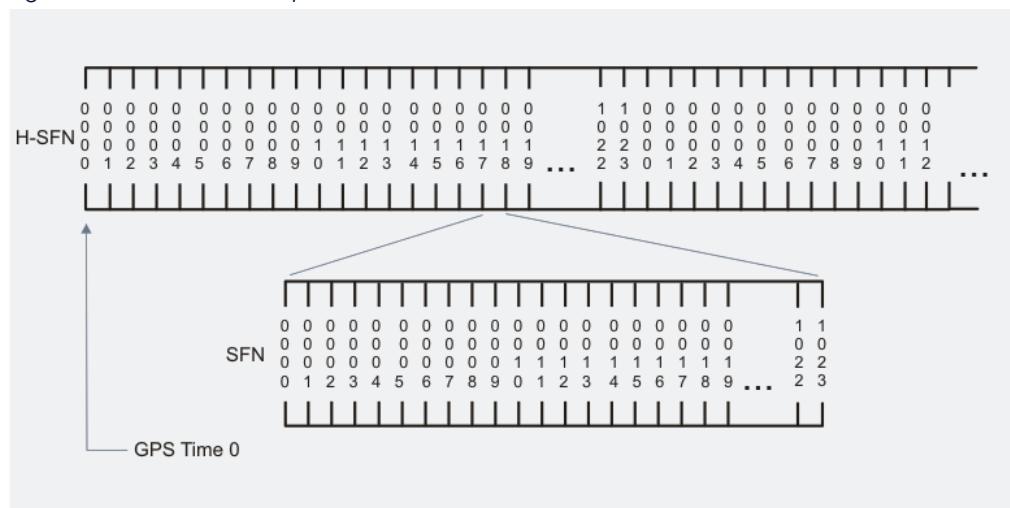
Calculation of eDRX paging opportunities

Timing for standard UE paging is measured in frames of 1/100th of a second. A paging frame is identified with a system frame number (SFN). SFN is a cyclic counter going from 0 to 1023.

Each SFN cycle from 0 to 1023 is referred to as a hyper system frame number (H-SFN). The H-SFN is the count of SFN cycles (from 0 to 1023) that have occurred since epoch start time (for example, 1980-01-06 00:00:00 UTC).

The diagram illustrated the relationship between SFN and H-SFN:

Figure 113: Relationship between SFN and H-SFN



The eDRX paging time window (PTW) start time is calculated using SFN and H-SFN as specified in 3GPP TS 23.682.

Key terms related to eDRX paging opportunity calculation are:

Table 63: Key terms of eDRX paging opportunity calculation

eDRX cycle length	Time interval between the start of one eDRX paging opportunity and the start of the next paging opportunity.
eDRX paging time window (PTW) length	The time period in which a UE monitors the paging channel when it has eDRX enabled.
eDRX paging time window (PTW) start time	The point in time when the eDRX PTW begins for a specific eDRX paging opportunity.
eDRX paging time window (PTW) end time	The point in time when the eDRX PTW ends for a specific eDRX paging opportunity.

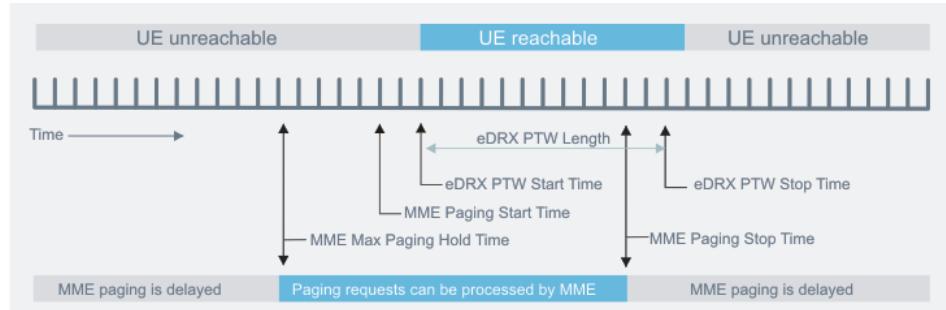
The eDRX paging opportunity calculations allow the MME to determine the eDRX PTW start time and PTW end time based on the following inputs:

- UE type (WB-S1 UE or NB-S1 UE)
- UE's MTMSI value
- UE's eDRX cycle length
- UE's eDRX PTW length

In addition, there are provisionable time offsets related to MME actions related to the eDRX PTW.

MME PTW time offsets

The diagram illustrates how MME time offsets relate to the PTW start and end times and to each other.

Figure 114: MME time offsets and eDRX PTW

The MME PTW time offsets are:

Table 64: MME PTW time offsets

Time offset	Description
MME paging start time	<p>This is the time when the MME starts sending S1AP Paging messages to the eNB. The MME sends the Paging message to the eNB prior to the eDRX PTW start time so that the eNB will receive the Paging message before the paging opportunity begins, even if there is a small difference (for example, 2 seconds) in the MME's clock and the eNB's clock. If the eNB receives the Paging message prior to the eDRX PTW start time, it will wait to page the UE when it is reachable.</p> <p>The value is specified by the <code>edrxPagingStartTime</code> global parameter, in terms of milliseconds prior to the eDRX PTW start time.</p>
MME paging stop time	<p>This is the time when the MME does not attempt to page the UE if a call processing procedure requiring UE paging is received after this point. If a call processing procedure requiring UE paging is received after this point, the MME indicates the UE is unreachable since there is insufficient time to complete even a single page attempt. The MME paging stop time is calculated using the MME paging start time. The exact same time interval between the MME paging start time and the eDRX PTW start time is present between the MME paging stop time and the eDRX PTW end time.</p>
MME max paging hold time	<p>This is the earliest time when the MME attempts to page the UE during a call processing procedure. If a call processing procedure requiring UE paging is received after this point, the MME indicates that the UE is reachable and the MME will start paging of the UE when the MME paging start time is reached. If a call processing procedure occurs prior to this point, the MME responds that the UE is unreachable.</p> <p>The value is specified by the <code>edrxMaxPagingHold</code> global parameter, in terms of milliseconds prior to the MME paging start time.</p>
MME notify HSS time	<p>This is the time when the MME will send a Notify Command to HSS in order to indicate that the UE is now reachable. The Notify Command is sent during processing of a delayed SGs Page Request (for example, the MT SMS scenario).</p> <p>The value is specified by the <code>edrxNotifyHssTime</code> global parameter, in terms of milliseconds prior to the MME paging start time.</p>

eDRX feature activation

The feature requires activation per PLMN using the `edrxEnabled` parameter of the `uePlmnServices` command.

Additionally, you can:

- specify the power saving method (eDRX or PSM or both) to be selected for use if the UE selects both eDRX and PSM. This is controlled by the `edrxModeWithPsm` parameter of the `uePlmnServices` command.
- enable or disable support for the delayed processing of LCS location requests when a UE is unreachable due to eDRX or PSM. This is controlled by the `edrxPsmDelayedLcsLocReqAllow` parameter of the `lcsOptionsProfile` command.

eDRX profile provisioning

If no eDRX profile is provisioned, the eDRX feature operates as follows:

- UEs will be assigned the eDRX cycle length that was requested by the UE, as long as the value is valid for the UE type.
- UEs will be assigned the eDRX PTW length that was requested by the UE, as long as the value is valid for the UE type.

You can override the eDRX parameters that the MME selects for UEs through the use of eDRX profiles (`edrxProfile`). If specified and enabled, the eDRX profile parameters are used by the MME during negotiation of eDRX parameters during the attach and TAU procedures.

eDRX profile parameters are:

- a set of eDRX override parameters to specify if the MME should override the eDRX parameters requested by the UE.
- a set of eDRX cycle override parameters to specify the eDRX cycle length selected by the MME when the UE requests a specific eDRX cycle length. Overriding of the eDRX cycle length occurs only if the following conditions are met:
 - the associated `edrxOverride` parameter is set to `true`
 - the associated `edrxProfile` record is referenced by the `uePlmnServices` record of the current PLMN
 - the specified eDRX cycle length value is valid for the current UE type.
- a set of WB-S1 eDRX PTW override parameters to specify the eDRX PTW length selected by the MME when a WB-S1 UE is assigned a specific eDRX cycle length. Overriding of the

eDRX cycle length occurs only if the following conditions are met:

- the UE is operating in WB-S1 mode
- the associated `edrxOverride` parameter is set to `true`
- the associated `edrxProfile` record is referenced by the `uePlmnServices` record of the current PLMN
- the specified eDRX cycle length value is a valid for the current UE type.
- a set of NB-S1 eDRX PTW override parameters to specify the eDRX PTW length selected by the MME when a NB-S1 UE is assigned a specific eDRX cycle length. Overriding of the eDRX cycle length occurs only if the following conditions are met:
 - the UE is operating in NB-S1 mode
 - the associated `edrxOverride` parameter is set to `true`
 - the associated `edrxProfile` record is referenced by the `uePlmnServices` record of the current PLMN
 - the specified eDRX cycle length value is valid for the current UE type.

Paging policy provisioning

You can use the paging policy provisioning (`pagingPolicy`) to define:

- paging type to be used when a UE has eDRX enabled. Paging type is selected using the `pagingType` parameter of the `pagingPolicy` command. An eDRX paging type is selected based on the eDRX cycle length used by the UE and the general UE type (WB-S1 or NB-S1 UE).
- page response timer (`t3415Timer`) for eDRX paging types.

 **Note:**

eDRX paging types are only defined for eDRX cycle length values that are applicable to that UE type. For example, there is no `WB_EDRX_15` paging type because an eDRX cycle length of 10485.76 seconds cannot be assigned to a WB-S1 UE.

 **Note:**

The default paging policy records are used when the operator has not manually provisioned the paging policy records for eDRX paging types. You should carefully provision the paging policies for each eDRX paging type in order to be compatible with both the eDRX PTW length and the DRX value used by the associated UE type.

PTW time offset provisioning

PTW time offset parameters to control time at which various MME actions are triggered relative to the eDRX PTW start time or eDRX PTW end time. The global parameters are:

- `edrxMaxPagingHoldTime`

This parameter holds the maximum time (in milliseconds) prior to the TSPM time that the MME will wait to start paging during a call processing procedure. If the MME determines it needs to page a UE within the paging hold time interval, the MME will accept the request and wait until the TSPM time to start paging the UE. If the MME receives a paging request outside of the paging hold time interval (that is, too early), the MME will reject/delay the request and (if appropriate) indicate the next available paging opportunity.

- `edrxPagingStartTime`

This parameter holds the time (in milliseconds) before paging time window (PTW) start that the MME should send the S1AP Paging messages to the eNB. This parameter is set to account for small time synchronization differences between the MME and the eNB.

- `edrxNotifyHssTime`

This parameter holds the time (in milliseconds) prior to the TSPM time that the MME should send the Notify Command message to HSS when handling a pending SMS request for an idle UE with eDRX enabled. This parameter is set to account for the time needed for the SMS service center to be informed of the UE's availability and for the MME to receive the resulting SGs Request.

eDRX epoch time provisioning

eDRX epoch time parameters can be used to define:

- The exact date/time of the epoch start time (which defaults to 1980-01-06 00:00:00). This is the exact point in time when the GPS time clock was started. In most cases, the default time should be used, but this parameter can be updated as needed if the RAN is using a different epoch start time. The MME and the rest of the network must have the same epoch start time. The epoch start time is controlled using the global parameter `edrxEpochTime`.
- The number of leap seconds that have occurred since epoch start time. This leap second count is used in the eDRX UE paging opportunity calculations. The number of leap seconds is needed because no adjustment for leap seconds is made for GPS time. As a result, the GPS time is 18 seconds ahead of UTC time as of February 2017. The number of leap seconds is controlled using the global parameter `edrxEpochLeapSeconds`.
- The date/time when an additional leap second will occur. If this parameter is set, MME's internal paging opportunity calculations will automatically adjust to account for the new

leap second when that date/time is reached. This parameter should be set when a leap second is about to occur, otherwise the parameter should be left blank. Once the leap second has occurred, the `edrxEpochLeapSeconds` parameter should eventually be manually updated to reflect the new number of leap seconds that have occurred since the `edrxEpochTime` date and time and the `edrxNewLeapSecondTime` parameter can be changed to be blank.

Alarms and counters

Alarm `40510_LSS_softwareAllocatedResourceOverload` contains eDRX-related resource types:

- Long Duration Timer (on IPDS)
- Long Duration Timer for UE Load Balancing (on IPDS)
- GMLC Request Pool (on CPPS)

A wide variety of counters is available for the eDRX feature.

Impact on external interfaces

The feature introduces:

- information elements on the S1AP interface to support negotiation of eDRX cycle length and eDRX PTW length values during the attach and TAU procedures
- information elements on the S1AP interface to include eDRX information in the Paging message
- cause values for a variety of interfaces.

Dependencies and restrictions

If the paging timer increment provisioned for the *Extended NAS timer* feature (f11707-01) is large, then the MME will not be able to complete all configured paging attempts within the eDRX PTW, especially if the paging time window is small. Future updates to 3GPP standards are expected to clarify how these two features should work together.

The MME will avoid enabling eDRX for a UE if the resulting eDRX PTW is too short to complete even a single page attempt.

13.9 MME support for HLCOM (Feature f11603-02)

Functions of high latency communication are used to handle mobile terminated (MT) communication when a UE is unreachable due to power saving such as PSM (power savings mode) or eDRX (idle mode extended DRX).

High latency refers to the initial response time before normal exchange of packets is established. That is, the time it takes before a UE has woken up from its power saving state and responded to the initial downlink packets. The high latency communication is only used for delay tolerant PDN connections. P-GW indicates to the MME whether the PDN connection is delay tolerant in Create Session Request.

The high latency communication includes the following capabilities:

- If DDN is received for UE in eDRX or PSM, MME indicates S-GW to buffer MT data at the S-GW. MME also indicates to S-GW on how many packets to buffer and how long to buffer. MME introduces a new flag in UE bearer context that the UE has buffered data and starts DL Data Buffer Expiration Timer. If UE has buffered data, then MME pages the UE at the next paging occasion.
- MME activates user plane when an idle UE in eDRX or PSM sends TAU request and if there is buffered data or pending SMS message.
- At TAU/RAU procedures with MME change, the old MME indicates in the context response to the new MME/SGSN that buffered DL data is waiting and hence the new MME establishes the user plane for delivery of the buffered DL data. When the DL Data Buffer Expiration Time has expired, the MME/SGSN considers no DL data to be buffered and no indications of Buffered DL Data Waiting are sent during context transfers at TAU procedures.
- At TAU procedures with S-GW change, the buffered DL data is forwarded to the new S-GW.

13.10 Aging out UE contexts from CPPS cache (Feature f14103-01)

Aging out UE contexts from CPPS cache feature supports optimization of the CPPS cache on the MME by aging out the UE context entries for IoT UEs. A copy of the UE context entries continue to be stored on the DBS and can be retrieved when the UE performs its next procedure.

Aging out UE contexts from CPPS cache feature supports the removal of CPPS cache (VLR) entries on the MME by aging them out. This feature is only available for IoT UEs. The IoT

Quiet Period Timer specifies the duration an EMMState-Registered and ECMState-Idle UE can be inactive on the MME before its context entry gets aged out (removed) from the CPPS cache. However, a copy of the UE context is still stored on the DBS.

When the aged-out UE performs its next procedure ,such as service request, the UE context entry gets retrieved back from the DBS and populated into a CPPS cache after CPPS selection by the MME. The CPPS selected for the copy back of the UE context could be a different CPPS that the UE context was aged out from.

This feature can be enabled by setting the global parameter `enableCacheAgeOut` to Yes and provisioning the IoT Quiet Period Timer in minutes with parameter `iotQuietTimer`.

13.11 Configurable cause code sending in SGs for eDRX/PSM (Feature f11725-01)

This feature supports the sending of configurable cause code message SGs-UE-UNREACHABLE on the SGs interface. This feature is related to eDRX functionality.

When UE is out of paging window or active time, CMM will send SGs-UE-UNREACHABLE with the default SGs cause 'UE temporarily unreachable'. In some operators networks, the existing MSCs do not support this SGs cause and there is no plan to support it. This feature supports configurable SGs cause for the procedure specified in 3GPP TS 23.272 clause 8.2.4a.

The feature is controlled by global parameter `ueUnreachableMsgSgsEdrxPsmCause`. When the feature is activated, cause 'UE unreachable' is sent instead of the default cause code.

13.12 Handling MT SMS for UE in power savings (Feature f11721-02)

This feature supports mobile-terminated (MT) SMS delivery option 2 when a UE is not reachable due to extended idle mode (eDRX)/power saving mode (PSM).

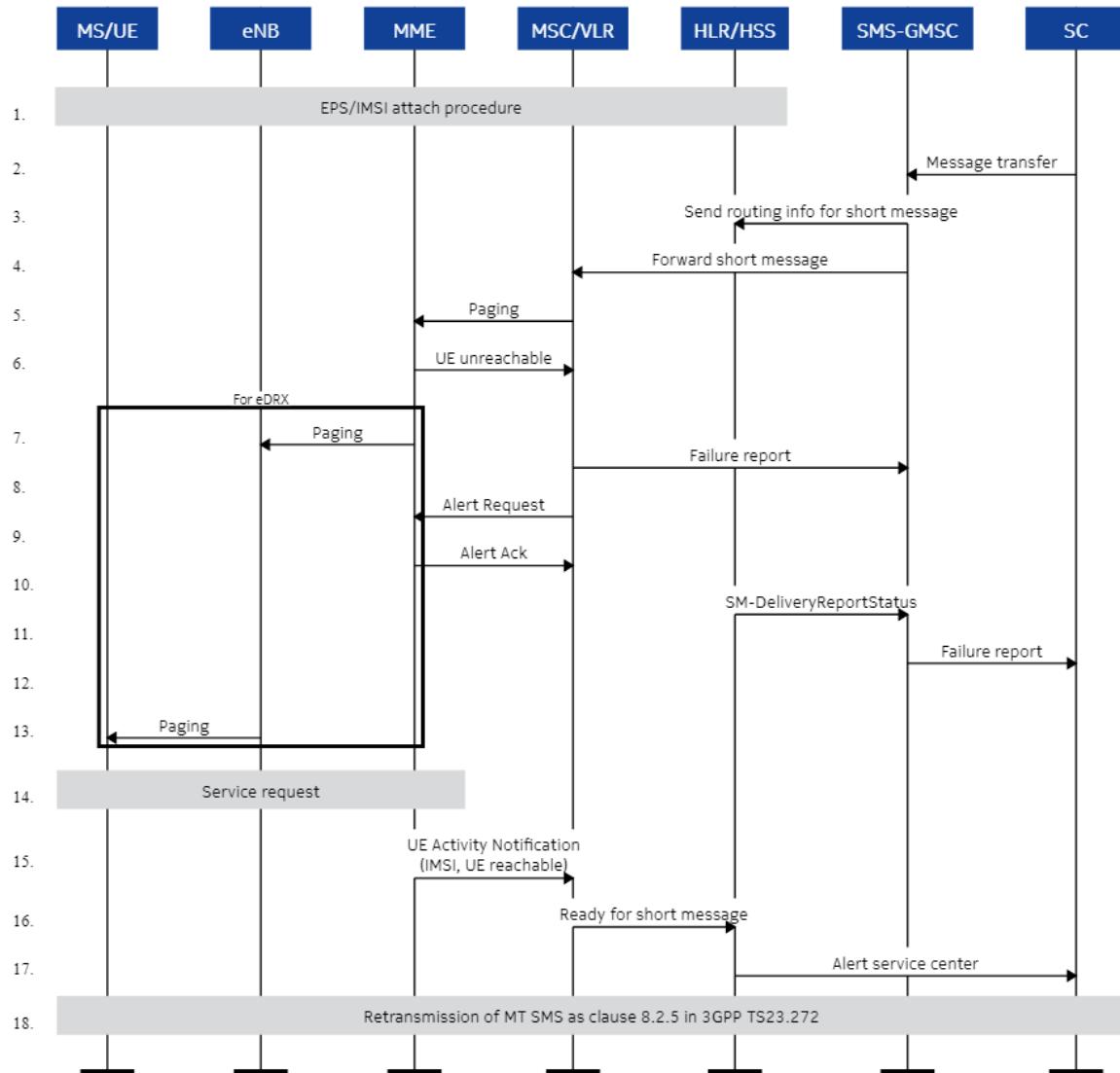
By default, the MME uses MT SMS deployment option 1 for MT SMS in eDRX and PSM. This is a per-PLMN setting.

MT SMS delivery option 2, which is an enhancement for MT SMS delivery option 1, adds some additional optimizations for reducing the signaling to HLR/HSS. Deployment option 2 is based on the transmission of SM Delivery Timer, SM Delivery Start Time, and Maximum Retransmission Time IEs by the MSC/VLR to the MME. The MME receives these IEs and takes

the values into account to determine if and how the enhancement of deployment option 2 is applied on the specific MT SMS delivery, when the UE is in power saving mode.

Handling of MT SMS for UE in the power saving mode is shown as follows:

Figure 115: Option 2 for handling MT SMS for UE in the power saving mode



When the UE is connected and the MT SMS arrives from MSC/VLR, there is no change and the SMS is delivered as stated in clause 8.2.5 of 3GPP TS 23.272.

When the UE is in idle mode and the MT SMS arrives, the MME determines if the paging window is open for the UE. If paging is possible, the MME pages the UE and the SMS delivery continues as stated in clause 8.2.4 of 3GPP TS 23.272.

If the paging window is closed and will be open for the UE, MT SMS delivery option 2 introduces a method for the MME to determine if the SMS can be buffered in the MSC/VLR

or retransmitted by the SMS-GMSC/SC at a later time. To achieve this, the SGsAP Paging Request message for MT SMS contains three IEs: SM Delivery Timer, SM Delivery Start Time, and Maximum Retransmission Time.

When SM Delivery Timer and SM Delivery Start Time are included in the SGsAP Paging Request message, the MME determines that the MSC/VLR is able to buffer the MT SMS. By comparing the timestamp defined by SM Delivery Timer and SM Delivery Start Time with the time that Paging will become possible, the MME determines if it can use the buffering option. If the buffering is possible until the paging window opens, the MME responds to the MSC/VLR with SGsAP UE unreachable with cause "UE temporarily unreachable" and sets the SM Buffer Request Indicator to indicate to the MSC/VLR that it buffers the MT SMS. When the paging window opens, the MME proceeds with paging the UE and then delivery continues as stated in clause 8.2.4 of 3GPP TS 23.272.

When the Maximum Retransmission Time IE is present in the SGsAP Paging Request message, the MME determines that the SMS-GMSC/SC can retransmit the MT SMS later until the timestamp defined by the Maximum Retransmission Time IE. When the retransmission option is followed, the MME responds to paging with SGsAP UE unreachable with cause "UE temporarily unreachable" and with the Requested Retransmission Time IE requesting the SMS-GMSC to retransmit the short message at a later time prior to the Maximum Retransmission Time and after the paging window opens. In that case, the MSC/VLR is expected to arm the NEAF (with the SGsAP Alert Request/Ack message) to request the MME to notify the VLR of any subsequent UE activity prior to the requested SM retransmission time.

When this feature is enabled for a PLMN and UE activity is observed, the SGsAP UE Activity Indication message, which is sent always, includes Maximum UE Availability Time IE to indicate the time until which the UE is expected to be reachable. The Maximum UE Availability Time IE is calculated as follows:

- Calculate when the UE is going to be in sleep mode due to PSM (PSM Sleep Start Time).
- Estimate until when the MME is going to keep up the S1 (value taken from the timer value of `cmm timer show controlPlaneUserInactivity` minus 500 ms, or 0 if UE Inactivity timer does not apply for this UE) (S1 Up Until Timestamp).

For example, when you use `cmm timer show controlPlaneUserInactivity` to get that the time value is 3000 ms, the estimated Maximum UE Availability Time value that you get is $3000 - 500 = 2500$ ms.

- Calculate when paging is going to stop due to eDRX (eDRX UE Availability).
- The estimation for Maximum UE Availability Time is taken as the closest to current time non-zero timestamp between PSM Sleep Start Time and the maximum of S1 Up Until Timestamp and eDRX UE Availability.

For example, for a UE that supports both eDRX and PSM:

- Assume that TAU is received when the current time is Fri Dec 28 07:08:02 UTC 2018.
- S1 will remain up at least for the value of Control Plane User Inactivity timer (default value 3000 ms).
- The calculation estimates that S1 will remain up at least until Fri Dec 28 07:08:04.500 UTC 2018 (current time + 3000 – 500 ms).
- The UE supports PSM and assumes that the timer T3324 (active timer) will expire on Fri Dec 28 07:08:25 UTC 2018.
- The UE also supports eDRX and assumes that paging will be stopped due to eDRX on Fri Dec 28 07:08:29 UTC 2018.

Since all timestamps are valid (non-zero), the Maximum UE Availability Time will be calculated as min (Fri Dec 28 07:08:25 UTC 2018, max (Fri Dec 28 07:08:29 UTC 2018, Fri Dec 28 07:08:24.500 UTC 2018)) = Fri Dec 28 07:08:25 UTC 2018. This is reasonable, because at that time the UE is expected to enter PSM, therefore it will not be reachable after that point in time.

- If the above calculations result in a non-zero value, this is encoded and sent with the SGsAP UE Activity Indication message.
- If the above calculations do not result in a non-zero value, no estimate is sent to the MSC (the IE is not encoded). For example, the S1 release is controlled by the eNB.

 **Note:**

The MME attempts retransmission when the MT SMS cannot be delivered via buffering either because buffering is not possible or because buffering duration is not sufficient for the paging window to open.

13.13 Minimum T3412 timer for UE power saving mode (PSM) (Feature f10409-01)

This feature allows operators to specify a minimum T3412 timer to be selected for UE power saving mode (PSM). This feature is used during attach and TAU procedures.

The MME sends the provisioned minimum T3412 timer in the Attach or TAU Accept message when the PSM UE is provisioned and the T3412 timer received from the UE in the Attach or TAU Request message is less than the provisioned minimum T3412 timer.

This feature is only applicable for the PSM UE with T3412 value provided in the Attach Request or TAU Request message, and the PSM UE provisioned by the `psmT3412TimerSrc` timer.

Table 65: Minimum T3412 timer

Timer name	Value range	Default value	Purpose
<code>psmT3412MinTimer</code>	1-31	31	T3412 value.
<code>psmT3412MinTimerUnit</code>	<ul style="list-style-type: none"> • 320Hours: set the unit of T3412 timer to 320 hours. • 10Hours: set the unit of T3412 timer to 10 hours. • 10Minutes: set the unit of T3412 timer to 10 minutes. • 2Seconds: set the unit of T3412 timer to 2 seconds. • 30Seconds: set the unit of T3412 timer to 30 seconds. • Hour: set the unit of T3412 timer to hours. • Minute: set the unit of T3412 timer to minutes. 	10Minutes	Used in conjunction with <code>psmT3412MinTimer</code> .

13.14 MME support for 320 hours unit in the T3412 extended timer (Feature f10409-02)

This feature supports the 320 hours unit in the T3412 extended timer for Attach/TAU Request and Attach/TAU Accept messages. The MME supports up to 31 units, allowing a maximum value of 31*320 hours for the T3412 extended timer negotiated with the PSM and LPA UE.

The UEs which support power saving mode (PSM) operation can negotiate an extended periodic TAU timer with the network.

This feature supports a larger periodic TAU timer for the power saving mode (PSM) and the low priority access (LPA). The CMM accepts the 320 hours unit for the timer specification in local provisioning and in the S6a messaging.

Prior to this feature, the timer value units for the 320 hours was capped at a maximum of six to reduce possible testing efforts. With this feature, the upper values of the extended T3412 timer can be: 320 hours, 640 hours, 960 hours, ... 30*320 hours, 31*320 hours.

It is not possible to negotiate a periodic timer between the discrete values due to the message definition in the 3GPP.

Enhancing T3412 extended timer for LAP (low access priority) devices (Feature m10115-01)

UEs that are not PSM is part of this feature.

13.15 Active timer in the UE subscription (Feature f11732-01)

This feature uses Active-Time AVP and Maximum-Response-Time AVP in HSS subscription data for T3324 timer when UE requests power saving mode (PSM).

If the `psmT3324TimerSrc` parameter in the `svcAgreementProfile` command is set to `HSS` and UE requests PSM, then the MME uses Active-Time AVP and Maximum-Response-Time AVP in HSS subscription data for T3324 timer in Attach Accept and TAU Accept messages as specified in the following:

- Maximum-Response-Time AVP is used only when UE reachability monitoring is enabled. If there are multiple Maximum-Response-Time AVPs, the largest value is used.
- If both Active-Time AVP and Maximum-Response-Time AVP exist, Maximum-Response-Time AVP has higher priority.
- If neither Active-Time AVP nor Maximum-Response-Time AVP exists, use locally provisioned value for the T3324 timer.
- If Active-Time AVP only exists, T3324 timer takes the value of Active-Time AVP.

13.16 Configuration of eDRX and PSM parameters per APN and IMSI series (Features f11721-01 and f11603-05)

This feature supports provisioning of power savings parameters (PSM active timer and eDRX) per APN and per IMSI series and/or TAC. In addition, this feature supports a capability to select eDRX parameter from UE subscription or locally provisioned eDRX parameters if there is no APN match.

If an operator selects to use eDRX parameter from UE subscription, the MME uses the eDRX cycle duration from the UE subscription data. In this case, the MME selects provisioned eDRX paging time window (PTW) corresponding to the eDRX cycle length and RAT type obtained from the UE subscription. If HSS does not provide the AVP, the MME uses the local provisioning.

If locally provisioned option is selected, the MME first selects power savings parameters (eDRX and PSM) for an APN when the first PDN connection is set up if per APN power savings (eDRX, PSM) profile is provisioned. If APN power saving profiles are provisioned at both UE PLMN level and IMSI series level, the IMSI service level profile has higher precedence. If no

APN power savings profiles are provisioned at UE PLMN level or IMSI service level, the MME uses the eDRX profile of feature *Extended Idle Mode DRX (eDRX) (f11603-01)*.

The MME uses eDRX parameters profile introduced in feature *f11603-01* when UE attaches without a PDN connection.

The MME continues to use the eDRX parameters set up for the first PDN connection for the following conditions:

- UE establishes subsequent PDN connections.
- The first PDN connection is deactivated. In this case, UE may have other PDN connections or no PDN connections.

Any changes to the provisioning of PSM or eDRX parameters are handled on a subsequent TAU request.

For provisioning, this feature introduces:

- eDRX and PSM parameters in `uePlmnServices` and `imsiRangeServices`
- commands `edrxApnList` and `edrxApn` for provisioning of eDRX cycle and PTW values for WB-S1 and NB-S1 UEs
- commands `psmApnList` and `psmApn` for PSM timer provisioning
- command `edrxHssPtwProfile` for PTW length provisioning for different eDRX cycle lengths for WB-S1 and NB-S1 UEs

Feature *APN based PSM/eDRX enhancement (f11603-05)* adds the `source` parameter to `edrxApn` and `psmApn` provisioning, allowing the operator to select either UE-provided or APN-based (local configuration) values.

The `cmm subscriber show` command displays eDRX values sent to the UE and in HSS subscription data, as well as the first APN NI used for determining APN NI matching (in `edrxApn` and `psmApn`).

13.16.1 Functionality of eDRX and PSM provisioned per APN and IMSI series

eDRX and PSM can be provisioned per APN and IMSI series. The MME always checks IMSI range provisioning first. If the UE does not fall into any provisioned IMSI range service, the MME uses the provisioning for the UE PLMN services.

In order to determine whether to enable eDRX and to select eDRX parameters for a UE, the MME first checks IMSI range services provisioning (`imsiRangeServices`). If the UE IMSI falls within the provisioned IMSI range and TAC, the MME first checks whether an APN eDRX

profile is provisioned (`edrxApnListName`). If an eDRX APN list (`edrxApnList`) is provisioned, the MME will use the eDRX parameters provisioned for the APN if the following conditions are met:

- The UE-requested APN NI matches with the APN NI in the profile.
- eDRX is enabled for this APN (using the `edrxEnabled` parameter in `edrxApn` profile). If eDRX is not enabled, the MME does not enable eDRX for the UE.

If there is no eDRX APN profile provisioned or eDRX APN profile exists but no APN match is found, the MME checks the `edrxEnabled` parameter of the `imsiRangeServices`.

- If the `edrxEnabled` parameter is set to `true`, the MME checks the `edrxSource` parameter of the `imsiRangeServices`. If the parameter is set to `Local`, the MME selects locally provisioned eDRX parameters.
- If the parameter is set to `HSS`, the MME uses the eDRX parameter received in UE subscription data from the HSS (using the `edrxHssPtwProfile` specified by `edrxHssPtwProfileName`). In this case, the MME selects provisioned PTW corresponding to the eDRX cycle length and RAT type obtained from UE subscription. If the HSS does not provide the AVP, the MME uses the local provisioning.

If the UE does not fall into any provisioned IMSI range service, the MME uses the provisioning for the UE PLMN services (`uePlmnServices`). The scheme used for the selection of the eDRX parameters is identical to the eDRX parameters selection for the IMSI range services: first check `edrxApnListName` provisioning, then `uePlmnServices` provisioning, and so on.

The PSM active timer selection is identical to the selection of the eDRX parameters: The MME checks `psmApnListName` provisioning for an APN match and the `psmEnabled` flag prior to checking the `imsiRangeServices psmEnabled` flag, and so on.

MME continues to use the eDRX parameters set up for the first PDN connection for the following conditions:

- UE establishes subsequent PDN connections
- The first PDN connection is deactivated. In this case, UE may have other PDN connections or no PDN connections.

Note that if UE registers without a PDN connection and then establishes a PDN connection, the UE will be updated with the provisioned power savings parameters on a subsequent TAU request.

The figures show the procedure used to determine eDRX parameters and PSM active timer based on the provisioning.

Figure 116: eDRX selection at Attach/TAU Request

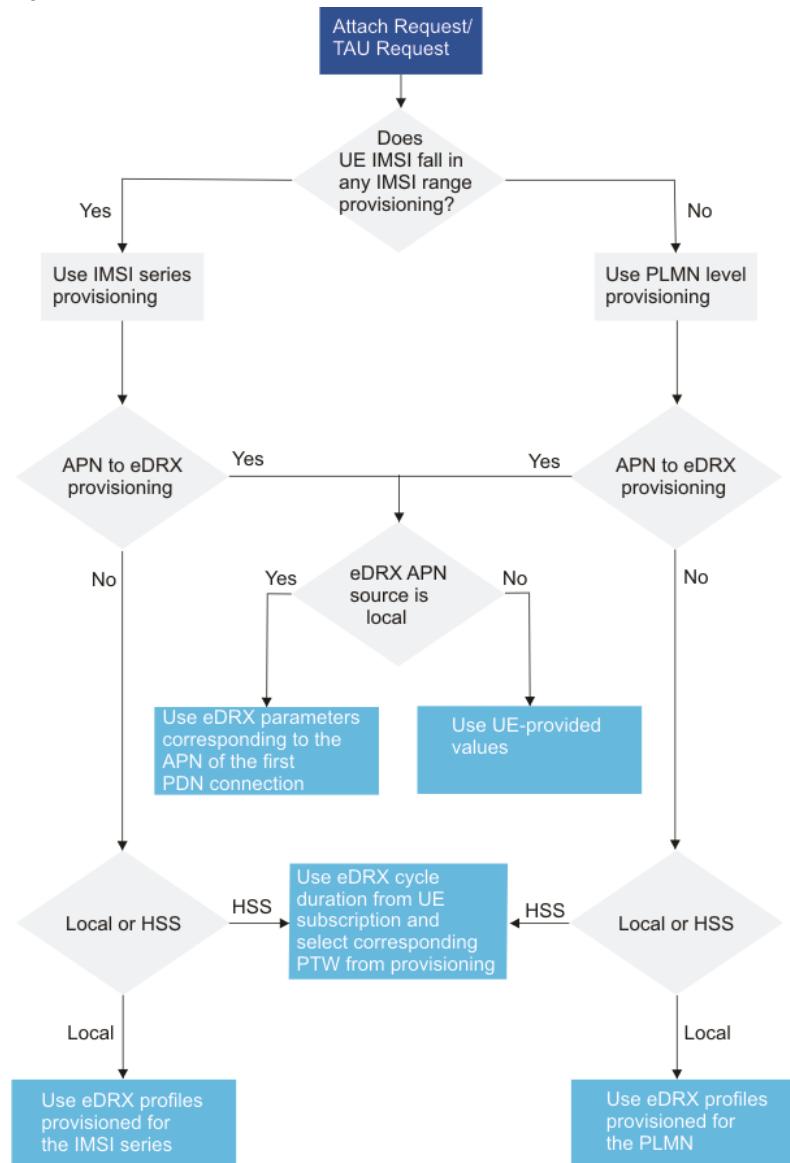
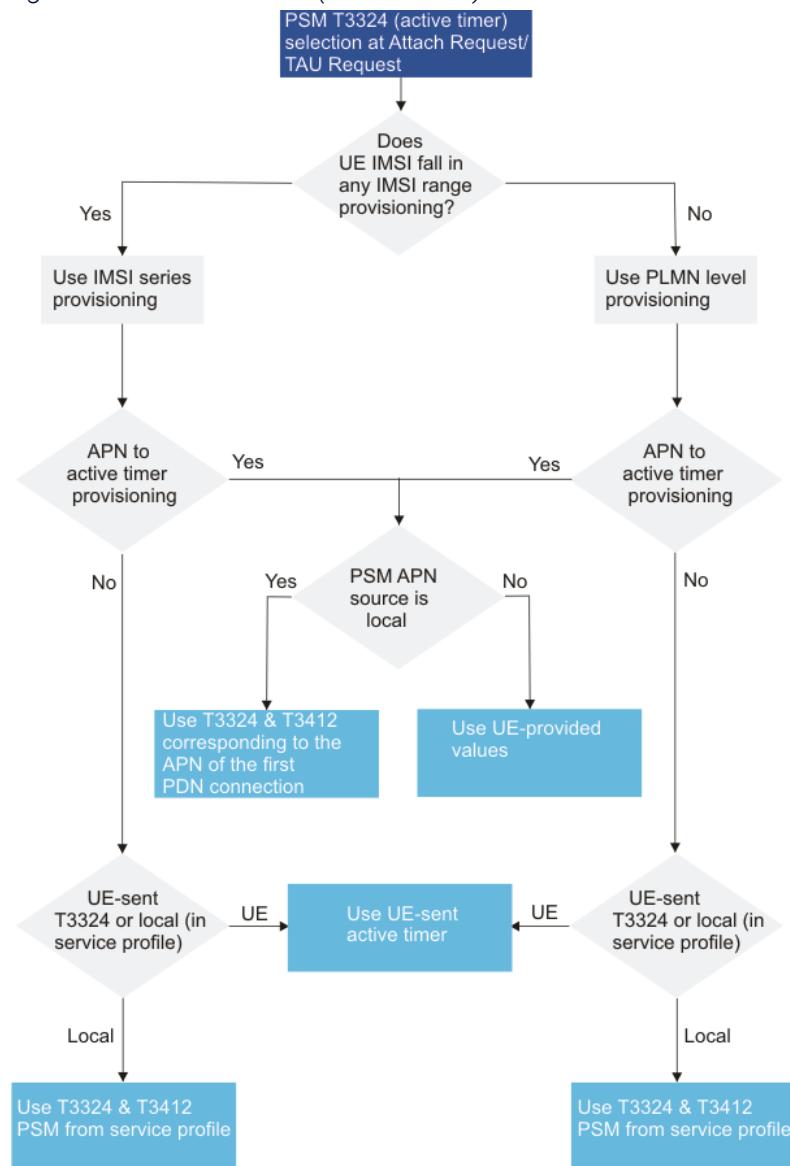


Figure 117: PSM T3324 (active timer) selection at Attach/TAU Request



13.16.2 MME support for 10K APNs in a list (Feature f11708-07)

The feature supports the maximum number of supported APNs, maximum number of APN-eDRX profiles, and maximum number of PSM-APN profiles.

The details are as follows:

- 5000 eDRX-APN profiles (such as edrxApnList).
- 5000 PSM-APN profiles (such as psmApnList).
- Total number of APNs (such as edrxApn) across all the eDRX-APN profiles is 10 000.

- Total number of APNs (such as psmApn) across all the PSM-APN profiles is 10 000.
- APNs within a single list must be unique. However, the same APN can be added to multiple lists. For instance, adding the same APN to three different eDRX-APN lists would count as 3 APNs towards the 10 000 APNs allowed across all eDRX-APN lists.
- The MME allows an eDRX-APN profile with maximum of 10 000 APNs.
- The MME allows a PSM-APN profile with maximum of 10 000 APNs.

 **Note:**

A single profile of eDRX-APN with 10 000 APNs and a single profile of PSM-APN with 10 000 APNs can only be created by an operator. If the operator wants to create a second list, the first list has to be split so that the total number of APNs across the two profiles remains 10 000.

13.17 MME support for subscription-based aerial UE identification (Feature f11337-01)

This feature provides MME ability for 4G LTE networks to support aerial vehicles.

This 3GPP 4G LTE networks feature that supports aerial vehicles includes capabilities for identifying the UE in subscription data, improvements for mobility and interference detection, and reporting. UE subscription information is passed from the HSS to the MME. The MME relays the information to the eNBs. With this feature, the MME supports the Aerial-UE-Subscription-Information IE in the subscription data AVP on S6a interface and in S1AP messages (Handover Request, Path Switch Request Ack, Initial Context Setup Request, and UE Context Modification Request). The procedures are defined in 3GPP TS 29.272, TS 36.413, and TS 36.423.

13.18 MME support for IoT purge timer provisioning range to 30 days (Feature f12005-01)

This feature introduces a new purge timer for IoT devices on the MME. The new purge timer provides the ability to extend the purge timer for IoT devices to 30 days (1 - 720 hours).

With this feature, the provisioning range for the IoT purge timer is 0 to 720 hours. There is no change to the existing 4G Purge Timer functionality.

The IoT purge timer is disabled by default on the MME with value of 0. When the IoT purge timer feature is disabled, the existing purge timer in the range of 1 to 120 hours will continue to apply for all 4G UEs including IoT devices.

The IoT purge timer can be enabled on the MME when provisioned with a value between 1 and 720 hours. When the IoT purge timer feature is enabled, it only applies to the IoT devices. The 4G purge timer continues to apply for regular mobile broadband (MBB) devices.

This feature applies only to 4G IoT devices on the MME.

If this feature is in use and feature MME support for 320 hours unit in the T3412 extended timer (Feature f10409-02) is configured to the maximum values, the UE context (VLR) can be kept on the MME for 413 + 30 days (up to 14 months).

14. CloT optimization

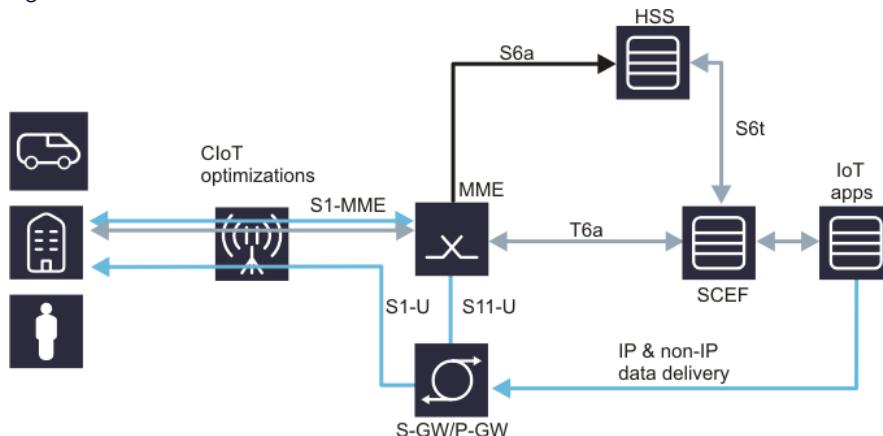
CloT (cellular internet of things) optimization features support IoT devices on LTE WB-EUTRAN and narrow band networks.

MME supports large numbers of IoT devices by supporting the following:

- Highly efficient handling of frequent and in-frequent small data transmissions
- Power savings to prolong battery life by supporting power savings mode (PSM) and idle mode extended DRX (eDRX).
- Simplifications of mobility management and session management procedures
- Paging optimizations for UE requiring extended coverage.

The figure shows the control plane (CP) CloT architecture:

Figure 118: CloT architecture



- UE and network can negotiate to use either control plane (CP) CloT or user plane (UP) CloT for all PDN connections.
- Data is delivered over NAS signaling and S11-U interface; this is the path of the CP CloT.
- Data is delivered over the S1-U interface; this is the path of UP CloT.
- All PDN connections data transport for a UE are either CP (S11-U) or UP (S1-U); switching data transport between control plane and user plane, for example, bearers over control plane (NAS and S11-U) is switched to data radio bearers (DRB) and S1-U.

UE and network can negotiate to use either SCEF-based non-IP Data Delivery (NIDD) or SGi-based NIDD for all PDN connections.

- The light blue line in the figure is the path of SGi-based NIDD; data is delivered over the SGi interface.
- The grey line in the figure is the path of SCEF-based non-IP data delivery; data is

delivered over T6a to SCEF.

14.1 LAP (low access priority) devices (Feature m10115-01)

The *Low access priority (LAP) devices feature provides capabilities to handle signaling traffic generated by a large number of machine type devices on the MME*

The MME supports the following major capabilities with regard to UEs configured with low priority access:

- Recognition and indication to gateway of low priority access UEs
- Overload control enhancements
- Optimization of periodic tracking area update (TAU) signaling
- Use of dedicated nodes for SMS only service
- Separate paging policy
- Separate mobile reachable timer
- Command-line interface (CLI) command enhancement
- Roaming restriction enhancement

Recognition of low priority access UEs and related non-access stratum (NAS) signaling

A UE configured for low priority access indicates to the MME that it is a low priority access UE by including the Device properties information element (IE) in Attach Request, Extended Service Request, or TAU Request and by setting the IE to mobile subscriber (MS) configured for NAS signaling low priority. The MME can use this indication to assign UE to a dedicated CPPS for low priority access UEs. The MME stores the low priority access indication in the UE context. The UE can also include the device properties IE in the following session management messages:

- Bearer Resource Allocation Request
- Bearer Resource Modification Request
- PDN Connectivity Request

The UE low priority access indication is sent over S11 to the gateways (GWs) by including the GTPv2C IE Signaling Priority Indication in the following messages if included by the UE in the PDN Connectivity Request message:

- S11 Create Session Request
- S11 Bearer Resource Command
- S10/S3 Forward Relocation Request (the Signaling Priority Indication IE is included in the

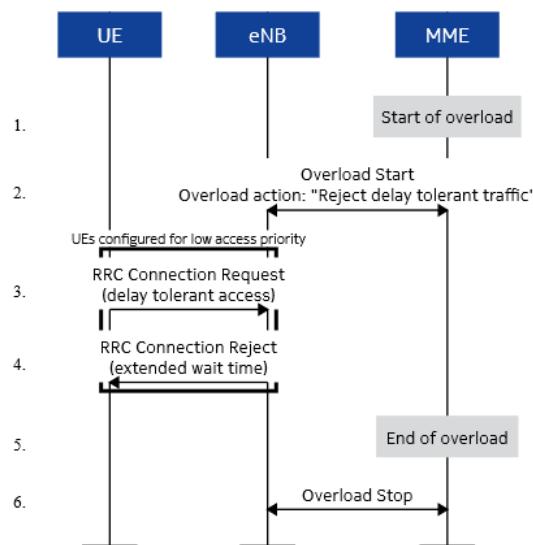
PDN Connection Type IE

- S10/S3 Context Response (the Signaling Priority Indication IE is included in the PDN Connection IE)

MME overload control enhancements – enhanced access barring for LPA UEs

If configured, the MME indicates to the eNB to reject new radio resource controller (RRC) connection requests from UEs that access the network with low priority access in S1AP Overload Start message in case of the MME overload caused by large amount of mobile-terminating call (MTC) traffic, so that the eNB can use access barring to prevent UEs to access the network.

Figure 119: Overload Start/Stop for LPA UEs (enhanced access barring)



MME overload control enhancements - throttling of downlink data notification (DDN) requests

The MME provides a configuration option to indicate the S-GW to selectively reduce the DDN messages for the low priority access UEs when the MME is in overload to reduce the network signaling traffic.

- The MME can indicate to the S-GW in the DDN Acknowledge message using the Data Notification Delay (Throttling Delay) IE and the downlink (DL) low priority traffic throttling IE.
- The MME computes the throttling delay and throttling factor based on the DDN arrival rate impact on the MME overload. Throttling delay and throttling rate can differ from an

S-GW to S-GW.

- For the MME to recognize that the DDN is for low priority traffic, the S-GW is required to include ARP. The MME uses the allocation and retention priority (ARP) to determine the priority of the DDN messages.

MME overload control enhancements – mobility management (MM) and session management (SM) congestion

If configured, the MME rejects a LPA UE Attach/TAU Request and Service Request/Extended Service Request with cause code #22 (congestion) and a provisioned back-off timer supported by the feature *Offloading overloaded CPPSs and support for T3346 timer*, except the MME rejects the LPA UE MM request first.

If configured, the MME also rejects the following LPA UE SM requests with evolved packet system session management (ESM) cause code #26 (insufficient resources) and also includes locally provisioned T3396 timer:

- PDN Connectivity Request
- Bearer Resource Allocation Request
- Bearer Resource Modification Request

Optimized of periodic TAU signaling

To reduce network load from periodic TAU signaling and to increase the time until the UE detects a potential need for changing the radio access technology (RAT) or public land mobile network (PLMN) (for example, because of network problems), the longer values of the periodic TAU timer and mobile reachable timer are supported.

The MME supports local configuration of separate T3412 timer for the LPA UEs and configuration to use the locally provisioned timer value, HSS-provided time value or maximum of the locally provisioned time value, and the HSS-provided timer value.

Separate mobile reachable timer

The MME provides an option to configure a separate mobile reachable timer for the low priority access devices so that these devices can exist in registered state for a long time.

- This timer is started after the expiration of the T3412 timer.
- The MME honors any network requests before the expiration of the timer.
- The UE is detached once the timer is expired.
- The timer is stopped if there is any UE MM activity.

CLI command support

CLI commands allow the operator to obtain the number of registered UEs configured with low priority access and the number of UEs with packet data network (PDN) connections to an access point name (APN).

Roaming restriction

This feature supports the ability to restrict a roamer low priority access UE and provides a configurable option to specify maximum percentage of roamer UEs allowed to access the MME.

Impacts

Transactions are prioritized and served when there is capacity for the transaction priority (overload control).

Low priority IoT devices stop signaling to the network, which allows the network to cope with the overload situations (LAP and back-off timer).

Signaling is reduced from low priority machine-to-machine (M2M) devices (long periodic TAU timer).

This feature requires that Low Access Priority indication is supported by the UE.

14.2 MME support for NB-IoT and EMM-REGISTERED UE without PDN connection (Feature f11701-01)

The **MME support for NB-IoT and EMM-REGISTERED UE without PDN connection feature** supports two important capabilities to support CloT devices: **Narrow Band Internet of Things (NB-IoT)** and **EMM-REGISTERED UE without PDN connection**.

Narrow Band Internet of Things (NB-IoT)

NB-IoT is a 3GPP Radio Access Technology (RAT) that forms part of cellular IoT. This RAT is developed to enable a wide range of new IoT devices and services. NB-IoT allows access to network services via E-UTRAN with channel bandwidth limited to 180 KHz. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Battery life of more than 10 years can be

supported for a wide range of use cases. The term WB E-UTRAN (wide band E-UTRAN) is used to refer to current LTE RAT excluding the NB-IoT. Support of NB-IoT requires eNB to be upgraded to support NB-IoT RAT and dedicated tracking areas for NB-IoT.

MME can be provisioned support NB-IoT only, WB E-UTRAN only, or both NB-IoT and WB E-UTRAN RAT. An MME enabled to support NB-IoT RAT learns the TAs that support NB-IoT RAT through S1AP SETUP or using local provisioning. A NB-IoT device can request an IP PDN connection or a non-IP PDN connection. NB-IoT devices can request SMS service with normal attach and TAU request. 3GPP standards in R13 version of the specifications do not support the following capabilities for NB-IoT devices:

- IMS voice services
- Emergency services
- Intra-RAT handover
- IRAT handover
- Public warning system (such as CMAS, ETWS)
- MBMS
- CSG

EMM-REGISTERED UE without PDN connection

This capability allows a device to be registered to the network without a PDN connection. If this capability is supported by UE and MME, the MME will not detach the UE even if it does not have a PDN connection. A UE at attach time is not required to piggyback PDN Connectivity Request. However, UE can request a PDN connection and request to disconnect a PDN connection any time after attach.

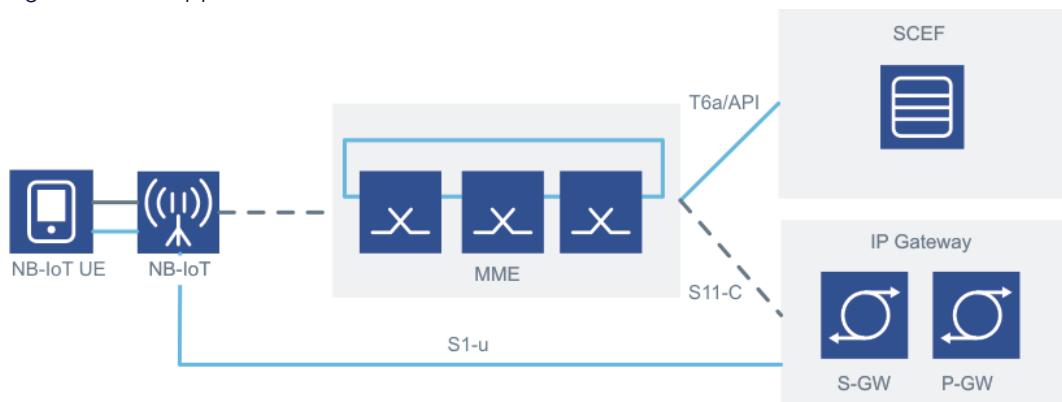
This feature also supports preferred network behavior (PNB) negotiation. The PNB negotiation involves UE indicating support of various IoT capabilities and preference to use control plane optimization and user plane optimization in attach or TAU request. MME can indicate the network support of IoT capabilities and granted IoT capabilities in Attach Accept or TAU Accept message.

This feature would be useful for two types of IoT applications:

- IoT applications that send indications like ON, OFF to a client or server. This type of applications can make use of SMS to send the data instead of a PDN connection. Use of SMS eliminates signaling overhead in setting up a PDN connection to send a small amount of data.
- IoT applications that require infrequent data to be sent using a PDN connection. The PDN connection is only required for the duration of sending the data. Once the data is sent, UE will release the PDN connection so that all the PDN connection resources can be

released.

Figure 120: Support for EMM-REGISTERED UE without a PDN connection



14.3 Extended Protocol Configuration Option (ePCO) (Feature f11711-01)

MME supports extended protocol configuration option (ePCO) per home and shared PLMNs.

The Extended Protocol Configuration (ePCO) IE is added in most of 3GPP messages. The IE has the exact same encoding/decoding logic as in the PCO IE but an extended length of 16 bits; thus it can be used when the existing PCO cannot accommodate the intended content. The ePCO is mainly introduced to expand the size of the current PCO to include items such as APN rate control.

MME supports a maximum ePCO size of 1KB (1024 bytes). MME transparently passes the ePCO between UE and P-GW. There is no need to save ePCO in VLR.

If the feature is enabled and UE indicates the support of ePCO, MME indicates to UE that ePCO is supported by setting ePCO bit in the EPS network feature support IE of Attach Accept and TAU Accept messages. UE indicates support of ePCO by setting the ePCO bit of octet 8 of UE network capability IE.

MME sets the Extended PCO Support Indication bit of Indication flag IE of Create Session Request if UE and MME support ePCO. MME also sends ePCO in Create Session Request if received from UE in PDN Connectivity Request message. MME also sends PCO if it is received from UE.

MME supports reception of ePCO IE in Create Session Response, Create Bearer Request, Update Bearer Request, and other 3GPP messages. If both MME and UE support ePCO, MME

sends the ePCO information in Activate Default EPS Bearer Context Request and Activate Dedicated EPS Bearer Context Request messages.

MME considers the presence of the ePCO IE in message received from P-GW and S-GW as P-GW/S-GW also support ePCO IE.

As part of this feature, most of ESM and EMM procedures are enhanced or extended to add support for encoding or decoding of the ePCO IE. MME sending ePCO support to S-GW/P-GW is based on provisioning on MME and received ePCO support from UE.

3GPP TS 29.274 and TS 24.301 mandate the support of ePCO for NB-IoT UE and/or non-IP PDN data connections for all UEs. A NB-IoT or a UE requesting a non-IP PDN connection may include ePCO in PDN Connectivity Request sent in Attach Request with the assumption that MME and P-GW support ePCO.

14.4 Preferred network behavior provisioning (Feature f11307-01)

This feature introduces support for a provisioning option to select default preferred network behavior when MME has not received Preferred-Data-Mode AVP from HSS for a PDN connection.

This feature provides provisioning to set default preferred network behavior to Control Plane or User Plane. By default, the `defaultPreferredDataMode` global parameter is set to value `Control Plane`.

Once a preferred data transfer is selected, all PDN connections will use the same mode of data transfer irrespective of existence or value of the Preferred-Data-Mode AVP.

14.5 Group service provisioning (Feature f11701-07)

The *Group service provisioning* feature allows feature capabilities and service level agreements to be provisioned for a group of UEs.

The group of UEs is identified by Group-Service-ID AVP of IMSI-Group-ID and the services supported are provided by the Location-Group-ID AVP.

The following bits of Local-Group-ID are supported:

Bit 0 - SGs registration required	The MME expects UE to use SMS over NAS. If a UE does not request SMS service, the MME rejects the UE attach with a provisioned cause code.
Bit 1 - Disable SGs registration	Only EPS attach is allowed. The MME does not support SMS service.
Bit 2 - Attach with PDN connection restricted	<p>If the MME receives attach request with PDN connection and the UE supports ERw/oPDN, the MME does not set up PDN connection.</p> <p>If the UE does not support ERw/oPDN and is provisioned to reject attach request, the MME rejects attach request with EMM cause #19 (ESM failure) and ESM CC #32 (Service option not supported).</p> <p>If the UE does not support ERw/oPDN and is provisioned not to reject attach request, the MME proceeds with the PDN connection and logs a message indicating the inconsistency.</p> <p>The MME only allows a subsequent request for PDN connection when PDN-Connection-Restricted flag in Subscription-Data-Flags AVP is not set.</p>
Bit 3 - SGs-Lite interface to be used	The MME sets up dummy bearers for the UEs via SGs-Lite interface, and sends location update report to GW-TS. Dakota device uses SGs-Lite for combined attach.

This feature is not supported for roammers.

This feature is compliant with 3GPP TS 29.272 v13.8.0 and 3GPP TS 23.003 v13.8.0.

14.6 MME support of NB-IoT/CIoT trials with R12 HSS (Feature f11713-01)

This feature supports a configurable global parameter to send RAT-Type AVP set to EUTRAN for a NB-IOT UE in S6a messages.

Before this feature, for NB-IoT UE, the MME always populates RAT-Type AVP in ULR/IDA with EUTRAN_NB_IOT.

With this feature, the MME can be configured to populate the RAT-Type AVP in ULR/IDA with EUTRAN or EUTRAN_NB_IOT.

For NB-IoT UE, if the global parameter `nbiotRatTypeToHss` is set to Yes, the MME

populates RAT-Type AVP with EUTRAN_NB_IOT as before.

If the global parameter is set to `No`, the MME populates RAT-Type AVP with EUTRAN. By default, the global parameter is set to `Yes`, specifying to send RAT-Type AVP value correctly set.

The MME sends the correct RAT-Type to the gateway irrespective of the setting of the global parameter.

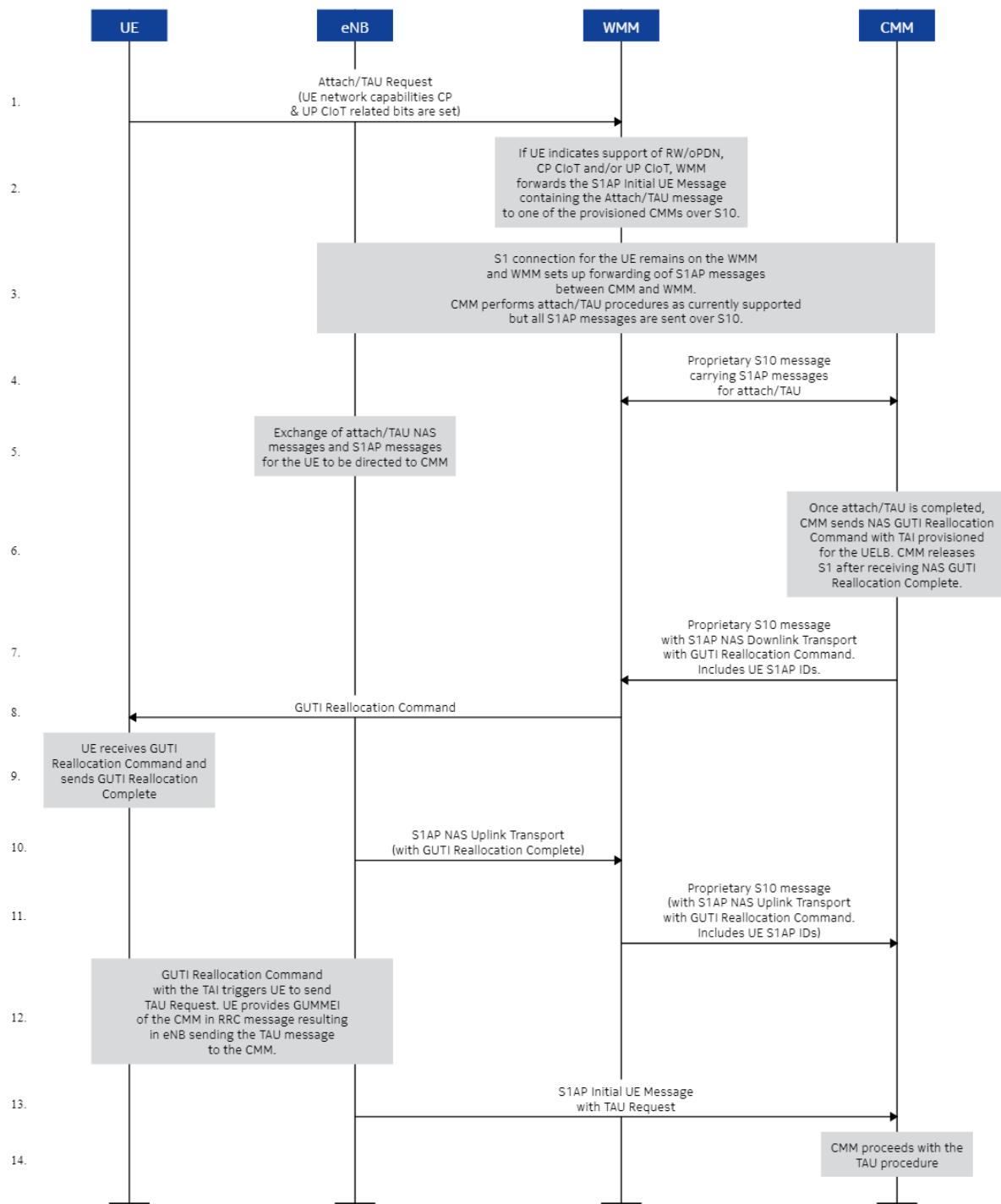
14.7 CMM support for tunneling of S1AP messages associated with CloT Attach/TAU Requests (Feature f11728-01)

The feature supports reception of S1AP Initial UE messages containing CloT Attach/TAU Requests over the S10 interface from a WMM or FNS node, as well as S10 tunneling of DCNR-capable UEs from a FNS node to a CMM node.

The CMM sends and receives all the S1AP messages associated with attach/TAU request procedure over the S10 interface to the WMM. The CMM sends a NAS message GUTI Relocation with a non-broadcasting TAI after the CMM completes the procedure successfully and releases the S1 connection. This triggers the UE to send a TAU Request message and the eNB sends the TAU Request message to the CMM.

The figure shows the procedure details:

Figure 121: Tunneling of S1AP messages associated with CloT Attach/TAU Requests



14.8 MME support for enhancement of CloT interoperability (Feature f11726-01)

This feature allows the service providers to control if the Extended UE Identity Index Value IE is included in S1 Paging messages sent by the CMM to the eNB according to the

needs of their network.

This IE is included in the Paging message by default from this release. However, the service provider can suppress the inclusion of the Extended UE Identity Index Value IE by setting the global parameter `includeExtUeIndexInPagingMsg` to `No`.

The Extended UE Identity Index Value IE was previously introduced to support NB-IoT UEs in applicable networks. This `includeExtUeIndexInPagingMsg` parameter is provided to suppress the inclusion of this IE in networks that have HSSs or eNBs that have not been upgraded yet to support the new AVPs and/or IEs for NB-IoT. In such cases, the presence of the Extended UE Identity Index Value IE adversely impacts standard UEs' access to LTE service.

14.9 CloT traffic control (Feature f11701-06)

With the feature, the MME supports CloT traffic control functions, including PLMN rate control and congestion control for transport of user data via the control plane specified in 3GPP TS24.301 CR2766.

The MME supports PLMN rate control as follows:

- At PDN connection establishment, the MME may inform the UE and the P-GW/SCEF of any local serving PLMN rate control that the serving PLMN intends to enforce for NAS data PDUs. The MME only indicates serving PLMN rate control command to the P-GW if the PDN connection is using S11-U and set to control plane only. The MME only indicates serving PLMN rate control command to the SCEF if that PDN connection is using SCEF.
- Controlling of traffic from and to the CloT UE is supported so that traffic from a CloT UE complies to the traffic parameters locally provisioned traffic parameters. The MME can enforce locally provisioned downlink/uplink rate limit for control plane NAS data. Traffic parameters may include serving PLMN rate control (number of downlink per decihour and number of uplink packets per decihour). The MME drops packets if the rate exceeds the provisioned rate.

The MME supports congestion control for transport of user data via the control plane as follows:

- The MME supports T3448 and the T3448 IE in UE is optional.
- The MME makes congestion control for the transport of user data via the control plane.
- The MME includes a value for the control plane data back-off timer in Attach Accept, Tracking Area Update Accept, Service Accept, or Service Reject message. The MME stores a control plane data back-off timer on a per UE basis if the UE supports the T3448 timer.
- The network may reject the transfer of user data via the control plane initiated by the UE,

based on the stored control plane back-off time for the UE.

The MME has the ability to enable NB-IoT overload throttling during minor overload. When the MME decides to reject NB-IoT request due to overload, the MME uses T3346 timer ranges.

14.10 User plane CloT EPS optimizations - bearer activation without SR (Feature f11701-04)

This feature supports R13 CloT optimizations to activate bearers of a idle UE without using service request procedure.

This feature supports user plane data (user data over S1-U) without the need for using the service request (SR) procedure to establish Access Stratum (AS) context in the serving eNB and UE.

This feature requires UE, eNB and MME to support User Plane CIOT EPS optimizations.

If the UP optimization is supported by UE and MME, the MME indicates to the eNB that UE supports UP optimization. Additionally, UE, eNB and MME is required to support connection suspend and connection resume procedures.

A UE that supports UP CloT always indicates support of S1-U data transfer. Additionally,

- A UE supporting UP optimization can support EMM-REGISTERED without PDN connection and CP CIOT optimization.
- A UE supporting UP optimization can have a PDN connection over S11-U. However, all PDN connections must be over S11-U or S1-U. If the first PDN connection is over S11-U, then all other connections will be over S11-U and vice versa.
- A UE supporting UP optimization can have a SCEF PDN connection.
- A UE in suspended ECM-IDLE state can be in eDRX mode.
- A UE in suspended ECM-IDLE state can be in PSM.

Provisioning

The feature supports activation per PLMN, IMSI range, and TA.

- Use the `upCIoT` parameter in the `uePlmnServices` table to enable user plane (UP) CloT EPS optimization per home PLMN and shared PLMN (by default the capability is disabled). If UP CloT optimization is enabled, S1-U data transfer is also enabled automatically irrespective of provisioning.
- Use the `upCIoT` parameter in the `tai` table to enable UP CloT optimization per TAI. By

default, the capability is enabled for existing TAI and when a new TAI is provisioned. If UP CloT optimization is enabled, S1-U data transfer is also enabled automatically irrespective of provisioning.

- Use the `keepUpCIOtUEs1Bearer` global parameter to keep or delete UP connections if UE moves into a TAI where S1-U data transfer and UP CloT is not supported. By default, UP connections are preserved.
- Use the `s11uBearerSetUp` global parameter to select S11-U bearer setup if a MME is not provisioned to support UP CloT optimization when a UE supporting UP CloT optimization and CP CloT optimization and indicates UP CloT optimization preferred in the Additional update type IE. If the global parameter is set (`Yes`), the MME sets up S11-U bearers and sets the Additional update result IE in Attach/TAU Accept to CP CloT. If the global parameter is not set (`No`), the MME uses the current behavior: standard (or normal) S1-U bearer setup will occur.
- Use the `s1ResumeSecurityContextUpdate` global parameter to enable the inclusion of the security context IE in S1AP UE CONTEXT RESUME RESPONSE message. If enabled, the IE is set as specified in *TS 33.401 clause 7.2.11.4*.
- Use the `s1SuspendSecurityContextUpdate` global parameter to enable the inclusion of the security context IE in S1AP UE CONTEXT SUSPEND RESPONSE message. If enabled, the IE is set as specified in *TS 33.401 clause 7.2.11.2*.

14.10.1 Procedure descriptions

MME supports connection resume and connection suspend procedures, and indicates UP CloT support to the eNB if MME grants UP CloT to a UE.

MME supports the following S1AP messages to support UP CloT optimization:

- UE CONNECTION SUSPEND REQUEST
- UE CONNEXT SUSPEND RESPONSE
- UE CONTEXT RESUME REQUEST
- UE CONTEXT RESUME RESPONSE
- UE CONTEXT RESUME FAILURE

The following messages have the UE User Plane CloT Support Indicator IE to indicate UP CloT support to the eNB if MME grants UP CloT to a UE:

- INITIAL CONTEXT SETUP REQUEST, in the following procedures
 - attach
 - TAU procedure with activation of radio bearers
 - CPSR with radio bearer activation

- service request
- HANOVER REQUEST
- PATH SWITCH REQUEST ACKNOWLEDGE.

If MME determines that UP CloT can be supported for a UE on handover, it indicates support of UP CloT to the target eNB by including the UE User Plane CloT Support Indicator IE in PATH SWITCH RESPONSE and HANOVER REQUEST messages.

If service request is received from a UE that is in suspended, the MME will treat the UE as though it was not in suspended state and proceed with service request as it is currently supported.

For idle mode TAU requests, eNB is notified of MME and UE support of UP CloT optimization when UE sends Service Request.

Attach and TAU

MME indicates to the UP CloT UE that UP CloT data transfer is supported in Attach Accept or TAU Accept if the following conditions are met:

- UE indicates support of UP CloT,
- UP CloT support is enabled for the serving PLMN,
- UP CloT support is enabled for the current TAI,
- there is at least one APN configuration with Preferred-Data-AVP mode is set to Data Over UP Preferred, and
- provisioning indicates support of Data over UP Preferred for UE APN configurations have mix of Data over CP Preferred and Data Over UP is Preferred.

When MME indicates support of UP CloT, it sets all PDN connection data transport over S1-U.

This feature does not support switching of data transport either by MME or UE between CP and UP. Hence, MME rejects UE SR or CPSR indicating establishment is user plane when a UE has all its PDN connections using CP data transport. MME will use the provisioned rejection cause code. Note that switching bearers over S11-U to S1-U is supported through feature *MME support for switching data transport between control plane and user plane* (f11708-01).

A UE indicates support of UP CloT optimization (UP CloT) by setting bit 4 of octet 8 of the UE network capabilities IE. If the UP CloT bit is set, UE must set the S1-U data transfer bit (octet 8, bit 5) irrespective of S1-U provisioning. MME must assume that UE supports S1-U data transfer if the UE indicates the support of UP CloT.

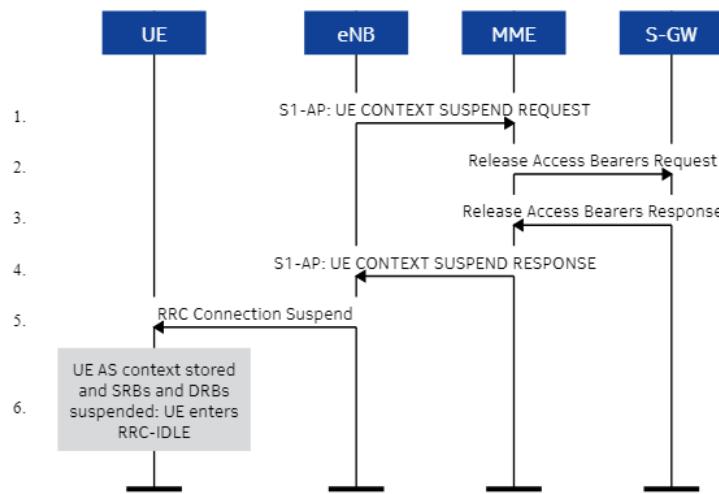
MME UP CloT support is indicated by setting the bit 1, octet 4 of EPS network feature

support IE in Attach Accept and TAU Accept messages.

Connection suspend procedure

MME supports connection suspend procedure as specified in *clause 5.3.4A of TS 23.401*, *clause 5.3.1.3 of TS 24.301*, *clause 7.3a.3 of TS 36.300*, and *TS 36.413*. A connection suspend is always initiated by an eNB supporting UP CloT when the eNB determines to suspend RRC connection.

Figure 122: Connection suspend procedure



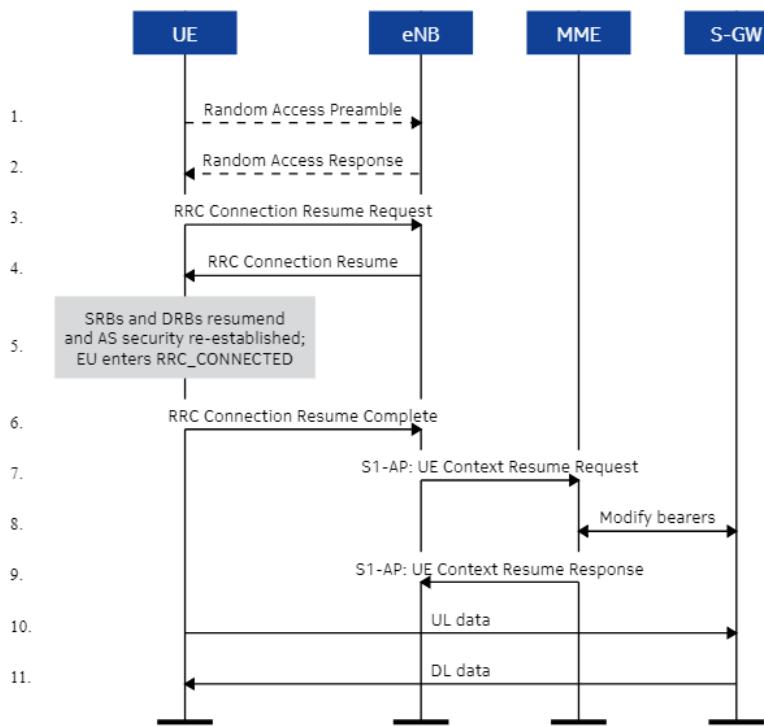
Upon sending the UE CONTEXT SUSPEND RESPONSE message, MME changes the UE state to ECM-IDLE and MME shall keep the S1AP association info, UE context and bearer context necessary to resume the connection. MME saves the Cell Identifier and Coverage Enhancement Level IE for subsequent paging if the IE received in the UE CONTEXT SUSPEND REQUEST.

The information stored at MME is reset if MME receives INITIAL UE message while UE is in suspended ECM-IDLE state.

Connection resume procedure

MME supports connection resume procedure as specified in *clause 7.3a.3 of TS 36.300*.

Figure 123: Connection resume procedure

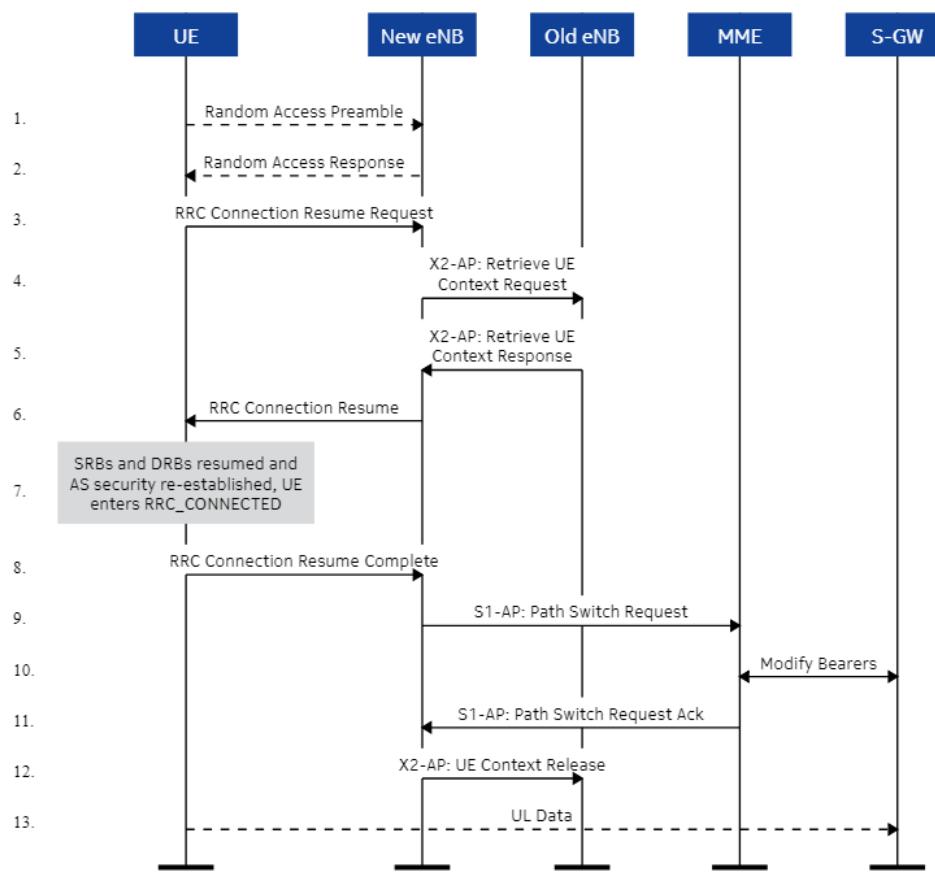


MME actions upon receiving the UE CONTEXT RESUME REQUEST:

- MME sends MBR to S-GW. MME populates the Bearer Contexts to be Removed IE of the MBR with the bearers in E-RABs Failed to Resume List IE and deletes the bearers. MME populates the Bearer Contexts to be modified IE with the remaining bearers.
- If Modify Bearer Response includes the Bearer Contexts marked for removal, MME populates the E-RABs Failed to Resume IE with the bearers in the Bearer Contexts marked for removal IE and include the E-RAB Failed to Resume IE in RESUME CONTEXT RESPONSE.
- If MME fails to setup any bearers, MME will send UE CONTEXT RESUME FAILURE with an appropriate S1-AP cause value.

MME supports connection resume procedure from a different eNB as specified in clause 7.3a.3 of TS 36.300.

Figure 124: Connection resume procedure from a different eNB



An RRC connection can also be resumed in an eNB (the new eNB) different from the one where the connection was suspended (the old eNB). Inter-eNB connection resumption is handled using context fetching, whereby the new eNB retrieves the UE context from the old eNB over the X2 interface. The new eNB provides the Resume ID which is used by the old eNB to identify the UE context.

MME actions upon receiving the PATH SWITCH REQUEST are as currently supported except for the inclusion of the UE User Plane CloT Support Indicator IE if MME continues to support the UP CloT or the UE.

14.11 Switching data transport between control plane and user plane (Feature f11708-01)

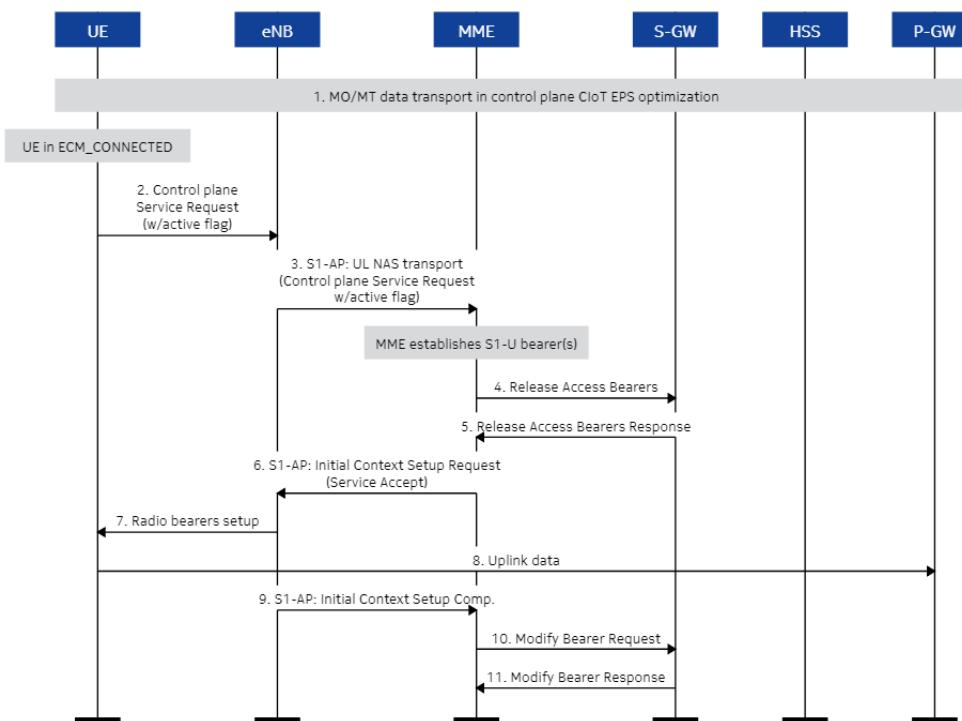
This feature supports switching bearers over S11-U to S1-U, for example, bearers over control plane (NAS and S11-U) are switched to data radio bearers (DRB) and S1-U. This feature supports both WB-EUTRAN UE and UE in NS-S1 mode. The feature does not apply

to SCEF PDN connections.

The MME or UE initiates bearer switching from S11-U to S1-U. A UE initiates the switching by sending Control Plane Service Request with active flag either in ECM-CONNECTED or ECM-IDLE state if the UE determines to send user data at a higher rate. The MME only initiates switching of the S11-U bearers if all the S11-U bearer are not marked with “Control plane only indication”. The MME rejects Control Plane Service Request with active flag to initiate switching if a single S11-U is marked with “Control plane only indication”.

See the following figure for details:

Figure 125: Establishment of S1-U bearer during data transport in control plane CloT EPS optimization



14.12 Current location event report enhancement (Feature f11015-01)

The feature enhances current location event report for current location type for an UE in the idle mode in the MME.

The feature enhances current location event report for current location type for an UE in the idle mode in the MME. The feature enables the MME to send the location report to the SCEF via Reporting-Information-Request (RIR) for an UE in the idle mode upon a query of

current location of an UE from the SCEF if it is allowed by provisioning.

This feature also enables the MME to send the location report to the HSS via IDA for an UE as provisioned when it is possible.

14.13 MME support for sending immediate S6a:IDA for MONTE current location request (Feature f11733-08)

The MME responds with the Insert Subscriber Data Answer (IDA) message via the S6a interface to the HSS before paging the UE, after receiving the request for the current location for the monitoring event (MONTE) in the Insert Subscriber Data Request (IDR) message when both the `pageIdleUe4Location` and `pageIdleUeForLocImmediateIda` parameters in the `ueMonitoringProfile` command are set to Yes.

The MME continues with the paging to determine the current location and send out the event report via the Reporting Information Request (RIR) message over the T6a interface regardless the setting for the `eventReportPreferIda` parameter.

14.14 Inter-UE QoS for NB-IoT UEs using control plane CloT EPS optimization (Feature f11720-01)

The feature allows E-UTRAN to prioritize resource allocation between different NB-IoT UEs when some of the UEs are using the control plane CloT EPS optimization.

The eNB requests the MME to provide the negotiated QoS profile for any UE that is using the control plane CloT EPS optimization.

To reduce signaling load on the MME, the eNB is configured to request the QoS profile from the MME by using the UE's S-TMSI as an identifier. For example, when the eNB's NB-IoT load exceeds certain threshold or when the eNB needs to cache the QoS profile, the eNB is configured to request the QoS profile.

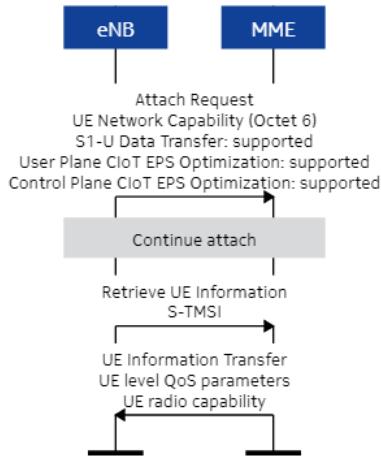
If the UE has more than one active EPS bearer, the MME sends the QoS profile for only one EPS bearer to the eNB. In this case, the MME chooses the non-GBR EPS bearer with the QCI in the highest priority level to determine which EPS bearer's QoS to send to the eNB. If the MME has no active EPS bearer for the UE, the MME does not include the UE level QoS parameters in the S1AP Information Transfer message. The MME always includes the UE Radio Capability IE if available.

The MME supports UE information retrieving and UE information transfer procedures so that

the eNB can request the UE information, including UE level QoS parameters and UE radio capability, from the MME.

When an NB-IoT UE which uses CP CloT EPS optimization sends the Retrieve UE Information message to the MME, the MME responds with the UE Information Transfer message to the eNB as shown in the following figure:

Figure 126: Inter-UE QoS for NB-IoT UEs using control plane CloT EPS optimization



14.15 eDRX cycle 5.12 seconds for EUTRAN (Feature f11603-06)

This feature introduces support for an eDRX cycle length of 5.12 seconds, which is eDRX value 0.

Extended idle mode DRX (eDRX) is a mechanism for extending the idle time (sleeping duration) beyond what is possible with standard discontinuous reception (DRX) used during the paging of UEs. The key benefit of eDRX is the reduction of battery consumption by the UE.

An eDRX cycle length of 5.12 seconds is not associated with an eDRX paging time window (PTW). As a result, a UE using the eDRX cycle length of 5.12 seconds is considered to be always reachable by the MME. There is no need for the MME to wait to page UEs during their eDRX paging time window as is required for other eDRX cycle length values.

Support for the eDRX cycle length of 5.12 seconds is introduced because it can provide the optimal balance between power savings and responsiveness in some use cases.

When this feature is enabled, the MME will allow the use of an eDRX cycle length of 5.12 seconds.

This feature also introduces support for overriding the selection of eDRX value 0. For example, you can provision the MME to assign a different eDRX cycle length when the UE requests eDRX value 0. In addition, you can provision the MME to assign eDRX value 0 when the UE requests another eDRX cycle length.

In addition, this feature introduces paging type `WB_EDRX_0` for use with the paging profile. You can provision the paging policy to indicate the number of page attempts, the T3415 timer interval, and the paging methods used when the MME needs to page a UE that is using an eDRX cycle length of 5.12 seconds.

This feature is only applicable if the overall eDRX feature is enabled in the UE PLMN services (the `edrxEnabled` parameter is set to `true`).

This feature only applies to WB-S1 UEs. NB-S1 UEs are not allowed to be assigned an eDRX value of 0.

14.16 Service gap control (Feature f11730-01)

The service gap control capability feature is intended for controlling the frequency at which CIoT UEs can access the network. This helps to reduce peak load situations when there are a large number of these devices in the network. The MME supports the option to use either locally provisioned service gap timer or service gap timer obtained in the subscription data.

The MME supports the service gap control feature (SGC) for homer and roamer UEs, for shared network, and roamer treated as homer.

The MME accepts the Service-Gap-Time attribute in the Subscription-Data AVP in S6a messaging from the HSS and stores the received value in the UE context. The MME accepts updates to the service gap timer in subsequent Insert-Subscriber-Data-Request (IDR) operations.

- The service gap timer can be overwritten through local provisioning.
- If the HSS updates the service gap timer, the MME provides the new value to the UE at the next TAU or attach.

The MME implements withdrawal of service gap time from UE subscription per 3GPP TS 29.272 CR 0797.

The MME sends the UE its service gap timer (T3447) as part of the attach and TAU procedures if all of the following are true:

- The SGC feature is active in the MME.
- The UE identified itself during the attach or TAU procedure as supporting SGC (in the UE

network capability IE).

- The UE context at the MME contains the UE gap timer (provided by the HSS in the subscriber profile).
- The MME does not reject the attach or TAU (for example, due to SGC).

Note:

- The UE does not include SGC capability for periodic TAU.
- If the UE receives a service gap timer in the attach or TAU procedure, the UE activates its SGC per 3GPP procedures. If the UE does not receive a service gap timer after having indicated support in the attach or TAU procedure, the UE deletes its service gap timer if present.
- A pre-R15 UE does not support the service gap timer. Not all R15 UEs will support the timer.

The MME has a global flag to specify whether the MME is to provide a back-off timer T3346 if the MME rejects a UE access attempt due to SGC. If the MME rejects the attach or TAU due to service gap control, the MME sets the cause to #22 (congestion). The MME includes the back-off timer T3346, set to the remaining T3447 time, if provisioned.

The MME starts the SGC T3447 timer in the UE context if all the following conditions are met:

- The UE transitioned from ECM_CONNECTED to ECM_IDLE (S1 connection is released or suspended).
- T3447 is not already running for the UE.
- The SCG feature is active in the MME.
- The UE context in the MME has a service gap timer as provided by the HSS.
- The UE established the prior S1 connection (entered ECM-CONNECTED mode) due to an event other than paging, attach request without PDN connection request, or TAU without the active or signalling active flag set.

When the T3447 timer is running for a UE context in the MME, the MME allows that UE service for:

- attach requests for emergency bearer services
- attach requests without PDN connection request
- TAU requests without the active or signalling active flag set
- MT service requests triggered by paging and subsequent MO signalling or MO data, if any, until the UE enters EMM-IDLE

The MME keeps the T3447 timer running if the UE:

- transits to EMM-CONNECTED for the above cases
- enters EMM-DEREGISTERED state
- powers off

The T3447 timer value used by the MME depends on whether the UE identified itself as supporting the SGC feature during its prior attach or TAU procedure. If the UE supports SGC, the MME sets T3447 to be 4 minutes less than the Service-Gap-Time in the UE context (or 0 if T3447 would otherwise be negative). If the UE does not support SGC, the MME sets the T3447 timer to be the service gap time in the UE context.

The MME supports the following provisioning:

- Global feature activation to specify whether the MME is to apply SGC monitoring for the applicable UEs registered on the MME.
- Per UE PLMN service feature activation for the SGC feature. Note: IMSI-based level activation is not used.
- Local provisioning to override the SGC value sent by the HSS in the subscriber profile. A separate override applies for homers and roammers.

Note:

The override applies only if the HSS includes service gap timer in the subscriber profile. The MME never adds SGC timer to the UE profile if the HSS did not include an SGC timer.

- Global parameter to specify whether the MME is to provide a back-off timer T3346 if the MME rejects a UE access attempt due to SGC.

14.17 NIDD and IP via S11/SGi

CIoT features enabling non-IP data delivery (NIDD) via S11/SGi.

14.17.1 Extended NAS timer values (Feature f11707-01, f11707-02)

This feature supports large timer values for NB-IoT UE and CAT M1 mode B UE to support coverage enhancement capability.

MME supports provisioning to choose an increment to be added to the current NAS mobility management and session management timers. This feature supports full functionality but

feature testing was limited to limited scenarios to support IoT trials.

Table 66: Timers

Parameter	Type	Value range	Default
<code>t3422Wbs1CeMode</code>	timer, EMM	1 - 60 s	24
<code>t3450Wbs1CeMode</code>	timer, EMM	1 - 60 s	18
<code>t3460Wbs1CeMode</code>	timer, EMM	1 - 60 s	24
<code>t3470Wbs1CeMode</code>	timer, EMM	1 - 60 s	24
<code>t3485Wbs1CeMode</code>	timer, ESM	1 - 60 s	16
<code>t3486Wbs1CeMode</code>	timer, ESM	1 - 60 s	16
<code>t3489Wbs1CeMode</code>	timer, ESM	1 - 60 s	12
<code>t3495Wbs1CeMode</code>	timer, ESM	1 - 60 s	16
<code>s1hoCompleteExtended</code>	timer	5 - 100 s	5
<code>catM1bPagingTimerIncr</code>	global parameter	1 - 100 s	0
<code>nbIotEmmTimerIncr</code>	global parameter	0 - 240 s	0
<code>nbIotEsmTimerIncr</code>	global parameter	0 - 180 s	0
<code>nbIotPagingTimerIncr</code>	global parameter	0 - 240 s	0

Timers `t3422Wbs1CeMode`, `t3450Wbs1CeMode`, `t3460Wbs1CeMode`, and `t3470Wbs1CeMode` replace global parameter `catM1bEmmTimerIncr`.

Timers `t3485Wbs1CeMode`, `t3486Wbs1CeMode`, `t3489Wbs1CeMode`, and `t3495Wbs1CeMode` replace global parameter `catM1bEsmTimerIncr`

The *Extended NAS timer values – Phase 2 (f11707-02)* feature completes the feature testing in CMM17.5.

Related descriptions

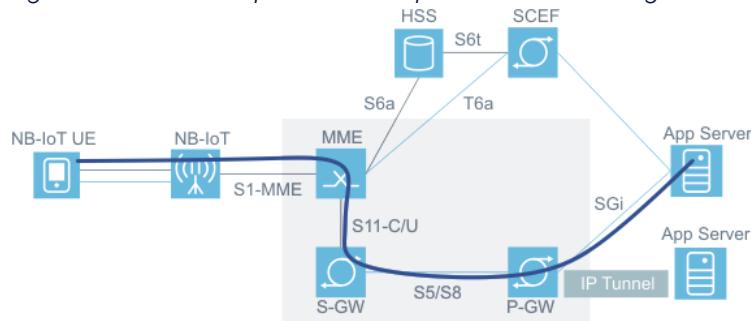
- [Release 13 and Release 14 standards update for MME \(Feature f10002-01\)](#)

14.17.2 Control plane CloT EPS optimizations for both non-IP data and IP through SGi (Feature f11701-03)

The **Control plane CloT EPS optimizations for both non-IP data and IP through SGi** feature supports transport of small non-IP data or IP data between Internet of Things (IoT) device and application in non-access stratum (NAS) signaling depending on the data type selected and the supported packet data network (PDN) connection at PDN connection establishment.

This feature introduces a new S11-U interface that enables MME to transport small user data. UE and MME use PNB negotiation to select data transport over the new control plane or existing user plane (S1-U). Exchange of data over control plane does not require setting of radio bearers. MME uses APN configuration to determine whether to set up an IP connection or non-IP connection.

Figure 127: Control plane CloT optimizations through SGi



Both NB-IOT and WB-EUTRAN UEs can make use of this capability.

This feature eliminates overhead involved with setting of radio bearers for IoT applications that send small amount data infrequently. The non-IP PDN connections are useful to reduce the overhead of IP header for small data packets for some applications.

This feature is supported on home and shared PLMN but not for roaming PLMN.

Both non-IP data and IP data can be transported through SGi when either of the following conditions is fulfilled:

- Data transport over control plane (when S11-U is correctly configured).
- Data transport over user plane (when MME support for S1-U is correctly provisioned).

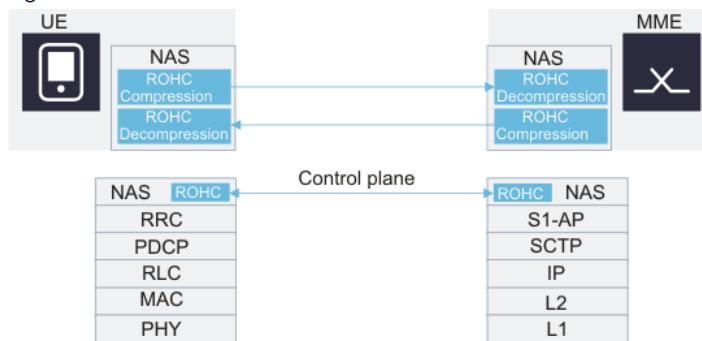
Alarm `40524 LSS_externalLinkDown` is raised when S11-U link is down.

14.17.3 Robust Header Compression (ROHC) (Feature f11701-09, f11701-10)

This feature supports robust header compression to compress IP headers to reduce the packet size of IP packets of an IP PDN connection over control plane.

The MME compresses IP data when the downlink data is transferred from the S-GW to the UE. For the uplink data, the MME acts as a decompressor.

Figure 128: ROHC



The feature supports the following ROHC profiles:

- UDP/IP (profile 0x0002) (RFC 3095)
- ESP/IP (encapsulating security payload) (Profile 0x0003) (RFC 3095)
- IP (profile 0x0004) (RFC 3843 and RFC 4815)
- TCP/IP (profile 0x0006) (RFC 4996)

Profiles are different types of header compression algorithms at a specific network layer.

Header compression contexts (including the type of profile, the number of context IDs supported, and CP-IoT features) are exchanged and negotiated between the MME and the UE based on the provisions made by the MME and UE capacities.

ROHC IEs are included in the following procedures based on which uplink/downlink data headers can be compressed or decompressed once the procedure is successful:

- Attach procedure
- PDN connectivity procedure
- Tracking area update procedure
- Inter-MME handover procedure
- UE-initiated bearer modification procedure

The *Robust Header Compression (ROHC) – Phase 2* feature (f11701-10) completes the feature testing in CMM17.5.

14.17.4 MME support for S11-U downlink user data buffering (Feature f11701-11)

This feature supports buffering of 1 to 3 S11-U downlink user data if MME is awaiting UE response for a signalling or session management procedure.

MME will send the buffered data after the completion of the procedure, if the outcome of the procedure allows MME to send downlink data. Otherwise, MME drops the downlink user data.

This feature uses the NAS NON-DELIVERY INDICATION introduced in feature *Control plane CloT optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF)* (f11701-02). MME will buffer any downlink packets received over S11-U, if MME is waiting for NAS NON-DELIVERY message. If MME receives NAS NON DELIVERY INDICATION, MME will resend the downlink packets on first come first basis.

The maximum number of downlink user data packets buffered will be 3 for all the PDN connection. The average size of data packets is around 128 octets and maximum size supported of 1400 octets.

MME supports a global parameter `s11uDlDataBuffering` to activate this feature. By default, the feature is deactivated. If the feature is not activated, then MME will use current behavior of sending S11-U packets. This feature extends the capability to the Delete Session Request.

14.17.5 MME support for non-IP with S1-U transferred (Feature f11723-01)

This feature adds support for non-IP PDNs over S1-U.

With this feature enabled,

- MME supports non-IP PDNs over S1-U for WB-EUTRAN (eMTC) and NB-IoT UEs which are neither allowed UP CloT nor CP CloT.
- If `upCiot` parameter is enabled under `uePlmnServices` and an UE is allowed UP CloT as in feature *User plane CloT EPS optimizations* (f11701-04), MME supports non-IP PDNs over S1-U for such UEs.

This feature is applicable for home subscribers and treat as home subscribers for WB-EUTRAN (eMTC) and NB-IoT UEs in home and shared PLMN.

When the feature is enabled, the MME determines non-IP PDN type support as follows:

- UE sends PDN request with PDN type set to non-IP
- Non-IP-PDN-Type-Indicator AVP in APN configuration is set to TRUE and
- Non-IP-Data-Delivery-Mechanism is set to SGi-BASED-DATA-DELIVERY

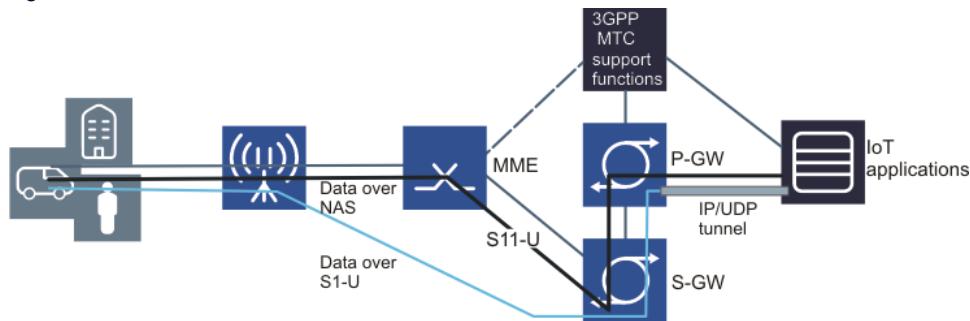
In addition, MME checks non-IP PDN type is set in CIOT features in the Node features IE, for establishing the non-IP PDN with an S-GW.

Non-IP type support for S1-UP bearer is independent with CP optimization or UP optimization.

MME indicates support of feature Non-IP PDN type APNs to HSS in Supported-Features AVP (ULR/ULA and IDR/IDA), in the same way as in feature *Control plane CloT EPS optimizations for both non-IP data and IP over SGi* (f11701-03). If the MME does not indicate support of this feature in the ULR command, the HSS does not send APN configurations with a non-IP PDN type in the subscription data sent in ULA or in IDR, and does not send IDR commands with the only purpose to update such subscription data. If the Update Location Request is received over S6a, from an MME that does not support the non-IP PDN type APNs feature, and the user's subscription profile contains only APN configurations of type non-IP, the HSS returns a result code of DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION.

Also, as with feature f11701-03, MME supports Additional-Context-Identifier in APN-Configuration-Profile AVP. If present, the Additional-Context-Identifier AVP identifies another default APN configuration, only for those subscriptions containing both, APNs with an IP-based PDN type and APNs with a non-IP PDN type; in this case, each of those two default APN configurations have a different PDN type category (one default APN with an IP-based PDN type, and another default APN with a non-IP PDN type).

Figure 129: Non-IP with S1-U



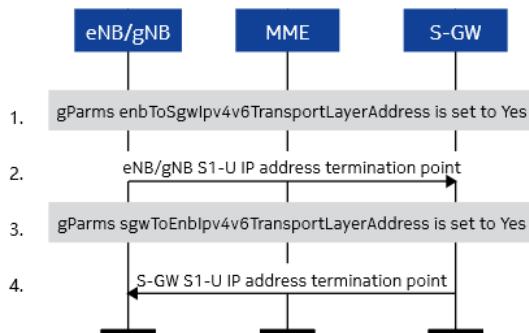
If the UE requests for non-IP PDN Type and this is not enabled at the MME, the request will be rejected with provisioned cause code. The MME will use EMM CC #19 (ESM Failure) and ESM CC #32 (Service Option is not supported) in the Attach Reject message.

This feature can be enabled through parameter `allowNonIpOverS1u` in UE PLMN services.

14.17.6 IPv6 address selection when presented with IPv4/IPv6 in transport layer address (Feature f11723-02)

This feature allows the MME to support and pass the S1-U transport layer address (TLA) of IPv4v6 address type received in either the S-GW or the eNB.

Figure 130: S1-U transport layer address (TLA) of IPv4v6 address type



In case the global parameters `enbToSgwIpv4v6TransportLayerAddress` and `sgwToEnbIpv4v6TransportLayerAddress` are set to `No`:

When the MME receives IPv4/IPv6 S1-U transport layer address from the eNB, the MME sends single IP to the S-GW that matches the eNB S1-C IP type.

When the MME receives IPv4/IPv6 S1-U transport layer address from the S-GW, the MME sends single IP to the eNB that matches the eNB S1-C IP type.

14.18 NIDD via SCEF

CIoT features enabling non-IP data delivery (NIDD) via services capability exposure function (SCEF).

14.18.1 Control plane CiOT optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF) (Feature f11701-02)

The Control plane CiOT optimization for non-IP data delivery (NIDD) via Services Capability Exposure Function (SCEF) supports the exchange of non-IP data packets over the T6a interface. The MME and SCEF node exchange non-IP data packets over the T6a interface

using Diameter/SCTP/IP protocol stack.

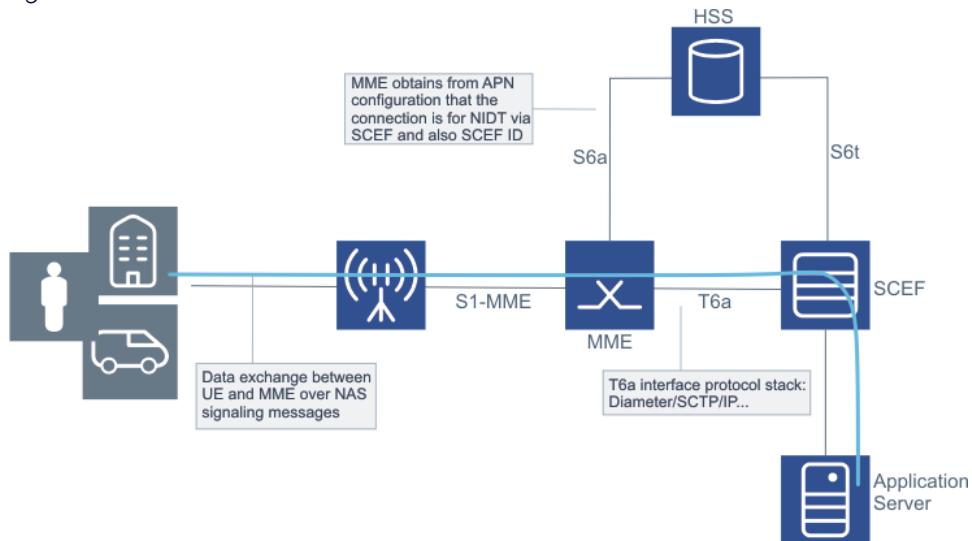
NB IoT architecture

IoT applications require non-IP data transfer between application servers and CloT devices. Support for non-IP data delivery is part of CloT optimization features. The CMM supports non-IP data delivery through the following mechanisms:

- Non-IP data delivery (NIDD) over T6a / SCEF (this feature)
- Non-IP data delivery over S11-u / GW / SGi (Control plane CloT EPS optimizations for both non-IP data and IP through SGi (Feature f11701-03))

The following graphic shows the architecture for NIDD over T6a/SCEF.

Figure 131: NIDD over T6a/SCEF architecture



In the 3GPP architecture, the Service Capability Exposure Function (SCEF) securely exposes the services and capabilities provided by the 3GPP network.

The SCEF node uses the T6a and S6t interfaces for registration procedures. The UE registers with the SCEF (for bearer availability) and the application server registers with the SCEF as the application for a UE.

- S6t - interface is between the SCEF and HSS. Diameter commands include NIDD Information Request and NIDD Information Answer.
- T6a - interface is the interface between the MME and the SCEF. Diameter commands include the following:
 - Connection Management Request and Connection Management Answer
 - Mobile-Originated Data Request and Mobile-Originated Data Answer
 - Mobile-Terminated Data Request and Mobile-Terminated Data Answer

The following capabilities are delivered with this feature.

- Establishing T6a interface to SCEF
- Selection of SCEF based on APN configuration in UE subscription data
- Exchange of mobile originated and mobile terminated data between MME and SCEF using T6a
- Simultaneous support of S1-U bearers and T6a bearers (that is, NIDD via SCEF)

The feature does not support roammers and simultaneous support of S11-U and T6a bearers.

 **Note:**

Support for S11-U and T6a bearers is provided with feature *Simultaneous support of SCEF with S11-U (f11701-12)*.

Provisioning

The feature supports the following provisioning:

- CP CloT Delivery Mechanism – This parameter is supported per home PLMN and shared PLMN and enables or disables support of data transfer over SGi (S11-U) and/or SCEF (T6a). Valid values SGi only, SCEF only, or all. The default is SGi only.
- SCEF Diameter and SCEF provisioning. For this release, MME sets up the SCTP association and Diameter connection to a SCEF using provisioning data. SCEF provisioning consists of the following:
 - SCTP parameter provisioning
 - Diameter parameters profile - at least two DRAs
 - SCEF IPv4/IPv6 address
 - MME T6a termination IPv4/IPv6 address - maximum number is 128

The SCEF nodes and/or end points can be provisioned into groups:

- The maximum number of groups supported is 64.
- The maximum number of SCEF modes within a group is 16.
- SCEF nodes within a group can be provisioned in load sharing or in primary/secondary configuration.
- All SCEF nodes within a group have the same UE context and MME can send T6a messages to any SCEF mode within a group.

The following parameters are also configurable:

- Delete T6a connection of UE if UE moves into a TA that does not support CP CIOT - if

enabled, the MME deactivates the SCEF PDN connections when the UE moves in to a TA that does not support CP CIOT. If disabled (the default), the MME maintains the SCEF PDN connections when UE moves in to a TA that does not support CP CIOT, and the MME handles all interactions between MME and SCEF as though the CP CIOT capabilities for T6a are enabled.

- Retry different SCEF – When MME receives certain errors from SCEF (too busy, out of space, unable to deliver) or if the SCEF does not respond (timeout), the MME sends one retry request to another SCEF by selecting the next available SCEF from the same SCEF group. By default it is disabled.
- Connection Management Answer timer – Time to wait for receiving or responding to Connection-Management-Answer (CMA) after sending Connection Management Request (CMR) or receiving a CMR Release request from the SCEF.
Range: 100 to 6000 milliseconds, in increments of 100 milliseconds. The default is 1000 milliseconds.
- SCEF CMR Answer Timer – This timer is used for responding with CMA to the SCEF that sent CMR for an update. The timer applies to SCEF CMR updates other than T6a connection release. CMR for Release from SCEF answer uses the Connection Management Answer timer.
Range is 100 to 30000 milliseconds, in increments of 100 milliseconds. The default: 12000 milliseconds
- MO-Data-Answer (ODA) timer – Time to wait for ODA after sending ODR (MO-Data-Request).
The range of values is from 100 to 6000 milliseconds, in increments of 100 milliseconds. The default is 1000 milliseconds.
- MT Data Answer Timer – This timer is used for responding to SCEF with TDA when the SCEF sends TDR and does not include the SCEF-Wait-Time AVP. Operators must ensure that the MT Data Answer timer is larger than the time to complete all the paging attempts if the MME is required to page a UE upon the receipt of the TDR. If the SCEF sends the SCEF-Wait-Time AVP, operators must ensure that all the page attempts must be completed before the SCEF-Wait-Time expires.
The range of values is from 100 to 30000 milliseconds, in increments of 100 milliseconds. The default is 12000 milliseconds.
- Control Plane User Inactivity Timer – This timer is used to detect user inactivity and releases the S1 connection of the UE that has user data over NAS only.
The range of values is from 500 milliseconds to 10000 milliseconds in increments of 100 seconds. The default is 3000 milliseconds.
- NAS NON-DELIVERY INDICATION message handling. It is disabled by default.
- SCEF High Latency Communication Support - This parameter indicates to the MME whether SCEF supports buffering of MT data if the UE is not reachable due to power

savings. It is enabled by default.

- Accept TAU with active flag or CPSR with active flag when a UE has only SCEF PDN connections. It is enabled by default.

For configuration details and examples, see the *MME User Guide*.

SCEF selection based on APN configuration

The MME supports T6a connection establishment during attach UEs that are allowed for NIDD via SCEF. That is, the APN configuration's Non-IP-PDN-Type-Indicator AVP is set to "TRUE" and Non-IP-Data-Delivery-Mechanism is set to "SCEF-BASED-DATA-DELIVERY". The MME uses the SCEF ID AVP in APN configuration data to select a provisioned SCEF or DRA to send T6a Connection Management Request (CMR) command.

The MME use the SCEF-ID AVP that it received in the subscribed APN associated to the T6a connection at its establishment as the Destination-Host AVP and the Destination-Realm AVP in the Non-IP data related request commands sent over the T6a interfaces.

If the SCEF ID and/or SCEF realm is not received, the MME uses the default SCEF ID and SCEF realm, if provisioned.

 **Note:**

Default SCEF ID and SCEF realm are only supported with DRA remote end-points (for example, parameter `draSupported` is enabled). When the end-point is a direct connection to an SCEF (for example, `draSupported` is disabled), the learned SCEF Identity is used as default - provisioned DRA parameters on an end-point or a rule (Destination Host or Realm) are not used.

If SCEF (that is, the NIDD feature via SCEF) is not enabled, then MME takes actions as follows:

- If the MME and UE support "Attached to EPS without PDN connection", the MME proceeds with the Attach request with PDN connection request even if the MME fails to set up PDN connection for any reason. In this case, MME sends the Attach Accept message with PDN connection reject with cause value "Service option not supported" (cause #32). The UE is expected to send Attach Complete message with ESM DUMMY message to the MME.
- If MME or UE does not support "Attached to EPS without PDN connection", then MME rejects the Attach Request with provisioned ESM cause code and PDN connectivity request with cause value "Service option not supported" (cause #32).

For PDN connections over T6a, the MME always set the bit 1 of "Control plane only indication" IE of the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to indicate

to that the PDN associated with the bearer is only for CP CloT optimization and the bearer is not switched to use S1-U.

Diameter error code handling

The MME handles Diameter error codes as follows:

- Received during connection establishment: MME actions depend on whether the UE and MME supports “Attach without PDN Connection”.
- Received during connection update: the MME deactivates the PDN connection with reactivation required and detach the UE with reattach indication if the PDN connection is the last connection and if UE is not allowed to be attached without a PDN connection.
- Received during connection release: the MME continues with the procedure and may log a message.
- Received during MO data request: the MME deactivates the PDN connection with reactivation required and detach the UE with reattach indication if the PDN connection is the last connection and the UE is not allowed to be attached without a PDN connection.

Related descriptions

- [Simultaneous support of SCEF with S11-U \(Feature f11701-12\)](#)

14.18.2 MME support for CloT monitoring procedures (Feature f11702-01)

This feature uses the T6a interface from the MME to report events of interest from specific UE and services on the 4G network. When the MME receives UE subscriber data from the HSS, monitoring configurations are present in the HSS data, and this feature is enabled on the MME, specific reports can be enabled.

This feature supports monitoring event configuration and deletion via the HSS as specified in 3GPP TS 23.682. The MME supports to report monitoring event to the service capability exposure function (SCEF) via the T6a interface.

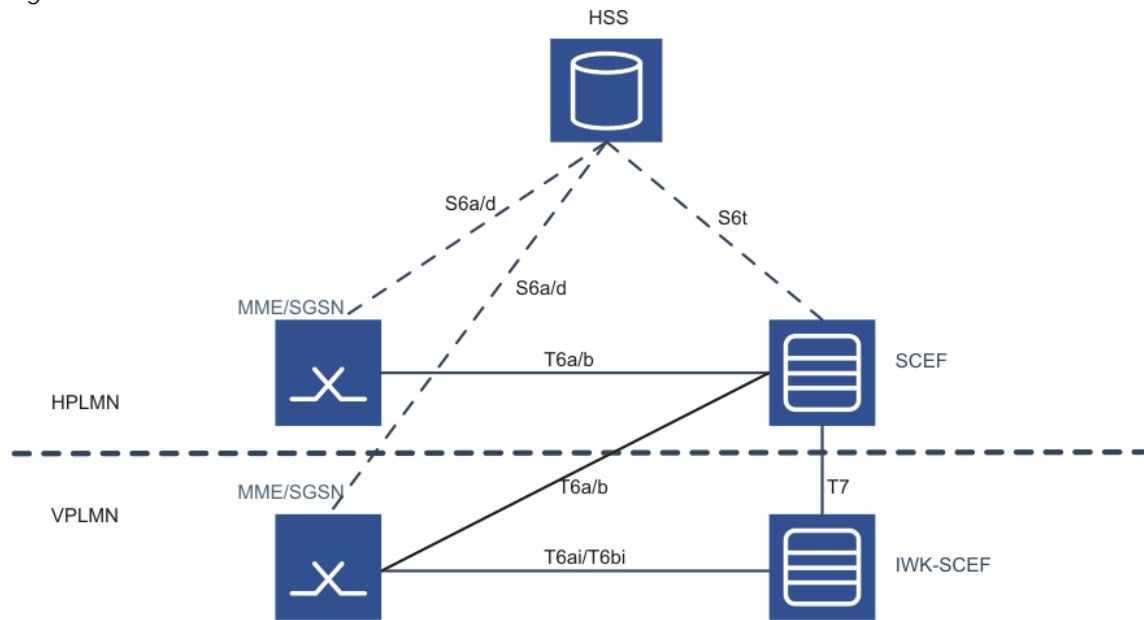
The MME supports the following events:

- Location of the UE and change in location of the UE
- Loss of connectivity (mobile reachability timer expired)
- UE reachability (sent when UE transitions to connected mode)
- Availability after Downlink Data Notification (DDN) failure

When a UE-related event or condition is present for reporting, the applicable monitoring events are reported to one or more SCEFs based on the monitoring event configuration received from an HSS in the UE subscription data. The SCEF used to report a monitoring event is identified by SCEF-ID and SCEF-Reference-ID.

The architecture figure shows the monitoring interfaces:

Figure 132: Architecture



- The S6a interface allows the MME to receive monitoring events configuration and deletion from the SCEF via an HSS.
- The T6a interface allows the SCEF to receive reports of the monitoring events from the MME.

Complete monitoring event solution covers the following scenarios:

- monitoring event configuration for home
- monitoring event configured by the SCEF via the HSS
- monitoring event detection by the MME after the event is configured
- report monitoring events by the MME to the SCEF (via T6a)
- transfer and handle monitoring event data over S10

Roaming support and interworking with IWK-SCEF is not included.

Related descriptions

- [Sending AADDNF notification during eDRX and send LoC when entering PSM \(Feature f11702-04\)](#)
- [PDN connectivity status event reporting \(MONTE\) \(Feature f11733-04\)](#)

14.18.3 CMM support for Rel 16 MONTE and CloT CRs (Feature f11733-11)

The feature updates the existing monitoring event (MONTE) and CloT functionality with 3GPP R16 CRs.

Table 67: CMM support for Rel 16 MONTE and CloT CRs

Standard/CR	Description
3GPP TS 29.272 v16.1.0 CR 0810	<p>This CR supports access restrictions within the Access Restriction Data AVP in S6a messaging for LTE-M and WB-E-UTRAN. The CMM supports these access types from the ARD AVP. The CMM supports the NB-IoT access type from the same AVP, which was added in an earlier CR.</p> <p>The CMM supports pairs of cause codes (homer and roamer) in the <code>restNasMappingProfile</code> command for each IoT RAT: NB-IoT, LTE-M, WB-E-UTRAN, excluding LTE_M.</p> <p>For scenarios where the LTE-M access is allowed but the WB-E-UTRAN access is not allowed for the UE due to the HSS access restriction data or local provisioning in the svcAgreement profile, the MME sends UE Radio Capability Match Request message to the eNB. Based on the eNB UE Capability Info Indication Response message, the MME either accepts or rejects the LTE-M. Similar logic applies when the LTE-M access is not allowed but the WB-E-UTRAN access is allowed for the UE.</p> <p>Command <code>plmn ueRadioCapabilityMatch</code> must be set to <code>true</code> to enable the current implementation.</p>
3GPP TS 29.128 v16.1.0 CR0075	This CR supports the cause code Reachability-Cause AVP in the UE reachability monitoring event report. Possible values are <code>CHANGE_TO_CONNECTED_MODE</code> and <code>REACHABLE_FOR_PAGING</code> .
3GPP TS 23.401 CR 3486	This CR supports serving PLMN rate control per PDN/APN connection.
3GPP TS 23.401 CR 3461	This CR allows the S1 release procedure when the S1 UE Context Release Request message comes with cause User inactivity and drops when one of the following conditions is fulfilled:

- If there is any pending downlink traffic or session signaling.
- When the MME receives the NAS ReleaseAssistanceIndication showing that downlink data is expected.

Standard/CR	Description
3GPP TS 29.272 v16.1.0	If the CMM supports the External-Identifier, the External-Identifier is included in Reporting Information Request message. The External-Identifier allows the CMM to receive the External-Identifier in the subscription data and to be prepared to modify and delete the External-Identifier in the subscription data over the S6a interface. Up to five External-Identifiers are allowed per user.

14.18.4 PDN connectivity status event reporting (MONTE) (Feature f11733-04)

With PDN connectivity status monitoring event, the MME notifies the SCEF when a PDN connection is created or deleted for the UE. The PDN connectivity status event report includes the IP address allocated for the UE PDN connection, the PDN type, the APN, the interface (T6a or SGi), and the PDN status. The event is configured at the MME via S6a (IDR and ULA).

This feature supports the PDN connectivity status event. The feature builds on the set of MONTE events and reports defined in feature *MME support for CIoT monitoring procedures* (*f11702-01*).

The MME supports the following capabilities as part of this feature:

- Recognizes the PDN-Connectivity-Status-Configuration on S6a and stores it in the VLR and UE context.
- Sends the PDN connectivity status event either via the HSS using Insert-Subscriber-Data-Answer (IDA) or directly to SCEF using Reporting Information Request (RIR). Provisioning determines whether the first report is sent via IDA or RIR.
- Updates the event in the VLR and UE upon changes in UE subscription on S6a or errors in the T6a Reporting-Information-Answer (RIA).
- Notifies the SCEF for the PDN connectivity status report on a per-UE basis, provided that the UE is subscribed to the event and that the global feature control is active.

PDN-Connectivity-Status-Report includes:

Service-Selection This is the APN.

PDN-Connectivity-Status-Type CREATED (0)/DELETED (1)

PDN-Type	IPv4, IPv6 or IPv4v6. The value IPv4_OR_IPv6 is not used for this event reporting. If PDN-Type AVP is present, the Non-IP-PDN-Type-Indicator and Non-IP-Data-Delivery-Mechanism AVPs will be absent.
Non-IP-PDN-Type-Indicator	Indicates whether the PDN connection is of type Non-IP. If this AVP is present, it is set to TRUE and the PDN-Type AVP will be absent.
Non-IP-Data-Delivery-Mechanism	This will be present if the Non-IP-PDN-Type-Indicator AVP is present and set to TRUE.
Served-Party-IP-Address	It may be present 0, 1 or 2 times, and contain the IP address(es) used by the UE, if available.

Apart from these AVPs, it may include the following non-standard AVPs based on the provisioning:

Bearer-Identifier	EPS bearer ID
RAT-Type	RAT type
MIP6-Agent-Info	The P-GW IP information (FQDN and/or S5/S8 IP addresses)

Note:

- There is no additional control to specify whether to include FQDN and/or IP addresses for MIP6-Agent-Info. The MME will send whatever is available.
- The AVP MIP6-Home-Link-Prefix is not used in S6a/S6d (and will not be set by the MME in this application), but it is included in the above definition to reflect the complete IETF definition of the grouped AVP.
- The MIP6-Agent-Info settings as used in PDN connectivity status report are independent from those specified in feature *Sending P-GW IP in NOR (f10169-01)*.

The report is generated not only when a PDN is created or deleted, but also at event configuration by IDR.

The MME supports:

- Setting/clearing of the PDN connectivity status monitoring event configuration in the UE

context as part of the S6a-RSR (Reset-Request) procedure and S6a-IDR procedure.

- Clearing of the PDN connectivity status monitoring event configuration in the UE context as part of the S6a-DSR (Delete-Subscriber-Data-Request) procedure and S6a-CLR (Cancel-Location-Request) procedure.

 **Note:**

- SCEF-Reference-ID-for-Deletion AVP presence indicates to delete the event.
- SCEF-Reference-ID presence indicates to add or update the monitoring event.

PDN-Connectivity-Status-Configuration is sent either via IDR or ULA. If it is via IDR, the MME returns the current PDN status in the IDA. Otherwise, the MME reports via Reporting Information Request (RIR). Sending of the first report in IDA is controlled by the `eventReportPreferIda` flag in UE monitoring profile. If the reporting is continued, subsequent PDN changes are reported in Reporting Information Request (RIR).

PDN-Connectivity-Status-Configuration may contain an optional AVP Service-Selection. If present, MME will report PDNs based on service selection. Otherwise, all the PDNs will be reported on status change.

No RIR is sent in the following scenarios:

Table 68: No RIR sent scenarios

Scenario	PDN-Connectivity-Status-Configuration AVP in	Impact
Attach with PDN	ULA	No RIR immediately after ULA as the PDN is not yet created. The report is sent in an RIR message after completion of the attach procedure.
Attach without PDN		No RIR immediately after ULA as the PDN is not yet created.
Attach failure		No RIR after attach procedure since no PDN is to report.
		No RIR immediately after ULA as the PDN is not yet created.
		No RIR after attach failure since PDN did not create it.
Attach without PDN	IDR	No RIR since empty report (without PDN report AVP) is not supported.
Attach without PDN gParms <code>eventReportPreferIda=Yes</code>		IDA without PDN report. No RIR since <code>eventReportPreferIda</code> is enabled .

Related descriptions

- [MME support for CloT monitoring procedures \(Feature f11702-01\)](#)

14.18.5 MME support for MONTE communications failure event (Feature f11733-05)

With the communication failure monitoring event, the MME notifies the SCEF when the MME sends or receives an S1AP cause code or if an ESM cause code error results in the bearer release. The event is configured at the MME via S6a interface (IDR and ULA).

This feature supports the communication failure event. The feature builds on the set of MONTE events and reports defined in the feature *MME support for CloT monitoring procedures (f11702-01)*.

The MME supports the following capabilities as part of this feature:

- Recognizes the “Communication_Failure (5)” monitoring type on S6a and stores it in the VLR and the UE context.

- Updates the event in the VLR and the UE upon changes in the UE subscription on S6a or errors in the T6a Reporting-Information-Answer (RIA).
- Notifies the SCEF for the Communication-Failure-Information Report on a per-UE basis, provided that the UE is subscribed to the event and that the global feature control is active.

The Communication-Failure-Information AVP parameter includes:

Cause type	The cause type.
S1AP-Cause	The S1AP cause codes that are sent in the MONTE report to the SCEF during communication failures.
SM-Cause	The ESM cause codes that are sent in the MONTE report to the SCEF during communication failures.

The report is generated when the MME sends or receives an S1AP cause code or if an ESM cause code error results in the bearer release.

The Communication-Failure-Information AVP is sent either via IDR or ULA.

14.18.6 MME support for MONTE number of UEs per location (Feature f11733-07)

With this monitoring event, the MME reports the number of UEs within a defined location area to the SCEF. The SCEF configures the event directly to the MME, providing a location area and an optional IMSI group ID. The MME then reports the outcome directly to the SCEF. Per R16 standards, only the last-known location is supported. Accuracy can be at the eNB, TAI, or ECGI level.

This feature supports the event for number of UEs present in a geographic area. The feature builds on the set of MONTE events and reports defined in feature *MME support for CloT monitoring procedures (f11702-01)*.

The MME supports the following capabilities as part of this feature:

- Recognizes the “Number of UEs Present in a Geographic Area (7)” monitoring type on the T6a Configuration-Information-Request message and stores it in a map on the IPDS.
- Updates the event in the map upon changes in the T6a Configuration-Information-Request (CIR) monitoring event configuration.

- Notifies the SCEF for the Number of UEs Present in a Geographic Area Report. This report is not on a per-UE basis.

The Number-Of-UE-Per-Location-Report parameter can include:

EPS-Location-Information The user location information relevant to the EPS.

UE-Count The number of UEs in the geographic area.

IMSI-Group-Id The IMSI group ID (optional).

The report is always sent in a T6a: Reporting-Information-Request (RIR) message.

14.18.7 UE monitoring enhancements (Feature f11733-01)

This feature supports two monitoring types in addition to the ones already implemented in feature *MME support for CloT monitoring procedures (Feature f11702-01)*.

For these monitoring types, additional information needs to be included in the reports towards the services capability exposure function (SCEF).

The feature supports two additional monitoring types that can be requested by the HSS in the Monitoring-Event-Configuration IE during the insert subscriber data (IDR)/update location answer (ULA) procedures as described in 3GPP TS 29.366:

- UE_REACHABILITY_AND_IDLE_STATUS_INDICATION (type 8)
- AVAILABILITY_AFTER_DDN_FAILURE_AND_IDLE_STATUS_INDICATION (type 9)

14.18.8 MME support for generating idle status report if configured when UE is idle (Feature f11733-10)

This feature extends *UE monitoring enhancements (Feature f11733-01)* to allow the MME to send the idle status monitoring report when the UE is idle and the event is configured via the Insert Subscriber Data Request (IDR) message of the S6a interface.

The feature applies only if parameters `monIdleStatusIndication` and `monIdleStatusRptAtIdr` are active in the monitoring profile applicable for the UE. Otherwise, the function of *UE monitoring enhancements (Feature f11733-01)* applies.

For the MME to generate an idle status report for UE reachability, the UE must be configured at the MME via the S6a interface with both the `UE_REACHABILITY_AND_IDLE_STATUS_INDICATION` (8) monitoring event and the `UE_REACHABILITY` (1) monitoring event.

For the MME to generate an idle status report for availability after DDN failure, the UE must be configured at the MME via the S6a interface with both the `AVAILABILITY_AFTER_DD_N_FAILURE_AND_IDLE_STATUS_INDICATION` (9) monitoring event and the `AVAILABILITY_AFTER_DD_N_FAILURE` (6) monitoring event.

The report is sent in:

- the IDA message via the S6a interface if the `eventReportPreferIda` parameter is set in the UE monitoring profile.
- the Reporting Information Request (RIR) message via the T6a interface.

The content of the idle status report is generated per operation of the `ueMonitoringProfile` command. If the maximum number of reports is supplied in the event configuration, the remaining number of reports is decremented by one after sending the report.

The idle status event continues to expire per operation of the `ueMonitoringProfile` command.

Error handling for faulty idle status event configuration continues to be handled per operation of the `ueMonitoringProfile` command.

Updated Location Answer (ULA) handling is not changed by this feature. If the event is configured via the ULA message, the first report continues to be sent when the UE transitions to the idle mode after the completion of the event that triggered the Update Location Request (ULR) message.

The process for reporting the first idle status report when the UE is configured in idle is as follows:

1. The MME receives the IDR message that configures the idle status monitoring event as `UE_REACHABILITY_AND_IDLE_STATUS_INDICATION` together with `UE_REACHABILITY`, or `AVAILABILITY_AFTER_DD_N_FAILURE_AND_IDLE_STATUS_INDICATION` together with `AVAILABILITY_AFTER_DD_N_FAILURE`, or both.
2. The UE is idle, that is, the UE can be anywhere in the idle window, such as in PTW or paging sleep window (PSW) sleep.
3. If *MME support for generating idle status report if configured when UE is idle (Feature f11733-10)* is active:
 - a. The MME sends the first idle status report as part of the IDR procedure or after the

- IDR procedure.
- b. The report is in the IDA message if the `eventReportPreferIda` parameter is set. Otherwise, it is in the RIR message.
 - c. The number of the remaining reports is decremented by one.
 - d. The MME generates subsequent idle status reports per operation of the `ueMonitoringProfile` command. For example, the MME generates idle status reports when the UE transitions from connected to idle by using the RIR message.
4. If *MME support for generating idle status report if configured when UE is idle (Feature f11733-10)* is not active, the existing *UE monitoring enhancements (Feature f11733-01)* logic applies for generating the first report. For example, the MME generates the first report when the UE transitions from connected to idle.

14.18.9 Using the S6a/S13/SLg SCTP association for T6a (Feature f11701-15)

The feature supports T6A application along with the S6a, S13 and SLg applications on the same SCTP association.

The MME can be configured to use the same SCTP association (same IP address pairs) with the same port towards DRA for all diameter applications. This feature adds T6A to a combination of already supported S6A/S13/SLG through feature *MME support for same SCTP association to DRA and higher peer count (f11304-01)*.

CER/CEA messages (Capability-Exchange-Request/Capability-Exchange-Answer) on one connection request will be advertised on one or more of the interfaces: S6a, S13, SLg and T6a.

When this feature is enabled (`combineApplType` has value `S6A/S13/SLG/T6A`), all diameter application IDs are combined with S6a and the connection is initiated from S6a local interface definition.

With this feature enabled, it is not possible to use direct link to service capability exposure function (SCEF) target (even if provisioned). If changes are done to add, delete, or modify T6a interface remote end points or links, it will have no impact on MME since T6a-specific links are no longer used and are combined with S6a.

Figure 133: CMM with the same SCTP association shared between different interfaces



Related descriptions

- [MME support for same SCTP association to DRA and higher peer count \(Feature f11304-01\)](#)

14.18.10 Simultaneous support of SCEF with S11-U (Feature f11701-12)

This feature supports UE containing bearers simultaneously to SCEF and S11-U.

Previous CMM deliveries have supported UEs with bearers over T6A and S1U, as well as independently bearers over S11-U. With this feature, a UE may establish:

- 2 bearers over T6A (bearers providing control plane data transport with SCEFs)
- 2 bearers over S11-U

However, T6A - S11-U and T6A - S1U switching is not supported with this feature.

If the MME is monitoring a UE's T6A PDNs for CP inactivity, the MME also monitors the UE's S11-U PDNs, if any, for CP inactivity. With this feature, the inactivity monitoring of S11-U PDNs can only start/continue after initial T6A CP monitoring starts. The same CP inactivity timer, `controlPlaneUserInactivity`, applies to all PDNs.

Control plane inactivity timer operates as follows:

1. UE with only T6A PDNs: inactivity timer is supported (this is existing behavior, Feature *Control plane Clot optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF)*, f11701-02)
2. UE with only S11-U PDNs: inactivity timer is not supported. However, if a T6A PDN is subsequently added, case (3) applies.
3. UE with T6A and S11-U: inactivity timer (same timer for both PDN types) is supported. However, if all T6A PDNs are subsequently released, CP inactivity monitor continues while there is activity on remaining S11-U PDNs, case (4) applies.
4. The CP inactivity timer is started with T6A bearers, and is extended based any control plane activity (either from S11-U or T6A).
5. S11-U to S1U switching with or without T6A: inactivity timer is not supported.

This feature extends and requires all previous configurations from features supporting T6A and S11-U:

- MME support for NB-IoT and EMM-REGISTERED UE without PDN connection (f11701-01)
- Control plane CloT optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF) (f11701-02)
- Control plane CloT EPS optimizations for both non-IP data and IP through SGi (f11701-03)

The feature may also combine functionality with (S11-U) MME support for S11-U downlink user data buffering (f11701-11).

Provisioning is the same as for previous T6A and S11-U features. Several existing parameters need to be set to support both S11-U and T6A mechanisms, including `cpCIoTDeliveryMechanism` in `uePlmnServices`: the parameter must be set to value `all` (delivery using both S11-U and T6A is supported).

Related descriptions

- [Control plane CloT optimization for non-IP data delivery \(NIDD\) via Service Capability Exposure Function \(SCEF\) \(Feature f11701-02\)](#)
- [MME support for NB-IoT and EMM-REGISTERED UE without PDN connection \(Feature f11701-01\)](#)
- [Control plane CloT EPS optimizations for both non-IP data and IP through SGi \(Feature f11701-03\)](#)
- [MME support for S11-U downlink user data buffering \(Feature f11701-11\)](#)
- [Switching data transport between control plane and user plane \(Feature f11708-01\)](#)
- [Using the S6a/S13/SLg SCTP association for T6a \(Feature f11701-15\)](#)

14.18.11 Simultaneous support of SCEF with S11U - part 2 (Feature f11701-16)

This feature supports simultaneous SCEF and S11-U PDN for additional scenarios: more bearers than the limit of 2 in Simultaneous support of SCEF with S11-U (f11701-12), CP-UP switching between S1-U and S11-U and ePCO updates from SCEF.

14.18.12 MME support for changing the range of controlPlaneUserInactivity timer (Feature f14612-01)

This feature allows an operator to increase the value of the `controlPlaneUserInactivity` timer to a maximum of 60 seconds. This timer is used

to detect user inactivity and release S1 connection of a UE that has no user data over NAS only. It is recommended to set the timer larger than NB-IoT inactivity timers at the eNBs.

If the UE has only SCEF, S11U bearers, or both (no S1U bearers), after the expiry of the `controlPlaneUserInactivity` timer, the S1 connection of the UE is released by the MME and is moved to ECM-IDLE state.

14.18.13 Validating the AVPs times are not out of date (Feature f11736-01)

This feature supports a change in the CMM behavior when handling Mobile Terminated Data Request (MTDR) messages from the SCEF.

The existing feature supports hard-coded (30 seconds) validity checking on the time value received in SCEF-Wait-Time and Maximum-Retransmission-Time AVPs in TDR messages to ensure that those time values are not too far out of date (such as, already past the current time).

If the MME finds such an invalid past-due time value by using the validity checking and the UE is temporarily unreachable, then that message would be rejected using the Diameter result code 5012 DIAMETER_UNABLE_TO_COMPLY.

This feature allows the operator to provision the exact validity time by adding a configurable timer (`scefExpiredTimeReject`) to specify the exact maximum past-due delta that is tolerated.

The value range of the `scefExpiredTimeReject` timer is 1 to 120 seconds. The default value is 30 seconds (for the existing hard-coded one).

14.18.14 MME support for early data transmission for control plane and user plane CloT EPS optimization (Feature f11701-18)

Early data transmission (EDT) is an optimization of control plane (CP) CloT and user plane (UP) CloT. The optimized procedure avoids transitioning the UE to an RRC-connected mode and minimizes message exchange.

The MME supports mobile-originated (MO) EDT and mobile-terminated (MT) EDT, which uses MO-EDT.

MO-EDT

The MO EDT allows for one uplink message and, optionally, one downlink (DL) message to be exchanged with the UE, allowing for fewer RRC messages and for the UE to stay in RRC-idle mode. If additional messages are needed, the MME and/or the eNB can move the UE into the RRC-connected mode, per the existing procedure.

For UP MO-EDT, there is no change to any of the MME procedures. The MME is not aware that EDT at the RRC level is taking place. UP MO-EDT is transparent to the MME because there is no change to the procedure for the S1 UE CONTEXT RESUME REQUEST/RESPONSE messages.

For CP MO-EDT, the MME recognizes a new EDT session IE in the S1AP initial UE message, then responds to that initial request according to TS 23.401. CP MO-EDT is supported for both S11-U and T6a data transfer.

EDT features can be used during an MO-EDT procedure if the following criteria are fulfilled:

- A CP Service Request message is received with the EDT IE set to `true`.
- The release assistance information (RAI) indicates whether the UE awaits data.
- The MME is configured to accept this UE based on the configuration of the `ciotprofile` or `plmn` commands.

The MME checks whether there is only one message that needs to be sent to the UE. Using the RAI, the UE indicates that it is expecting data. The MME then includes the end indication IE set to “no further data” in the S1AP message. If the UE indicates that is not expecting data but there is pending data in MME, then the MME sends this pending DL message with the end indication IE set to “no further data”.

The MO-EDT procedure is abandoned if a bearer synchronization is needed or if a common procedure, such as authentication, occurred previously.

 **Note:**

The Connection Establishment Indication (CEI) message or Service Accept is not sent when the requirements for the feature are satisfied, such as if the UE sent an EDT IE in the CP Service Request and the PLMN is provisioned. Only one DL message is exchanged with the UE and the message carries the end indication IE.

If there is only one expected or only one pending DL message from the gateway, the MME includes the end indication IE in the S1AP Downlink NAS Transport messages. If multiple DL messages are waiting for the UE after the MO-EDT procedure starts, the MME does not include the end indication IE in the S1AP Downlink NAS Transport messages.

The MME identifies the pending messages from the gateways based on the following scenarios:

- If the UE sends a CP Service Request to the MME and has only S11-U PDNs, the MME expects that any pending messages will be received between Modify Bearer Request and Modify Bearer Response, then decides whether to include the end indication IE.
- If the UE sends a CP Service Request to the MME and has only T6a PDNs, the MME immediately checks whether there are any pending messages, then decides whether to include the end indication IE based on the total number of messages.
- If the UE sends a CP Service Request to the MME and has both S11-U and T6a PDNs, the MME expects that any pending messages will be received between Modify Bearer Request and Modify Bearer Response for both S11-U and T6a PDNs, then decides whether to include the end indication IE.

MT-EDT

UP MT-EDT is supported for S11-U data transfer. CP MT-EDT is supported for both S11-U and T6a data transfer.

When selecting an S-GW for the UE, the MME uses existing mechanisms, such as topological proximity, Décor, or collocation, regardless of MT-EDT support. The MME determines whether the S-GW supports MT-EDT based on the node feature IE in the S11 messaging. MT-EDT support applies to both the UP and the CP, as only one bit is allocated for both in S11. If the S-GW supports MT-EDT, then the MME can receive the DL data packets size IE from the S-GW for an idle and pageable UE. The MME notifies the eNB that MT-EDT can be used by including the data size IE in the S1AP paging message, subject to the restriction that all TAIs within the TAI list previously sent to the UE must be marked in provisioning as supporting MT-EDT for the UP or CP, as appropriate for the scenario. If the MME's provisioning does not allow MT-EDT for the UE, the MME proceeds with the paging without including the data size IE in the S1 paging message.

In the TAU and attach procedures, or when the MME establishes or modifies an S11-U or S1-U PDN connection at the S-GW, the MME notifies the S-GW whether the PDN supports MT-EDT, based on the following criteria:

- the UE supports CP and/or UP MT-EDT
- TAI and `ueP1mnServices` provisioning are allowed
- the S-GW notifies the MME that the S-GW supports MT-EDT

The “MTEDTA” and “MTEDTN” indication flags IE for Create Session Request and Modify Session Request are used to notify the S-GW of the MT-EDT capability.

If the S-GW supports MT-EDT but the PDN does not, the MME notifies the S-GW that MT-EDT is not allowed for the PDNs.

The MME support for CP MT-EDT via the T6a interface differs slightly from the support via the S11-U interface because there is no DL data packets size IE in the T6a interface. The basic procedure is the same as for S11-U CP with the following changes:

- The MME derives the DL data packets size IE based on the data from the T6a:TDR message instead of receiving the value via the S11-U interface.
- The MME verifies that the UE is allowed CP MT-EDT, using the provisioning in the `uePlmnServices` or `imsiRangeServices` commands, because the SCEF does not provide the explicit indication on the T6a interface, whereas the S-GW sends the DL data packets size IE on the S11-U interface.
- The global parameter `allowScefMtEdt` must be set to `true` to allow the MME to include the DL data packet size IE in the S1AP Paging message.

14.18.15 MME support for accepting connection release from SCEF for temporarily unreachable UE (Feature f11701-20)

This feature changes the MME's logic for handling incoming Connection Management Request (CMR) messages with connection release for unreachable or idle UEs. If the UE is in or about to enter power saving mode (PSM), extended idle mode DRX (eDRX), or ECM-IDLE mode when the MME receives a CMR message from the SCEF to release a T6a bearer, the MME returns a Connection Management Answer (CMA) message indicating success to the SCEF for the bearer deletion request. The MME synchronizes the bearer status with the UE at the next UE access procedure.

This feature is activated on the MME by the global parameter `acceptScefRelForPsmEdrx`. By default, this parameter is disabled.

When the `acceptScefRelForPsmEdrx` parameter is disabled, the MME uses the existing logic for handling incoming CMR messages with bearer deletion, which includes returning the DIAMETER_ERROR_USER_TEMPORARILY_UNREACHABLE message to the SCEF for a UE in PSM or eDRX and attempting to page an idle UE not in PSM or eDRX for bearer cleanup.

When the `acceptScefRelForPsmEdrx` parameter is enabled, if the MME receives a CMR message from the SCEF to release a T6a bearer for a UE, the MME always returns a CMA message with the DIAMETER_SUCCESS message, indicating success to the SCEF for the bearer deletion request.

If the MME is unable to synchronize the bearer status with the unreachable or idle UE at the time it processes the CMR and CMA message, the MME synchronizes the bearer status with the UE at the next UE access (such as TAU or CPSR), as needed.

This feature is used in the following scenarios:

- the UE is either in or about to enter PSM or eDRX and the MME determines it cannot page the UE
- the UE is in ECM-IDLE mode and is pageable

14.19 Sending AADDNF notification during eDRX and send LoC when entering PSM (Feature f11702-04)

With this feature, the MME sends Availability after DDN failure (AADDNF) event notification when the UE moves from the idle cycle in eDRX into the paging timer window (PTW). In addition, the MME sends Loss of Connectivity (LoC) event notification when entering the PSM window.

When this feature is disabled, the MME sends the Availability after DDN failure notification only after the UE accesses the MME (for example, TAU, service request) per 3GPP procedures.

With this feature, the MME also sends this event notification when the UE moves from the idle cycle in eDRX into the paging timer window (PTW). This allows the application server to reach the UE during the PTW when the UE otherwise has nothing to send and does not access the network. This expanded use of AADDNF is not defined in 3GPP standards.

This feature also enhances the Loss of Connectivity Monitoring event to be sent when the UE is subscribed to the event and enters power saving mode (PSM) (T3324 expiration). This expanded use of LoC is not defined in 3GPP standards.

The feature is controlled by parameters `monAvailAfterDdnFail` and `monLossOfConnectivity` in `ueMonitoringProfile`.

Related descriptions

- [MME support for CloT monitoring procedures \(Feature f11702-01\)](#)

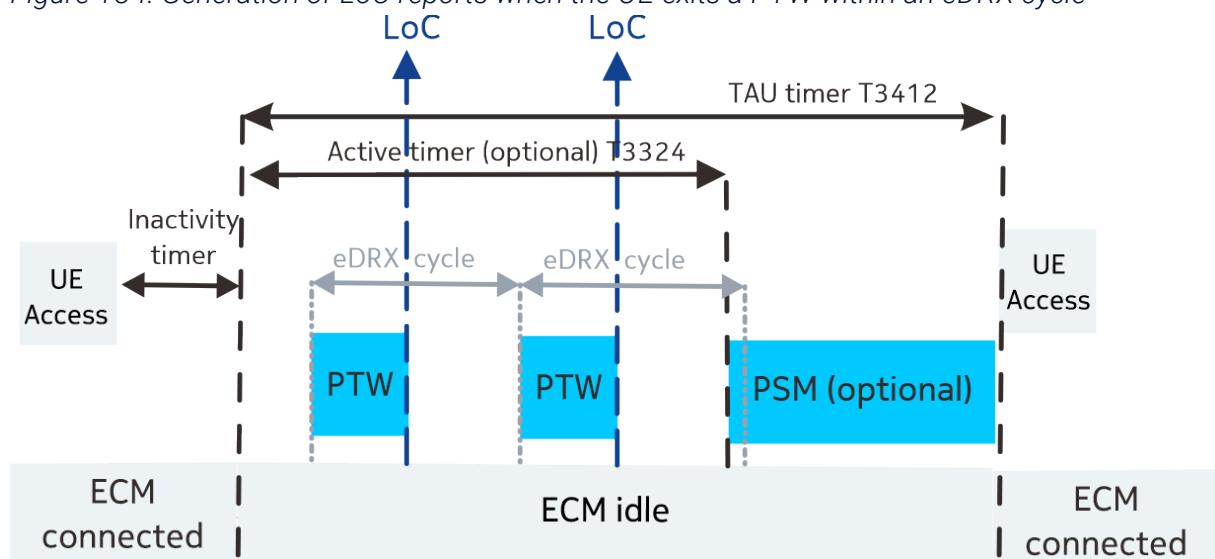
14.20 MME support for generating loss of connectivity (LoC) event reports during eDRX cycle (Feature f11735-02)

This feature allows the MME to generate a LoC report whenever the UE exits a paging timer window (PTW) within an eDRX cycle.

This feature extends the existing LoC reporting mechanism by optionally allowing the MME to generate a LoC report whenever the UE exits a PTW within an eDRX cycle. This feature primarily benefits UEs with longer eDRX cycles. UEs with an eDRX value of 0 (cycle length of 5.12 s) use the legacy DRX mechanism; the LoC reporting provided by this feature is not applicable to these UEs.

The HSS configures the 3GPP standard LoC event at the MME. The 3GPP standard defines sending a LoC report after a UE misses its T3412 TAU or upon detach. As shown in Figure *Generation of LoC reports when the UE exits a PTW within an eDRX cycle*, this feature allows the MME to generate a LoC report when the UE exits a PTW within an eDRX cycle. It is optional whether the UE also uses PSM. There is no change on the S6a or T6a messaging.

Figure 134: Generation of LoC reports when the UE exits a PTW within an eDRX cycle



The generation of a LoC report at the entry to PSM is described in feature *Sending AADDNF notification during eDRX and send LoC when entering PSM* (f11702-04).

Related descriptions

- [Sending AADDNF notification during eDRX and send LoC when entering PSM \(Feature f11702-04\)](#)

14.21 MME support for eNB CP relocation indication for NB-IoT UE (Feature f11727-01)

This feature introduces eNB CP relocation indication procedure which is to request the MME to authenticate the UE's re-establishment request and initiate the establishment of the UE-associated logical S1 connection after the UE has initiated an RRC re-establishment procedure in a new eNB.

When the new eNB receives the RRC Connection Re-establishment Request message, it triggers the eNB CP relocation indication procedure including the NAS-level security information received from the UE. If the MME authenticates the request, it initiates the connection establishment indication procedure including the NAS-level security information to be sent to the UE in the RRC Connection Re-establishment message. In addition, and if the old eNB has not yet released the old S1 connection, the MME initiates the MME CP relocation procedure to trigger the old eNB to return the non-delivered NAS PDUs to the MME. The latter are then delivered to the UE. In case of a successful authentication, where the old eNB has released the old S1 connection, the MME re-establishes the connection with the S-GW as part of the CP relocation procedure.

In case that the MME cannot authenticate the UE's request, the Connection Establishment Indication message does not contain the security information, the eNB fails the RRC re-establishment and the new S1 connection is locally released at both the eNB and the MME.

In case of a successful UE authentication, the MME initiates the UE context release procedure to release the UE's S1 connection in the old eNB. The MME initiates the CP relocation procedure before the context release procedure in order to trigger the old eNB to return the non-delivered NAS PDUs to the MME, if provisioned to initiate the procedure. Then, the MME delivers the non-delivered NAS PDUs from the old eNB and the MME non-delivered PDUs to the target eNB.

14.22 MME support for CIoT for inbound roamer phase - 1 (f11738-02)

This feature extends control plane (CP) CIoT capabilities, previously used for homer UEs only, to inbound roamers.

This feature supports CP CIoT operation but does not support MONTE events, such as connection to the SCEF-IWF. Prior to this feature, the CP CIoT operation is restricted to homer subscribers and shared PLMN subscribers.

The MME supports the following capabilities for inbound roamers:

- S11-u CP CloT using only IP
- Attach without PDN connection
- SMS for NB-IoT without combined attach
- ePCO
- PSM/eDRX
- MT-SMS
- Buffering in S-GW
- Extended NAS timers
- Service gap control
- Option 2 for handling MT SMS for UE in power savings
- HLCOM
- SMS in MME (SMS profile name)
- Restricting S-GW relocation enhancements (`sgwRelocationAllow`)
- MME support to S1-AP paging priority to paging profiles (`lapPagingPriProfileName`)

The capabilities are configured at the UE PLMN service level.

The MME supports the `cpCIoT` parameter in the `imsiRangeServices` command. This parameter allows the CP CloT service to be activated or deactivated on an IMSI range basis. The `cpCIoT` value takes precedence over the value provisioned at the UE PLMN service level.

14.23 MME support for CloT feature control via IMSI ranges (Feature f11737-01)

The feature enables an operator to control the CloT features, including NB-IOT, PSM eDRX, S1-U, or S11-U, based on IMSI ranges defined at the MME.

The feature introduces provisioning support at the IMSI range services level for all CloT features. Previously, the CloT features were not provisionable through the `imsiRangeServices` command but through the `uePlmnServices` command.

The following CloT features are part of the new profile `ciotProfile` that can be referenced at the IMSI range services level:

```
cmm ciotProfile [--name <string>]
[ --allowNonIpOverS1u <list-item> ]
[ --ciotEmmRegisterdWithoutPdn <list-item> ]
[ --cpCIoTDeliveryMechanism <list-item> ]
[ --ePcoSupport <list-item> ]
[ --hlcomDdnAckWithDlBuffering <list-item> ]
[ --hlcomEnabled <list-item> ]
[ --hlcomPsmDlBufferingPacketCount <integer> ]
[ --hlcomUseLocalDlBufferingPacketCount <list-item> ]
[ --mmeNbIotCptoUpSwitch <list-item> ]
[ --mmeWbEutranCpToUpSwitch <list-item> ]
[ --mtSmsOpt2ForUeInPowerSavings <list-item> ]
[ --nbIotDlDataSizeForCpToUpSwitch <integer> ]
[ --nbIotSmsWithoutCombinedAttach <list-item> ]
[ --nBIotUeCpToUpSwitch <list-item> ]
[ --nbIotUlDataSizeForCpToUpSwitch <integer> ]
[ --nonIpDataTrans <list-item> ]
[ --rohc <list-item> ]
[ --s1uDataTrans <list-item> ]
[ --serviceGapControlActive <list-item> ]
[ --serviceGapTimerSource <list-item> ]
[ --supportGrpSvcProvision <list-item> ]
[ --upCIoT <list-item> ]
[ --wbEutranDlDataSizeForCpToUpSwitch <integer> ]
[ --wbEutranUeCpToUpSwitch <list-item> ]
[ --wbEutranUlDataSizeForCpToUpSwitch <integer> ]
```

The following CloT features are already supported at the IMSI range services level and are not added to `cmm ciotProfile`:

```
[ --cpCIoT <list-item> ]
[ --edrxApnListName <string> ]
[ --edrxEnabled <list-item> ]
[ --edrxHssPtwProfileName <string> ]
[ --edrxModeWithPsm <list-item> ]
[ --edrxProfileName <string> ]
[ --edrxSource <list-item> ]
[ --psmEnabled <list-item> ]
```

14.24 MME support for CloT for inbound roammers (Feature f11738-01)

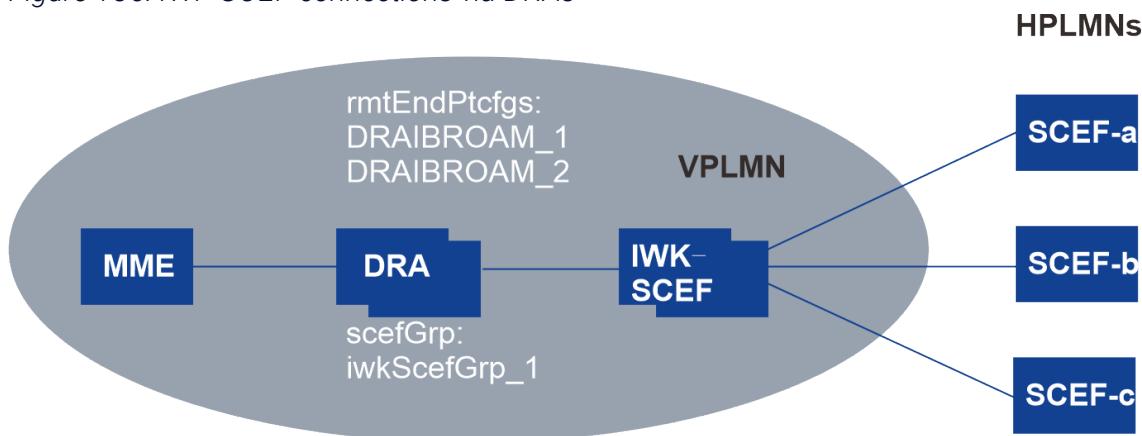
This feature supports CloT for inbound roammers. It supports connection to IWK-SCEF, NB-IoT, and LTE-M operation. This feature also controls the access to NB-IoT RAT for inbound roammers.

When NB-IoT access is rejected based on the new accRestNBiot field, the MME allows the provisioning of a configurable cause code, which is sent in the rejected access attempt (for example, attach CPSR).

The MME supports the following functionalities:

- The MME supports setting/updating the RAT type to LTE-M for T6a PDNs. Use global parameter `sendLteRatTypeToScef` to specify whether the MME can send the LTE-M RAT to the SCEF for an applicable UE.
- The MME supports LTE-M RAT type in the PDN Connectivity Status Report.
- The MME supports configuration of IWK-SCEFs. Existing T6a local provisioning is reused and shared with homers.
 - All SCEF nodes assigned to an IWK-SCEF group must support the same IWK-SCEF functionality, for example, the ability to support MONTE verification or T6ai management.
 - If the DRAs are used, the DRAs must be able to route the IWK-SCEF traffic (based on host/realm, IMSI, message type, or other means) to the proper IWK-SCEF.
 - The draSupported flag must be set for each node in the `rmtEndPtCfg` command, regardless of whether direct-connect or DRA-routing is used. This allows the MME to learn the various destination host and destination realm values. This is important since the IWK-SCEF functions as a diameter proxy.
 - The SCTP is brought up and diameter initialization (for example, CER/A or DWR/A) to the IWK-SCEFs is not changed. Alarming and PMs are not changed.
 - The DRAs supports the home SCEF applications or they can be dedicated to the IWK-SCEF functionality. It is also possible to configure direct-connect IWK-SCEFs. The following figure illustrates IWF-SCEF connections via DRAs:

Figure 135: IWF-SCEF connections via DRAs



- The IWK-SCEF group(s) are used for inbound roammers. They can be used for T6ai APNs and/or monitoring events. In this example, all IWK-SCEFs are behind the DRA(s).
- Each DRA in the network is defined with the `rmtEndPtCfg` command. New DRA(s) can be added for inbound roaming or existing DRA(s) can be used.
- The DRA(s) are assigned to a new SCEF group(s) to be used for inbound roammers with the `scefGrp` command.
- The MME supports `scefToGrp` provisioning with an extra flag `ikwScef` and PLMN equal to 0 to support roammers. CLI restriction are as follows:
 - 64 `scefToGrp` allowed for home PLMN + 64 `scefToGrp` allowed for roaming PLMN(0).
 - 32 active groups for home PLMN + 32 active groups for roaming PLMNs.
- The MME populates the Diameter-Realm (DR) and Diameter-Host (DH) AVP values for egress T6ai Request messages. These requests are always routed via `scefToGrp` rules.
 - T6ai APN DH/DR population:
 - As defined in 3GPP standards, the HSS must provide a SCEF ID and a SCEF realm for a T6a APN configuration. Furthermore, when the MME attempts to set up a T6ai APN/PDN (this could be part of attach or it could be later for attach without PDN scenarios), the MME sets the DH and DR for the initial CMR message to the SCEF ID and SCEF realm from the subscription APN configuration.
 - The MME supports local provisioning override of the T6ai DH/DR values (either in `scefToGrp` or `rmtEndPtCfg` command) which are consistent when routing through the `scefToGrp` translation, and consistent with current operation.
 - The MME fills in all other AVPs in the T6ai:CMR message in the same manner as for home/shared subscribers and TAHS.
 - The MME supports learned DH/DR for T6ai APN management, for example, new values in the CMA OH/OR AVPs. These learned values are used for the routing and DH/DR AVPs in subsequent CMR and ODR egress messaging.

Note:

The corresponding answers provide new learned values. These learned values are independent from the other learned DH/DR in this requirement.

- Monitoring event validation DH/DR population:
 - As defined in 3GPP procedures, the MME relays an inbound roamer's monitoring event configurations to an IWK-SCEF for authorization. The IWK-SCEF authorizes the inbound roamer's monitoring event configurations based on monitoring type, load, quota, rate and roaming agreement/SLA, and so on. The UE identifier is not sent to the IWK-SCEF for the authorization.
 - Authorization is accomplished by sending a T6ai:CIR message with the monitoring configurations AVP. The MME routes on and uses locally provisioned DR and DH values for the first CIR. The MME obtains these DR/DH values from the `scefToGrp` rules.
 - For the CIR validation, the MME sends all monitoring events from the ULA/IDR monitoring event configuration in one CIR message to the IWK-SCEF for validation.
 - The MME supports learned DR/DR for this CIR/CIA application. The locally configured data is used if the MME needs to send a subsequent CIR for the UE. The reason for this is that the MME does not know how long the learned DR/DH persists. Furthermore, the UE identities are not passed to the IWK-SCEF in the authorization.
- Monitoring event reporting DH/DR population:
 - When the MME detects a validly configured event, the 3GPP procedures dictate that the MME routes on and sets the DH/DR in the initial T6ai:RIR message to the SCEF-ID and SCEF-Realm from the event configuration. This is the same handling as for the non-roamers in the current implementation.
 - With this routing capability, the operator has flexibility in assigning inbound roaming traffic to the IWK-SCEFs. A given UE's three sets of traffic (CIR, RIR, and CMR/ODA) can be assigned to the same or separate IWK-SCEFs depending on the routing configuration. The existing diameter routing and weighting capabilities are reused for inbound roamers.
- The MME validates an inbound roamer's monitoring event configuration.
 - When the MME receives new or updated S6a monitoring event configurations for an inbound roaming UE, and the monitoring events are allowed per MME provisioning, the MME performs monitoring event validation with an IWK-SCEF as defined in 3GPP TS 29.128 Section 5.4. Basic steps are as follows:
 1. Create the CIR message and include the UE's S6a monitoring configuration data. Set the DH/DR and route per Req15.
 2. Determine from the CIA whether the IWK-SCEF modified or refused some

configurations. If so, the MME uses the modified event configurations for the UE. Furthermore, the MME notifies the HSS via NOR procedures of the modified/refused configurations. See the NOR procedures in 3GPP TS 29.272 Section 5.2.5.1.2.

3. If the CIR cannot be routed or if the CIA times out, the MME optionally performs retry depending on provisioning. If the retry fails or is not provisioned, the MME considers the validation to be failed for all configurations and notifies the HSS accordingly.
 - 3GPP procedures allow an event report to be included in the CIR message. The CMM MME implementation does not include a report within a CIR.
- The MME supports control and operation of CloT via `uePlmnServices` for inbound roamer.
- The MME supports the full set of MONTE capabilities (currently supported for home subscribers, shared PLMN subscribers, and Treat-as-home subscribers) for inbound roamer. This includes but is not limited to:
 - S6a capability negotiation, event configuration, error handling via NOR, and so on
 - Event reporting via RIR over T6ai to the IWK-SCEF, using the appropriate destination host and realm
 - Assignment of `ueMonitoringProfile` to inbound roamer in the `uePlmnServices` record
 - Use of assigned DRA messaging priority
 - Event expiration handling

 **Note:**

Event reporting via IDA is not used for inbound roaming. If an immediate report is generated, it must be sent either as part of T6ai:CIR or in a subsequent T6ai:RIR.

- The MME supports group service ID within IMSI-Group-ID based on feature *Group service provisioning (Feature f11701-07)* for inbound roamer.
- The MME supports the full set of capabilities (currently supported for home subscribers, shared PLMN subscribers, and Treat-as-home subscribers) for establishing, maintaining, and using T6ai PDNs to an IWK-SCEF, as defined in feature *MME support for CloT monitoring procedures (Feature f11702-01)*. These capabilities include but are not limited to:
 - T6ai APN mapping to the IWK-SCEF
 - Creation, deletion, modification, and use of PDNs to the IWK-SCEF
 - Use of assigned DRA messaging priority
 - Mobile Originated (ODR) and Mobile Terminated (TDR) operations
 - Message Buffering
 - Overload control
 - All AVPs currently supported in T6a messaging for home traffic

 **Note:**

The SCEF timers (CMR answer, ODA, TDA, CP user inactivity) are globally defined and are reused for this feature.

- The MME supports NIDD PDNs over S11u for inbound roammers. These capabilities include but are not limited to:
 - Creation, deletion, modification, and use of “NIDD” PDNs over S11u
 - Buffering
 - Throttling
 - Rate control
 - LTE-M indication
- The MME supports NB-IoT access control (`roamingNbIoTNotAllowed`). Separate access control is supported for roammers, homers, shared PLMN, and TAHS PLMN.
- The MME supports `disableUeMonitoring` flag in `imsiRangeServices` (disabled by default) for inbound roammers. The purpose is to allow gradual introduction of MONTE for inbound roammers. The same flag is available to be used for home/shared/TAHS subscribers.
- The MME supports communication failure event for inbound roammers.
- The MME accepts up to 16 total concurrent requests across all SCEFs for the number of UEs per location monitoring event configuration.
- Roamers in the following features are supported in this feature:
 - *MME support for non-IP with S1-U transferred (Feature f11723-01)*
 - *Switching data transport between control plane and user plane (Feature f11708-01)*
 - *Control plane CloT optimization for non-IP data delivery (NIDD) via Service Capability Exposure Function (SCEF) (Feature f11701-02)*
 - *Control plane CloT EPS optimizations for both non-IP data and IP through SGi (Feature f11701-03)*
 - *MME support for CloT monitoring procedures (Feature f11702-01)*
 - *User plane CloT EPS optimizations - bearer activation without SR (Feature f11701-04)*
- UE radio capabilities match procedure is supported as part of this feature. This procedure triggers the eNB to send the UE capabilities information indication, which is the only S1AP message that can contain the LTE-M indication.

14.25 MME support for wake-up signal for CloT (Feature f11701-21)

This feature enables MME to use the Wake Up Signal (WUS) to reduce UE's idle-mode

power consumption and the Group WUS (GWUS) to reduce the power consumption related to paging monitoring.

This feature adds core network support for WUS channels between the RAN and the UE to reduce UE's idle-mode power consumption, as defined in *3GPP TS 23.401 (Release 15)*. The WUS-capable eNBs provide the Recommended Cells for Paging IE to the MME in the Context Release Complete or Context Suspend Request message. The MME stores this information and provides it without any modification in the subsequent S1AP Paging message to the RAN. Also, the MME deletes and stores the recommended cells when a new S1 connection is established for the UE.

Additionally, this feature provides the Group WUS (GWUS) support between the RAN and the UE to reduce the power consumption used for paging monitoring, as described in *3GPP TS 36.300 (Release 16)*. In detail, this feature allows the WUS assistance information negotiation between the UE and MME via NAS messaging. The UE and RAN use this WUS assistance information to determine the proper WUS channel for monitoring. The selected GWUS channels are transparent to the MME.

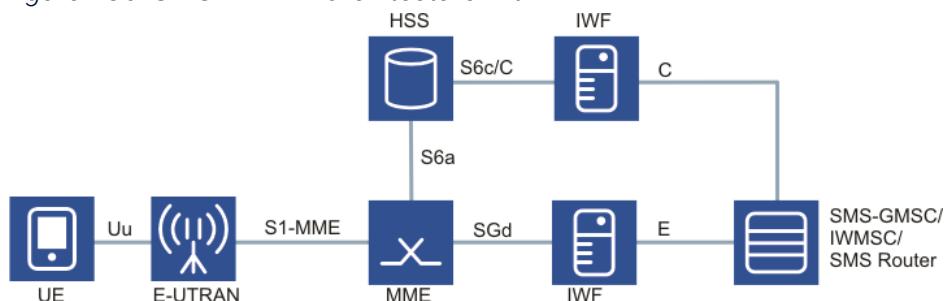
15. SMS in MME (Feature f11004-03)

This feature enables SMS service without the circuit-switched (CS) domain. MME performs the SMS service control and SMS relay functionalities previously done by the MSC/VLR.

In the SMS in MME option, the MME registers to the HSS for the SMS service for the UE. The MME receives SMS-related subscription data from the HSS and performs the SMS service control and SMS relay functionalities previously done by the MSC/VLR. The SMS is delivered via the Diameter-based SGd interface between the MME and the SMS entities.

The short messages are delivered towards the UE over the NAS interface similarly to the SMS over SGs case, but on the network side, the MME additionally adopts legacy MSC/VLR functionality and logic for the SMS delivery. Whether the network provides the SMS service via the SGs or the SGd interface is transparent for the UE.

Figure 136: SMS in MME architecture with IWF



Provisioning

The feature can be activated using the global parameter `smsInMme`. By default, the feature is disabled.

The feature requires provisioning of the S6d interface.

- The SGd application supports a standalone SCTP association.
- SCTP multi-homing (local and remote) is supported on the SGd interface.
- MME supports mapping from Diameter SGd error cause to SMS relay protocol (RP) error cause.

The MME supports the SGd paging type in paging profiles. For the SGd paging type, if also eDRX is provisioned, the eDRX value takes priority.

The MME supports provisioning of the SMSC/SMS router terminating the SGd Diameter interface. The maximum number of SMSCs is 16. The MME balances the load between the provisioned SMSCs. Deploying DRAs between the MME and the SMSCs is supported.

The MME supports provisioning of SMS profile for SMS delivery parameters, including message retransmissions, timers, and SMS registration preference.

When *SMS in MME* is supported, operators can configure on service agreement level whether SMS over SGd is allowed. It is also possible to select between SGs-based and SGd-based SMS delivery when both are deployed in the network and possible for an individual user.

The *SMS in MME* feature can be allowed per UE PLMN/serving PLMN combination, that is, as part of the service agreement profile:

- MME ISDN
- preferred option if both SGs and SGd are possible for the UE
- timers

The MME supports per serving PLMN provisioning of:

- non-broadcast LAI
- reserved TMSI value

15.1 SMS in MME procedures

Descriptions of SMS in MME procedures: SMS registration, SMS deregistration, mobile-terminating (MT) SMS delivery, and mobile-originating (MO) SMS delivery.

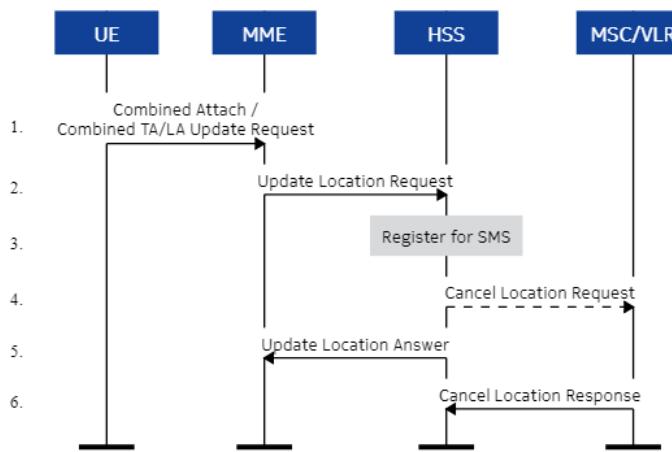
The MME supports SMS registration towards the HSS for a UE and SMS deregistration initiated by the HSS or the MME according to *TS 23.272 Annex C*.

When the MME has registered the UE towards the HSS for SGd-based SMS delivery, the MME forwards MO and MT SMSs for the UE via the SGd interface according to *TS 23.272 Annex C*, *TS 23.040* and *TS 24.011*.

SMS registration

The UE initiates a combined attach or combined tracking area (TA) or location area (LA) update to an MME. An NB-IoT UE may issue an EPS attach or TA update instead of a combined attach or combined TA/LA update.

Figure 137: SMS registration



The MME sends an S6a Update Location Request (ULR) message to HSS. The message includes SMS in MME feature flags, MME address for MT-SMS routing, registration for SMS request, and SMS only indication. The SMS only indication is included if it has been included in the request from the UE. The MME includes one of the following registration for SMS request values:

- SMS in MME Required
- SMS in MME Not Preferred
- No Preference for SMS in MME

For more information on registration for SMS request values and the impact of provisioning on the MME, see [SMS registration parameters](#).

Next, the HSS sends an Update Location Answer (ULA) message to MME, including indication whether the MME has been registered for SMS, subscription data including the network access mode and PS and SMS only indications, SMS subscription data, and SMS in MME feature flags.

If the HSS does not register the MME for SMS, it will indicate that the MME has not been registered for SMS and will not include any SMS subscription data.

The SMS in MME feature flag indicates that the HSS is capable of supporting the *SMS in MME* feature.

The MME stores the returned data and checks the result of registering the MME for SMS. If the registration for SMS is not accepted, the MME does the following:

- For a PS only subscription, the MME does not establish any SGs association (no SMS services are provided to the UE).
- For a PS and SMS only subscription where SMS can be provided over CS (circuit switched)

core), the MME tries to establish SGs for SMS.

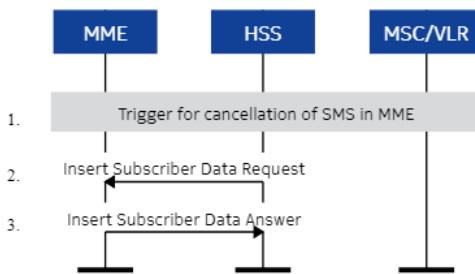
- For a PS and CS subscription where also other CS services are allowed, the MME tries to establish SGs for SMS and other CS services.

When the MME has registered the UE for SMS towards the HSS, the MME sends the provisioned values for the non-broadcast LAI (location area identity) and the reserved TMSI (temporary mobile subscriber identity) on the (Combined) Attach/TAU Accept message towards the UE.

SMS deregistration

When the HSS needs to indicate to the MME that it is no longer registered for SMS, the following procedure is applied:

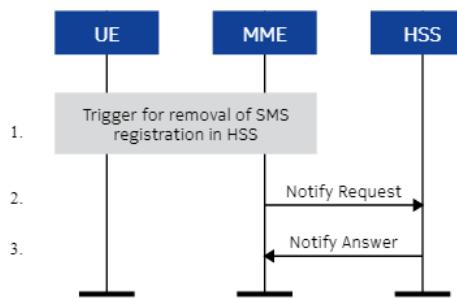
Figure 138: HSS-triggered SMS deregistration



- There is an event that triggers the cancellation of the MME being registered for SMS. This may be the removal of the SMS subscription for the UE or a CS location update, for example.
- The HSS sends an Insert Subscriber Data Request (IDR) (Remove SMS registration) message to inform the MME that it is no longer registered for SMS in MME.
- The MME sets its MME registered for SMS parameter as not registered for SMS and considers the SMS subscription data as invalid. The MME acknowledges with an Insert Subscriber Data Answer (IDA) message to the HSS.
- A normal Cancel Location of MME which results in the MME no longer being registered for PS services for that UE will also render the MME not registered for SMS.
- If the MME receives IDR with SMS registration removal, the MME triggers IMSI detach for the UE (provided UE is not in IDLE or not an NB-IoT UE in connected mode).
- In case of Delete Subscriber Data Request (DSR) message with DSR flags indicating SMS withdrawal, the MME removes the HSS-indicated codes from the UE data.

When the MME needs to indicate to the HSS that it is no longer registered for SMS in HSS, the following procedure is applied:

Figure 139: MME-triggered SMS deregistration

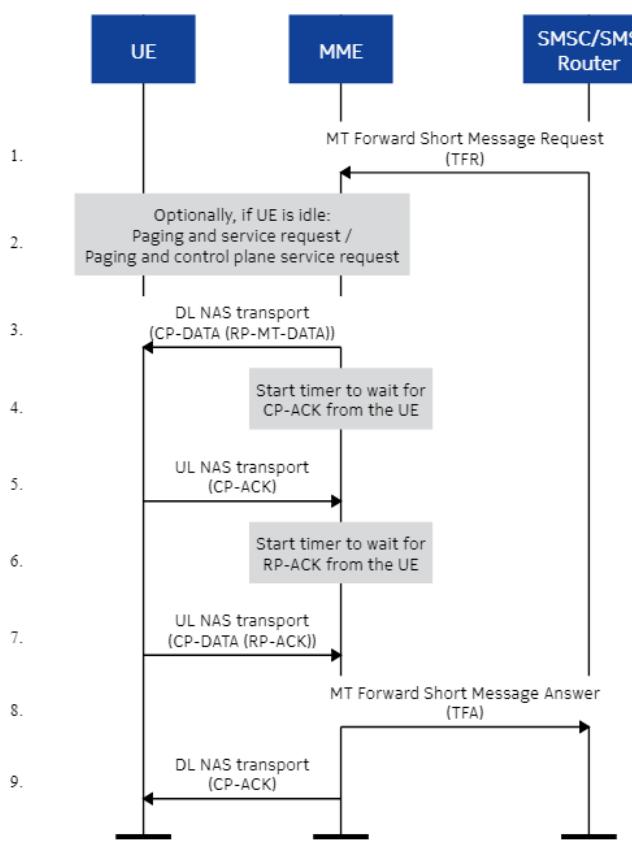


- There is an event that triggers the cancellation of the MME being registered for SMS. This may be a UE-initiated EPS attach only or a tracking area update (TAU), for example.
- The MME sends a Notify Request (NOR) message to inform the HSS to remove its registration for SMS in HSS.
- The HSS cancels the SMS registration for the UE in the MME. It acknowledges and responds with Notify Answer (NOA) to the MME.

Mobile-terminating SMS delivery

The MME supports SMS delivery towards the UE reusing the same NAS protocol mechanisms as on SGs-based delivery.

Figure 140: Successful MT SMS delivery



On incoming MT Forward Short Message Request (TFR), the MME validates the user and the message, by checking at least the following:

- There are no protocol errors.
- UE is registered on the MME.
- SGd is configured and the UE is registered for SMS delivery to the HSS.
- MT SMS (or all SMS) is subscribed based on the received Teleservice on the HSS subscription data.
- No barring of SMS is indicated on the HSS subscription data. If HSS is sending Update Location Answer (ULA) with any of the call barring info, the SMS will be completely barred by MME.
- UE is reachable, that is, not EPS detached, not IMSI detached.

If the MME validation is not successful, the MME reports the failure towards the SMSC/SMS router using Diameter result codes.

If the UE is EMM-DETACHED or in ECM-IDLE mode and does not respond to paging (but is not in power saving mode or not expected to respond due to eDRX), the MME reports this accordingly with DIAMETER_ERROR_ABSENT_USER to the SMSC/SMS router on the MT

Forward Short Message Answer (TFA). The MME also saves the mobile not reachable flag (MNRF) set on its subscriber data for this subscriber.

If the validation after receiving MT Forward Short Message Request (TFR) is successful, the MME encapsulates the received SM-RP-UI (user data field) inside a CP-DATA message as the RP-DATA (RP User Data). The MME then encapsulates the CP-DATA into a DL NAS transport and sends it towards the UE, starts the MME-provisioned timer TC1 and starts waiting for CP-ACK.

If the MME receives S1AP NAS non-delivery indication from the eNB for any SMS-related NAS downlink message and an X2/S1 handover is triggered and the MME is not relocated as part of the handover, the MME resends the corresponding NAS downlink message through the new eNB and after that, continues the SMS delivery procedure through the new eNB.

If the MME receives CP-ERROR or RP-ERROR from the UE, it reports with a Diameter result code to the SMSC/SMS router on TFA.

The TCI timer and the number of retransmissions of DL NAS transport can be locally provisioned in the MME and have the following impact on the procedure:

- If the timer expires while the MME is waiting for CP-ACK and the number of retransmissions of DL NAS transport is not yet reached, the MME retransmits the NAS PDU, restarts the TC1 timer and continues waiting for CP-ACK.
- If the timer expires while the MME is waiting for CP-ACK and the number of retransmissions of DL NAS transport is reached, the MME reports with DIAMETER_ERROR_SM_DELIVERY_FAILURE to the SMSC/SMS router on TFA.
- If the MME receives CP-ACK while waiting for it, the MME restarts the timer and starts waiting for CP-DATA (RP-ACK).
- If the timer expires while MME is waiting for CP-DATA (RP-ACK), the MME reports with DIAMETER_ERROR_SM_DELIVERY_FAILURE to the SMSC/SMS router on TFA.
- If the MME receives CP-DATA (RP-ACK) while waiting for it, the MME stops the timer, formulates a CP-ACK message, encapsulates it into a DL NAS transport and sends it towards the UE.

The MME includes the RP-ACK from the CP-DATA message from the UE into the SGd TFA, if received. If the MME does not receive CP-DATA (RP-ACK) from the UE, the MME reports this with DIAMETER_ERROR_SM_DELIVERY_FAILURE to the SMSC/SMS router on TFA.

If the MME receives a CP (control protocol) or an RP (relay protocol) message from the UE that the MME does not comprehend, the MME sends a CP-ERROR or an RP-ERROR message respectively as a reply towards the UE. The MME also complies with further protocol error handling as defined in *TS 24.011*.

CP-ACK lost scenarios (MT SMS)

Scenario 1:

- CP-DATA (RP-MT-DATA) is sent. Waiting for CP-ACK.
- CP-DATA (RP-MO-DATA) is received with different transaction identifier.
 - MME will stop the timer for CP-ACK and reset the timer for RP-ACK.
 - MME will hold the incoming MO SMS until the ongoing MT SMS is finished and process the incoming MO SMS.

Scenario 2:

- CP-DATA (RP-MT-DATA) is sent. Waiting for CP-ACK.
- CP-DATA (RP-ACK/RP-ERROR/RP-SMMSA) is received with different transaction identifier.
 - MME will drop the message.

Scenario 3:

- CP-DATA (RP-MT-DATA) is sent. Waiting for CP-ACK.
- CP-ACK is received. Waiting for RP-ACK.
- CP-DATA (RP-MO-DATA) is received with different transaction identifier.
 - MME will hold the incoming MO SMS until the ongoing MT SMS is finished and process the incoming MO SMS.

MT SMS attempted when UE is detached or not responding to paging

The MME stores the mobile station not reachable (MNRF) flag in its subscriber-related data to indicate a previously failed attempt for SMS delivery, if the UE was detached or not responding to paging (excluding the PSM/eDRX case when the UE is not even expected to be available).

When this flag is set in the MME for the UE and the UE next establishes S1 connection to the MME, the MME sends S6a NOR to HSS and sets the Ready for SM from MME flag on the NOR-flags AVP. The MME also sets UE_PRESENT on the Alert-Reason AVP. If the UE is using PSM or eDRX and thus the maximum availability time is applicable, the MME includes it to indicate the time that the UE is expected to be available.

Note that alerting through HSS is done normally when the MME is not aware of eDRX/PSM-caused unreachability. In this normal case, when the alert is done through the HSS, the MME is not required to store the SMSC address since the MME contacts the HSS to trigger the alert.

If the UE was previously detached (that is, MME de-registered the UE for SMS on HSS), and the UE reattaches with GUTI, the MME will send ULR to HSS regardless of the setting of the global parameter `hssUlrReduction` (*HSS signaling load reduction, m11308-01*). This is to ensure SMS service availability when SGd is selected for SMS.

UE in power saving mode or using eDRX

In case of MT SMS, if the UE is in power saving mode or not expected to respond to paging due to eDRX and the Maximum Retransmission Time IE was present in the TFR, the MME sends TFA back to the SMSC/SMS router with DIAMETER_ERROR_ABSENT_USER. If the UE is expected to be reachable before the reported Maximum Retransmission Time IE value, the MME additionally calculates the next UE reachability time and includes it into the TFA as the Requested Retransmission Time. If the Maximum Retransmission Time IE was not present in the TFR, the MME reports the SMS delivery as unsuccessful on the TFA (DIAMETER_ERROR_ABSENT_USER).

If the MME has reported a UE as absent for MT SMS due to eDRX or PSM and the MME has reported Requested Retransmission Time to the SMSC/SMS router, and after that the UE triggers transition to ECM-CONNECTED before the next PTW/UE reachability time (excluding the inter-RAT/MME mobility/outgoing case), after the UE-triggered procedure, the MME triggers an S6d alert service center procedure towards the SMSC/SMS router. This triggers the SMSC to resend the MT SMS immediately as the UE is again reachable at the MME. The MME sends an Alert Service Center Request (ALR) and waits for Alert Service Center Answer (ALA) as a reply.

On the above case, if the UE triggers inter-MME or IRAT TAU or the UE goes active but the eNB triggers inter-MME/IRAT handover before the MME has received TFR for the MT SMS retransmission from the SMSC/SMS router, the MME, on following Cancel Location Request (CLR), sends an Alert Service Center Request (ALR) with the new SGSN/MME address and waits for Alert Service Center Answer (ALA) as a reply. The MME also informs the new SGSN/MME about the pending MT SMS by setting the Pending MT Short Message Indication on the Forward Relocation Request/Context Response Indication Flags. The ALR triggers the SMSC to deliver the MT SMS through the new MME/SGSN.

On receiving the Pending MT Short Message Indication, the new MME includes the MME number for MT SMS IE and the MME identifier for MT SMS IE in the Forward Relocation Response/Context Ack and will not release the S1 connection after the TAU/IRAT TAU.

MT SMS buffering

The MME uses the provisioned SMS buffering time to buffer the MT SMS in case the UE is:

- busy with another procedure, for example, another MT SMS delivery
- currently not reachable due to eDRX/PSM, but is expected to make contact before the SMS buffering time has expired

In the above cases, on the receipt of a TFR for such a UE, the MME starts the `smsBufferingTime` and if the UE makes contact before the timer expires, the MME delivers the MT SMS.

If the timer expires and the MME has not yet been able to start the SMS delivery, the MME will respond to the SMSC/SMS router by TFA with either DIAMETER_ERROR_USER_BUSY_FOR_MT_SMS or DIAMETER_ERROR_ABSENT_USER, depending on the cause for the MME buffering.

After the timer expires, or if it cannot be applied, that is, the UE is not considered to be reachable before the timer's expiry, the MME does not buffer the SMS anymore but immediately responds to the SMSC/SMS router using TFA and the corresponding error.

The MME additionally limits the number of buffered MT SMSs to maximum 3 per a single UE. If the MME receives more messages and the message queue becomes full, the MME rejects the oldest TFR in queue with DIAMETER_ERROR_USER_BUSY_FOR_MT_SMS or DIAMETER_ERROR_ABSENT_USER.

MO reply to earlier MT SMS, related SMSC address storing and alerting

The MME configuration must be engineered to ensure that it is able to route (on Diameter level) a reply MO SMS to an earlier MT SMS.

Note that in such a case the UE will not use its internally stored (local) SMSC address but the SMSC address from a previously received MT SMS. The MME must thus ensure that the Diameter routing information for a received MT SMS will be available after a received MT SMS for routing a possible (reply) MO SMS using the same/given SMSC address.

If this storage of SMSC address - Diameter destination mapping becomes full, the MME will remove the oldest stored information.

The MME is also able to alert the UE (when the UE is reachable again and the MME performs the alert directly to the SMSC) towards multiple SMSCs related to MT SMS deliveries, when the UE was not reachable during an MT SMS delivery attempt. The MME is able to store up to 16 SMSCs per UE.

The MME will remove any stored SMSC addresses for pending Alert Service Center Requests (ALR) when the UE is considered detached. The MME will not invoke any ALR for a UE that is considered detached, or the UE is no longer considered registered for the SMS service.

Note that the UE may stay unreachable for hours or even a day or more. At the time that the MME triggers the alert, the MME needs to be able to also route the alert towards the corresponding SMSC. Whether the SMS is still available at the SMSC when the UE becomes available again depends on the validity period of the SMS (on layers not visible for the MME).

MT SMS overload handling

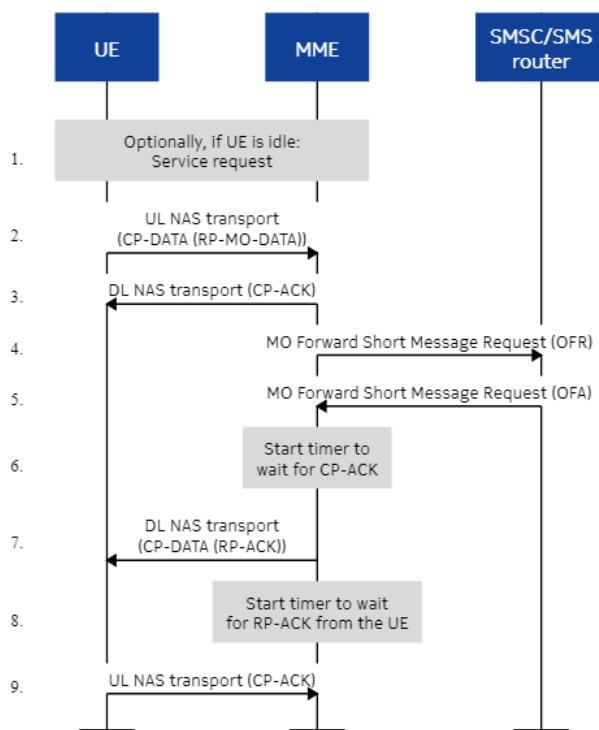
For MT SMS for an ECM-IDLE UE, when the MME is in overload, the MME drops the paging.

For MT SMS for an ECM-CONNECTED UE, when the MME is in overload, the MME sends back a TFA with "DIAMETER_TOOCBUSY" for a received TFR.

Mobile-originating SMS delivery

The MME supports MO SMS delivery:

Figure 141: Successful MO SMS delivery



On incoming UL NAS transport, or, if the UE is using CloT optimization, on incoming Control Plane Service Request carrying the UL NAS transport, the MME validates the user and the

message by checking at least the following:

- There are no protocol errors.
- UE is registered on the MME.

The MME decides whether to use SGs or SGd to forward the message. If SGd is configured and SMS registration to the HSS for the UE is previously performed, the MME uses SGd for SMS forwarding.

If the MME decides to deliver the message through SGd, it then checks the following:

- MO SMS (or all SMS) is subscribed based on the received Teleservice on the HSS subscription data.
- No barring for SMS is indicated on the HSS subscription data. If HSS is sending ULA with any of the call barring info, the SMS will be completely barred by MME.

If the MME successfully decodes the CP-DATA level message and if the MME validation is otherwise successful, the MME builds CP-ACK (or CP-ERROR in case of error), encapsulates that inside DL NAS transport and sends it towards the UE.

The MME will next, following its local configuration, map the SMS-SC address (destination address from the RP-DATA) into destination host and realm for the MO Forward Short Message Request (OFR) message. The MME builds an OFR message towards one of the provisioned SMSCs and includes the RP-ACK message out of the CP-DATA message from the UE into the OFR, and starts the timer waiting for the MO Forward Short Message Answer (OFA). The destination address from the RP-DATA message is included into the OFR.

If the MME is not able to map SMS-SC address into destination host and realm, it obtains the MCC/MNC values of the PLMN to which the SMS-SC belongs and uses them to build the MCC/MNC-based network domain as described in *subclause 19.2 of 3GPP TS 23.003* and includes it in the Destination-Realm AVP of the OFR. The OFR will then be routed to the next Diameter node.

When the MME receives the OFA, it will report the failure towards the UE on CP-DATA (RP-ERROR) message in RP-Cause IE, for example:

- Operator-determined barring
- Short message transfer rejected
- Unidentified subscriber
- Unknown subscriber
- Temporary failure
- Congestion

In case of successful OFA, the MME reports back to the UE using RP-ACK.

There will not be any retries for SGd message towards SMSC in case there is no response from SMSC.

The MME builds an RP-ACK (or RP-ERROR) message, encapsulates it into CP-DATA and further into a DL NAS transport and sends it towards the UE, starts the MME-provisioned timer TC1, and starts waiting for CP-ACK.

If the MME receives S1AP NAS non-delivery indication from the eNB for any SMS-related NAS DL message and an X2/S1 handover is triggered and the MME is not relocated as part of the handover, the MME resends the corresponding NAS DL message through the new eNB and after that, continues the SMS delivery procedure through the new eNB.

If the MME receives CP-ERROR from the UE while waiting for CP-ACK, the MME discards the SMS and terminates the procedure.

The TCI timer and the number of retransmissions of DL NAS transport can be locally provisioned in the MME and have the following impact on the procedure:

- If the timer expires while MME is waiting for CP-ACK and the number of retransmissions of DL NAS transport is reached, the MME terminates the procedure.
- If the timer expires while MME is waiting for CP-ACK and the number of retransmissions of DL NAS transport is not yet reached, the MME retransmits the NAS PDU, restarts the timer, and continues waiting for CP-ACK.
- If MME receives CP-ACK while waiting for it, the MME completes the successful MO SMS transfer.

If the MME receives a CP or an RP message that the MME does not comprehend, it sends a CP-ERROR or an RP-ERROR message respectively as a reply. The MME also complies with further/detailed protocol error handling as defined in *TS 24.011*.

CP-ACK lost scenarios (MO SMS)

Scenario 1:

- CP-DATA (RP-ACK) is sent. Waiting for CP-ACK.
- CP-DATA (RP-MO-DATA) is received with different transaction identifier.
 - MME will stop the timer and start new MO SMS.

Scenario 2:

- CP-DATA (RP-ACK) is sent. Waiting for CP-ACK.
- CP-DATA (RP-ACK/RP-ERROR/RP-SMMA) is received with different transaction identifier.
 - MME will drop the message.

MO SMS overload handling

For an MO SMS for an ECM-IDLE UE, when the MME is in overload, the MME rejects a SR/CPSR with EMM cause #22 "Congestion".

For an MO SMS for an ECM-CONNECTED UE, when the MME is in overload, the MME sends CP-ERROR to the UE with CP cause #22 "Congestion" for a MO sent CP-DATA.

15.2 SMS registration parameters

How SMS registration is handled depending on UE input and MME provisioning.

Parameters

The tables show whether or not SMS in MME is allowed with different combinations of the following parameters:

- UE input:
 - procedure is either combined attach, EPS attach, or inter-MME/inter-system TAU with combined TA/LA updating or TA updating
 - update type is 'SMS only' or not
 - NB-IoT is supported or not
- In the MME:
 - SMS registration preference in the SMS profile is one of the following:
 - SMS registration not preferred
 - No preference
 - SMS registration required
 - network access mode in service agreement profile is one of the following:
 - packet and circuit (PS+CS)
 - packet (PS)
 - SGd allowed in service agreement profile is either `true` or `false`
 - SGd interface is either configured or not
 - CSFB capability support in service agreement profile is set to one of the following levels:
 - `CSFB_2G3G` - Both SMS and CS are supported
 - `CSFB_Not_PREFERRED` - This option supports both SMS and CSFB
 - `SGS_None` - All CS-based services (CSFB and SMS based on CS) are restricted
 - `SMS_Only` - Only SMS is supported
 - SGs interface is configured or not

In the MME, global parameter `smsInMme` is set to `Yes`, unless otherwise stated.

Depending on the variables above, value of registration for SMS request in ULR is one of the following:

- SMS in MME not preferred
- SMS in MME required
- No preference for SMS in MME

SMS registration (UE input: combined attach or inter-MME/inter-system TAU with combined TA/LA updating, no update type, no NB-IoT)

Table 69: SMS registration (UE input: combined attach or inter-MME/inter-system TAU with combined TA/LA updating, no update type, no NB-IoT)

SMS registration reference	Network access mode	SGd allowed	SGd	CSFB support	SGs	ULR registration for SMS request	ULA MME registered for SMS	SMS in MME allowed
smsRegNotPref	PS+CS	Yes	Yes	CSFB_2G3G	Yes	SMS in MME Not Preferred	0	No
smsRegNotPref	PS+CS	No	No	CSFB_2G3G	Yes	SMS in MME Not Preferred	0	No
smsRegNotPref	PS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
smsRegNotPref	PS	Yes	Yes	SGS_None	No	SMS in MME Required	0	No
smsRegNotPref	PS+CS	Yes	Yes	SMS_Only	No	SMS in MME Required	1	Yes
smsRegNotPref	PS	No	No	SGS_None	No	N/A	N/A	No
smsRegNotPref	PS	Yes	Yes	SGS_None	Yes	SMS in MME Required	1	Yes
noPreference	PS+CS	Yes	Yes	CSFB_2G3G	Yes	No Preference for SMS in MME	1	Yes
noPreference	PS+CS	Yes	Yes	CSFB_2G3G	Yes	No Preference for SMS in MME	0	No
noPreference	PS+CS	No	No	CSFB_2G3G	Yes	SMS in MME Not Preferred	0	No

SMS registration reference	Network access mode	SGd allowed	SGd	CSFB support	SGs	ULR registration for SMS request	ULA MME registered for SMS	SMS in MME allowed
noPreference	PS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
noPreference	PS	Yes	Yes	SGS_None	No	SMS in MME Required	0	No
noPreference	PS+CS	No	Yes	SGS_None	No	N/A	N/A	No
noPreference	PS+CS	No	No	SGS_None	No	N/A	N/A	No
smsRegRequired	PS+CS	Yes	Yes	CSFB_2G3G	Yes	No Preference for SMS in MME	1	Yes
smsRegRequired	PS+CS	Yes	Yes	CSFB_2G3G	Yes	No Preference for SMS in MME	0	No
smsRegRequired	PS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
smsRegRequired	PS+CS	No	No	CSFB_2G3G	Yes	N/A	N/A	No
smsRegRequired	PS+CS	No	No	No	No	N/A	N/A	No
smsRegRequired	PS+CS	Yes	No	Yes	No	N/A	N/A	No
smsRegRequired	PS	Yes	Yes	SGS_None	Yes	SMS in MME Required	1	Yes
smsRegRequired	PS+CS	No	Yes	CSFB_2G3G	Yes	SMS in MME Not Preferred	0	No

If global parameter `smsInMme` is set to `No`, the rest of the settings are not applicable, and SMS in MME is not allowed.

SMS registration (UE input: EPS attach or inter-MME/inter-system TAU with TA updating, update type 'SMS only', NB-IoT true)

Table 70: SMS registration (UE input: EPS attach or inter-MME/inter-system TAU with TA updating, with 'SMS only' update type, NB-IoT true

SMS registration preference	Network access mode	SGd allowed	SGd	CSFB support	SGs	ULR registration for SMS request	ULA MME registered for SMS	SMS in MME allowed
smsRegNotPref	PS+CS	Yes	Yes	SMS_Only	Yes	SMS in MME Not Preferred	0	No
smsRegNotPref	PS+CS	No	No	CSFB_2G3G	Yes	SMS in MME Not Preferred	0	No
smsRegNotPref	PS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
smsRegNotPref	PS	Yes	Yes	SGS_None	No	SMS in MME Required	0	No
smsRegNotPref	PS+CS	Yes	Yes	CSFB_2G3G	No	SMS in MME Required	1	Yes
smsRegNotPref	PS	No	No	SGS_None	No	N/A	N/A	No
noPreference	PS+CS	Yes	Yes	SMS_Only	Yes	No Preference for SMS in MME	1	Yes
noPreference	PS+CS	Yes	Yes	SMS_Only	Yes	No Preference for SMS in MME	0	No
noPreference	PS+CS	No	No	SMS_Only	Yes	SMS in MME Not Preferred	0	No
noPreference	PS+CS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
noPreference	PS+CS	Yes	Yes	SGS_None	No	SMS in MME Required	0	No
noPreference	PS+CS	No	Yes	SGS_None	No	N/A	N/A	No
noPreference	PS+CS	No	No	SGS_None	No	N/A	N/A	No
smsRegRequired	PS+CS	Yes	Yes	SMS_Only	Yes	No Preference for SMS in MME	1	Yes
smsRegRequired	PS+CS	Yes	Yes	SMS_Only	Yes	No Preference for SMS in MME	0	No
smsRegRequired	PS+CS	Yes	Yes	SGS_None	No	SMS in MME Required	1	Yes
smsRegRequired	PS+CS	No	No	CSFB_2G3G	Yes	N/A	N/A	No

SMS registration preference	Network access mode	SGd allowed	SGd	CSFB support	SGs	ULR registration for SMS request	ULA MME registered for SMS	SMS in MME allowed
smsRegRequired	PS+CS	No	No	SGS_None	No	N/A	N/A	No
smsRegRequired	PS+CS	Yes	No	SMS_Only	No	N/A	N/A	No
smsRegRequired	PS+CS	No	Yes	SMS_Only	Yes	SMS in MME Not Preferred	0	No

If global parameter `smsInMme` is set to `No`, or NB-IoT is false in the UE input, the rest of the settings are not applicable, and SMS in MME is not allowed.

16. Presence reporting area (PRA)

Features supporting presence reporting area provisioning.

16.1 Presence reporting area (Feature f11003-01)

The MME supports reporting whether a requested UE is inside or outside of a defined area. MME may receive an action to start reporting via the S-GW/P-GW and when received, the MME updates every status change when UE enters or leaves a presence reporting area.

With this feature, the MME provides the S-GW/P-GW/PCRF the reporting on PDN connection level whether the UE is inside or outside a predefined area. The area can be configured either in PCRF or locally in the MME. A presence reporting area consists of any provisioned combination of TAIs, macro and/or home eNBs, and/or ECGIs.

Related to a PDN connection, the gateway can request MME to start or stop reporting whether the UE is inside or outside of the defined area. After starting to report changes, the MME will report first whether the user is inside or outside of the referred area, and after that, any change on status until the gateway requests stopping the reporting.

The *presence reporting area* feature can be used, for example, to provide differentiated charging based on accurate area. Cheaper service can be provided in a limited area, for example, discount for students on a university campus area. Continuous location reporting throughout the network can still be avoided and only the changes on the end user location status (entering or leaving the defined area) need to be reported.

This feature does not apply to roamers.

Functionality

The S-GW can request continuous reporting of a user entering or leaving a predefined area for a given PDN. The S-GW requests this reporting by sending a Presence Reporting Area Action IE in one of the S11 messages:

- Create Session Response
- Create Bearer Request
- Modify Bearer Response
- Update Bearer Request
- Change Notification Response

When the Presence Reporting Area Action IE is received, it contains an action:

- Action = start or stop
- Presence Reporting Area Identifier
- If the action is 'stop' and the presence reporting area is provisioned on the MME (Core Network pre-configured presence reporting areas), the items in the IE are only as above.
- If the action is 'start' and the presence reporting area is provisioned on the MME (Core Network pre-configured presence reporting areas), the items in the IE are only as above.

If action is 'start' and the S-GW is providing the area definition (UE-dedicated presence reporting areas), the IE will also contain at least one of the following:

- Number of TAIs
- Number of Macro eNB
- Number of Home eNB
- Number of ECGI
- if Number of TAIs is greater than 0, a list of TAIs (up to 15 TAIs)
- if Number of Macro eNB is greater than 0, a list of Macro eNBs (up to 63)
- If Number of Home eNB is greater than 0, a list of Home eNBs (up to 63)
- If Number of ECGI is greater than 0, a list of ECGIs (up to 63)

When the S-GW indicates action start, the MME will respond in one of the following messages, indicating if the UE is either inside or outside the defined area:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Update Bearer Response
- Change Notification Request

During MME relocation, the source MME relays presence reporting area action for a PDN in the following messages:

- Forward Relocation Request -> UE EPS PDN connections
- Context Response -> UE EPS PDN connections.

Provisioning

This feature is controlled by the global parameter `enablePra`. This provisioning controls both S-GW-provided and MME-provisioned presence reporting area. By default, handling of Presence Reporting Area IE is disabled.

If the operator chooses to provision presence reporting area definition (Core Network pre-

configured presence reporting areas), a maximum of 128 presence reporting area definitions can be provisioned.

A given Presence Reporting Area definition area ID (PRA-ID) can have:

- 63 ECGIs in the `praEcgi` table
- 63 home eNBs and/or 63 macro eNBs in the `praEnb` table
- 15 TAIs in the `praTai` table.

Related descriptions

- [PRA reporting for transitions from eNB to gNB \(Feature f10904-07\)](#)

16.2 PRA reporting for transitions from eNB to gNB (Feature f10904-07)

With this feature, radio resources of two nodeBs (a master and a secondary) may be used for a single UE at the same time. This feature is related to 5G NSA (non-standalone) option 3x and the dual connectivity feature.

When radio resources of two nodeBs are used for a single UE at the same time, the master LTE eNB terminates S1-MME and 5G gNB may be used as a secondary nodeB. In this feature, the MME utilizes presence reporting area (PRA) feature functionality to report towards the S-GW/P-GW/PCRF (upon the S-GW/P-GW/PCRF request) when 5G gNB is added as a secondary node for a PDN. MME can be configured with a single MME preconfigured PRA where a special IPv6 address segment of the 5G gNB corresponds to a presence reporting area. (The operator assigns static IPv6 addresses for gNBs.) The MME will thus report that the UE is 'inside' of the area when 5G gNB is added as a secondary node, and that the UE is 'outside' of the area when the 5G gNB is removed.

With the feature activated, the MME updates both the initial status (at the time of the S-GW/P-GW/PCRF requesting the start of the reporting) as well as any change to that status.

This feature is only applied to homers and roamers considered as homers.

Note:

If the MME receives action 'start' but no IP address segment is mapped with `cmm praDCSegmentMapping`, the MME reports the UE is outside the presence reporting area.

Provisioning

This feature is controlled by the `praDcSegment` global parameter. The value `dcSegmentBasic` activates the presence reporting area functionality to report on dual connectivity using a provisioned IPv6 address segment. The functionality uses core network predefined PRAs. By default, DC segment reporting is disabled.

It is possible to enable this functionality independently of the standard based PRA feature (f11003-01). Also, both features may be activated simultaneously.

Functionality

When all the below conditions are fulfilled:

- the `praDcSegment` gparam has the value `dcSegmentBasic`
- the MME receives a new PRA action IE from the S-GW/P-GW for a CN predefined PRA
- the PRA id on the received PRA action IE matches to one of the PRA ids on the MME local provisioning for the address segment reporting,

MME immediately updates the UE's initial presence (inside or outside) towards the S-GW/P-GW, as on the basic PRA feature. The MME includes the PRA information IE either on the next possible Modify Bearer Request during the same procedure if such will be sent as part of the procedure, or the MME sends an additional Change Notification Request to deliver the PRA information.

- The MME reports 'inside' if any current eNB endpoint Transport Layer Address (TLA), for any bearer belonging to this PDN where the PRA action is requested, belongs to the MME locally provisioned segment for the corresponding PRA id.
- The MME reports 'outside' if none of the current eNB endpoint TLAs, for any bearer belonging to this PDN where the PRA action is requested, belong to the MME locally provisioned segment for the corresponding PRA id.

Related descriptions

- [Presence reporting area \(Feature f11003-01\)](#)

16.2.1 PRA reporting procedures

MME may carry out DC segment reporting in X2 handover, S1 handover, inter-MME handover, E-RAB modification, and service request procedures.

 Note:

Modify Access Bearers Request cannot be used when the MME needs to report PRA status.

X2 handover

When MME receives an S1AP Path Switch Request message and IPv6 address segment reporting has been requested for any of the UE's PDNs previously, the MME checks the IP addresses of all the Transport Layer Address (TLA) IEs included in the E-RAB To Be Switched in Downlink List in the Path Switch Request message that belong to the PDNs for which reporting is requested. The MME analyzes if there are any changes to the previous inside/outside status related to each PDN. For the bearers that belong to each reporting requested PDN, the radio endpoint TLAs need to be compared to the MME locally configured IP address segment for the corresponding PRA id.

- If any of the Transport Layer Address IEs (for the bearers of the PDN) included in the Path Switch Request message match the MME locally provisioned address segment for the PRA id, the UE is considered inside the area.
- If none of the Transport Layer Address IEs (for the bearers of the PDN) included in the Path Switch Request message match to the MME locally provisioned address segment for the PRA id, the UE is considered outside the area.

If the inside/outside status has changed from the previous status, the MME includes the PRA information IE for the corresponding PDN towards the S-GW/P-GW in the subsequent Create Session Request/Modify Bearer Request triggered by the Path Switch Request.

 Note:

- With Path Switch Request, the endpoints can at this point in practice only either stay inside or need to be reported from inside to outside, that is, from DC (dual connectivity) to DC, if the same gNB is used, or DC to non-DC. The mobility from non-DC to DC will require a two-step procedure with first the handover and then the gNB addition (via E-RAB modification indication). Similarly, the DC to DC cases with different gNB require a two-step procedure: handover, E-RAB modification indication.
- X2 handover both without S-GW relocation and with S-GW relocation are supported.

S1 handover

When MME receives an S1AP Handover Request Ack message and IPv6 address segment reporting has been requested for any of the UE's PDNs previously, the MME checks the IP addresses of all the Transport Layer Address IEs included in the E-RABs Admitted List in the Handover Request Ack message that belong to the PDNs for which reporting is requested. The MME analyzes if there are any changes to the previous inside/outside status related to each PDN. For the bearers that belong to each reporting requested PDN, the radio endpoint TLAs need to be compared to the MME locally configured IP address segment for the corresponding PRA id.

- If any of the Transport Layer Address IEs (for the bearers of the PDN) included in the Handover Request Ack message match the MME locally provisioned address segment for the PRA id, the UE is considered inside the area.
- If none of the Transport Layer Address IEs (for the bearers of the PDN) included in the Handover Request Ack message match the MME locally provisioned address segment for the PRA id, the UE is considered outside the area.

If the inside/outside status has changed from the previous status, the MME includes the PRA information IE for the corresponding PDN towards the S-GW/P-GW in the first subsequent Create Session Request/Modify Bearer Request triggered during the S1 handover procedure.

With S1 handover, the endpoints are only required to be reported 'from inside to outside' during the actual procedure, that is, from DC to non-DC. The DC to DC to another gNB, or non-DC to DC, require a two-step procedure (first the handover during which the gNB is removed, and then possibly an E-RAB modification to add the gNB).



Note:

S1 handover cases for intra/inter-MME cases as well as intra/inter-S-GW cases are supported.

E-RAB modification

When MME receives an S1AP E-RAB Modification Indication message and IPv6 address segment reporting has been requested for any of the UE's PDNs previously, the MME checks the IP addresses of all the Transport Layer Address IEs included in the E-RAB To Be Modified list in the E-RAB Modification Indication message and in the E-RAB not to be Modified List that belong to the PDNs for which reporting is requested. The MME analyzes if there are any

changes to the previous inside/outside status related to the PDN. For the bearers that belong to the requested PDN, the radio endpoint TLAs are compared to the MME locally configured IP address segment for the corresponding PRA id.

- If any of the Transport Layer Address IEs (for the bearers of the PDN) included in the E-RAB Modification Indication message match the MME locally provisioned address segment for the PRA id, the UE is considered inside the area.
- If none of the Transport Layer Address IEs (for the bearers of the PDN) included in the E-RAB Modification Indication message match the MME locally provisioned address segment for the PRA id, the UE is considered outside the area.

If the inside/outside status has changed from the previous status, the MME includes the PRA information IE towards the S-GW/P-GW in the subsequent Modify Bearer Request (MBR) triggered by the E-RAB Modification Indication.

 **Note:**

E-RAB modification indication may be triggered due to a secondary node addition/removal of a gNB which does not belong to the provisioned segment. E-RAB modification may also be triggered when the UE moves between gNBs both belonging to the provisioned segment. PRA information IE is only included on MBR when the presence status changes from inside to outside or vice versa.

Service request

When MME receives an S1AP Initial Context Setup Response message and IPv6 address segment reporting has been requested for any of the UE's PDNs previously, the MME checks the IP addresses of all the Transport Layer Address IEs included in the E-RAB Setup List in the Initial Context Setup Response message that belong to the PDNs for which reporting is requested. The MME analyzes if there are any changes to the previous inside/outside status related to each PDN. For the bearers that belong to each reporting requested PDN, the radio endpoint TLAs need to be compared to the MME locally configured IP address segment for the corresponding PRA id.

- If any of the Transport Layer Address IEs (for the bearers of the PDN) included in the Initial Context Setup Response message match the MME locally provisioned address segment for the PRA id, the UE is considered inside the area.
- If none of the Transport Layer Address IEs (for the bearers of the PDN) included in the Initial Context Setup Response match the MME locally provisioned address segment for the PRA id, the UE is considered outside the area.

If the inside/outside status has changed from the previous status, the MME includes the PRA information IE for the corresponding PDN towards the S-GW/P-GW in the Modify Bearer Request triggered during the service request procedure.

Note:

- During the actual service request, as at least currently the initial radio endpoint is always assigned on the LTE side, the endpoints may only be required to be reported from inside to outside during the actual procedure. (Or no report required, since outside to outside is also naturally possible.) Adding a gNB requires a subsequent E-RAB modification.
- S1 release does not cause MME to trigger any PRA report.

Inter-MME handover

In inter-MME handover, the PRA action, if previously received on the old MME for any PDN, is forwarded from the old MME to the new MME. The old MME includes PRA action on S10 Forward Relocation Request/Context Response for any PDN for which segment reporting has been requested.

The new MME, when receiving PRA action on any inter MME HO/TAU from another MME via S10 on S10 Forward Relocation Request/Context Response, always (when the feature is activated) reports the initial status (inside/outside) as soon as available to the S-GW after receiving PRA action IE. The MME includes the PRA information IE on the first possible Modify Bearer Request, after receiving the RAN TLA endpoint, during either the TAU/HO, or when the initial RAN TLA user plane is established at the new MME.

After reporting the initial status, the new MME reports the status changes according to the global parameter value.

Note:

In inter-MME TAUs, when user plane is established during TAU (the active flag is set), it is assumed that a gNB cannot be directly added into the path in the Initial Context Setup, but an E-RAB Modification Indication is expected subsequently in case a gNB can be added under the new master eNB (MeNB).

16.3 PRA reporting optimizations for transitions from eNB to gNB (Feature f10904-10)

With this feature, MME optimizes the PRA IPv6 segment reporting and supports a provisioned timer on the Service Request message.

The MME optimizes the PRA reporting so that if at the time of the PRA reporting action 'start' is received (upon the SGW/PGW/PCRF request) and the UE utilizes only LTE resources (for example, the UE is 'outside' of the area), the MME sends the first report when the UE is 'inside' the area (for example, the gNB is added for the first time).

Additionally, MME supports a timer at the receipt of the Service Request message to withhold any status updating until the timer expires. This avoids any back and forth reporting if the radio triggers an E-RAB modification indication soon after the user data is established.

This feature is only applied to homers and roamers considered as homers.

Provisioning

This feature is controlled by the `praDcSegment` global parameter. The value `dcSegmentOpt` activates the feature. The functionality uses core network predefined PRAs. By default, the dual connectivity (DC) segment reporting is disabled.

It is possible to enable this functionality independently of the standard based PRA feature (Presence reporting area f11003-01). Also, both features may be activated simultaneously.

Functionality

When all the below conditions are fulfilled:

- the `praDcSegment` gparam has the value `dcSegmentOpt`
- the MME receives a new PRA action IE from the S-GW/P-GW for a CN predefined PRA
- the PRA id on the received PRA action IE matches to one of the PRA ids on the MME local provisioning for the address segment reporting,

the MME analyzes that the UE is currently 'inside' if any current eNB endpoint Transport Layer Address (TLA), for any bearer belonging to this PDN, belongs to the MME locally provisioned segment for the corresponding PRA id.

The MME analyses that the UE is 'outside' if none of the current eNB endpoint Transport Layer Address (TLAs), for any bearer belonging to this PDN, belong to the MME locally provisioned segment for the corresponding PRA id.

The MME will not report the UE's initial presence immediately towards the S-GW/P-GW, if the UE is currently 'outside' of the area. It only reports the first possible status change to 'inside'. If the UE is 'inside' the area, when the MME receives the PRA action 'start', the MME reports the first 'inside' status either on the next possible Create Session Request or Modify Bearer Request during the same procedure if such is expected to be sent, or utilizes the Change Notification Request to report the initial 'inside' of the area PRA information.

Whenever MME receives the Service Request for a UE for which PRA dual connectivity segment reporting has been requested for one or multiple PDNs, the MME starts the `praDcSegmentOptServReq` timer and withholds any segment PRA reporting until either the timer expires, or the MME receives an E-RAB modification indication message. The MME reports only possible status change at the expiry of the timer, if no E-RAB modification indication is received, and if any change to the previously reported status still needs to be reported. The MME utilizes applicable GTP message to include the PRA information IE towards the S-GW/P-GW/PCRF: Modify Bearer Request triggered during the Service Request procedure (if the timer was provisioned short enough), or a Change Notification Request message.

 **Note:**

The MME suppresses also the initial inside report, that is, the very first 'inside' report after PRA start for a PDN connection.

16.4 MME support for PRA 3GPP release 14 and 15 standard additions - part 1, part 2 (Features f10904-11 and f10904-16)

With this feature, the MME supports release 14- and 15-related standard additions related to presence reporting area (PRA).

The MME supports release 14- and 15-related standard additions related to presence reporting area, including support for multiple PRAs, PRA set, and modify action.

Note:

Maximum 11 PRAs may be requested for reporting by the S-GW/P-GW for a certain UE. These 11 PRA actions (start reporting) may be divided in any way within the sessions of the UE. The start reporting actions may be triggered simultaneously or one by one. When 11 start actions have been triggered altogether for a single UE, the MME ignores any subsequent start actions.

Multiple PRAs

Multiple instances of the presence reporting area action and presence reporting area information are allowed in the messages where they are applicable.

The MME supports multiple PRA IDs per PDN. The MME supports:

- receiving multiple PRA action IEs per corresponding GTPv2 message
- storing necessary information received on each PRA action IE
- performing corresponding action for each received PRA action IE

For standard PRA functionality, the MME supports receiving multiple PRA Action IEs per PDN in the following messages:

- Create Session Response
- Create Bearer Request
- Modify Bearer Response
- Update Bearer Request
- Change Notification Response
- Forward Relocation Request
- Context Response

For segment-based PRA functionality, the MME supports receiving multiple PRA Action IEs per PDN in the following messages:

- Create Session Response
- Forward Relocation Request
- Context Response

For standard PRA functionality, the MME supports sending corresponding multiple PRA information IEs per PDN in the following messages:

- Create Session Request
- Create Bearer Response
- Update Bearer Response

- Modify Bearer Request
- Change Notification Request

For segment-based PRA functionality, the MME supports sending corresponding multiple PRA information per PDN IEs in the following messages:

- Create Session Request
- Modify Bearer Request
- Change Notification Request

PRA set

The policy and charging rules function (PCRF) or online charging system (OCS) may request reporting changes of UE presence in a presence reporting areas set, which contains a list of core network pre-configured PRAs. PRA sets are identified by a PRA ID as any other PRA.

Reporting individual PRA information in addition to PRA set information is required:

- In the Presence Reporting Area Information IE, the Additional PRA Information (APRA) flag is added to indicate to the P-GW that the individual PRA (as part of the PRA set) information is provided from Octet 9, if the PCRF or OCS requested reporting changes of UE presence in a presence reporting areas set.

The MME supports PRA sets as follows:

- Only a single PRA set may be simultaneously triggered to be reported for a single UE.
- Up to 9 core network predefined PRA IDs may be provisioned as a PRA set locally in the MME.
- The MME supports receiving a PRA ID on PRA action that refers to a PRA set.
- The MME initially reports UE presence on all PRAs related to the set and after that, any change in UE presence on any PRA belonging to the set.
- When reporting UE presence for a PRA ID belonging to a set, the MME additionally indicates the PRA ID of the set on PRA information (and the presence status of the complete set).

Presence reporting area action

This feature adds support for:

- Action value 'modify'. It is used when the PCRF/P-GW modifies an existing UE-specific PRA definition, that is, for a PRA that is not pre-configured in the MME.
- Inactive PRA (INAPRA) indication is added in the Octet 5 to indicate to the target MME that the PRA is inactive in the source MME, that is, the PRA was requested by the P-

GW(/PCRF/OCS) but it was set to inactive by the source MME, for example, due to an overload situation.

- In Presence Reporting Area Information, the Inactive PRA (INAPRA) indication is added in the Octet 8 to be used if the PRA is inactivated by the MME.

 **Note:**

CMM MME in the current release does not set a PRA inactive, and reactivates any received inactive PRAs.

Support for dual connectivity PRA enhancement

The MME supports provisioning of multiple IPv6 segments for a single PRA ID. The MME supports reporting based on IPv6 segments as before, except that the 'inside' may be indicated by multiple IPv6 address segments instead of a single IPv6 segment only.

16.5 Dormant PRA state (Feature f10904-12)

This feature allows operators to set a CN predefined PRA and DC PRA in a new dormant state that suppresses any PRA reporting until the PRA is again set as active.

The dormant state is applicable for both standard-based PRA functionality and the dual connectivity segment-based reporting in the MME, but for the locally configured core network predefined PRAs only. The operator is able to set any core network predefined PRA into dormant state using the PRA id. When a PRA is in dormant state, the MME should suppress any PRA information reporting towards the S-GW/P-GW.

When MME receives PRA action (for a UE's PDN) for a currently dormant PRA, the MME will accept and store the PRA action, but not perform any further action. The MME is not required to evaluate the UE presence on a dormant PRA.

When a PRA is transferred from dormant to active, the MME evaluates the UE presence in the PRA for all PDNs (of the UE) for which PRA action has been received.

The MME sends PRA report to S-GW/P-GW indicating 'inside' for connected UEs and idle UEs when the PRA status can be evaluated.

The MME will not send PRA report if the UE is 'outside' when PRA is moved from dormant to active.

The MME will continue reporting PRA status changes normally (once the PRA is active).

When a PRA is transferred from active to dormant, the MME will:

- send PRA information 'outside' for all UEs/PDNs for which the MME has previously reported that the UE is 'inside'.
- suppress all next PRA report updates as the PRA is now dormant.
- maintain PRA action information related to the PDNs/UEs since the PRA may be transferred to active state again.
- not send any PRA information for those UEs/PDNs for which the MME has previously reported that the UE is 'outside' (or UE has been outside all the time and no report has been sent).

If any PRA optimization timer is running when the PRA status is changed from active to dormant, the timer will run until the end, unless an event stopping the timer occurs, for example, E-RAB modification indication. The PRA status will be updated on optimization cases after the timer has expired or the expected event has occurred.

 **Note:**

T1 timer of 30 seconds is imposed before the start of PRA status when a PRA state is changed from active to dormant or dormant to active. This timer will allow overload control to gather a batch of or all PRA id changes before starting any scan of the VLR table to perform matches.

PRA attributes table

The MME supports creating empty PRA, which is a PRA id not having any area or IP address segment/range associated with it, but PRA is present in the `praAttributes` table. The MME allows the S-GW/P-GW send PRA action related to an empty PRA. The MME will not send any PRA information back if the MME receives PRA action for a PRA that does not have any area or IP address segment/range associated with it.

The MME auto-creates a `praAttributes` table instance if one does not exist (when PRAs are created with the CLI commands `cmm praTai/praeNb/praeCg` or `praDcSegmentMapping`). When these commands are used to create PRAs, the MME ensures that the newly created PRA is defined to have status 'active'.

A PRA table entry can be created two ways:

- explicitly, using command `cmm praAttributes`.
- implicitly, using commands `cmm praTai / praeNb / praeCg / praDcSegmentMapping`, or by using the command for multiple areas, `cmm`

`multiPraOperation.`

When all areas have been removed related to a PRA id, the PRA table 'empty' entry will remain.

Feature activation

This feature is controlled by the global parameter `praDormantState` (by default, `No`). The parameter, when set to `Yes`, enables the functionality to change the state of the CN predefined presence reporting area between active (normal) and dormant. In dormant PRA state, the MME suppresses any PRA status (inside/outside) reports towards the S-GW/P-GW. In dormant PRA state, the MME still accepts and stores PRA action to request PRA status reporting.

 **Note:**

If the feature is disabled when some PRAs are currently set to the dormant state, PRAs are left as they are, dormant, despite the feature being disabled. That is, they are silently left in a state not included in the supported set of functionalities. The feature has to be re-enabled to move those PRAs back to the active state.

The two PRA state change PM counts, `VS.PraStateChangeDormantToActive` and `VS.PraStateChangeActiveToDormant`, indicate only updates during an effective delta time period.

16.6 PRA message pacing (Feature f10904-14)

This feature throttles presence reporting area (PRA) report towards GW/PCRF to avoid signaling burst.

With this feature, the MME can control the rate of transmission of PRA reports, such as PRA information IE sending towards the S-GW/P-GW. The MME sends PRA reports in a controlled manner. The MME is pre-configured for limiting the PRA reports into the defined maximum.

When the pacing feature is enabled, the MME limits the PRA reports related to both the standard-based PRA and the dual connectivity segment-based PRA functionalities. The MME needs to control the potential flood of reports towards the S-GW/P-GW and the PCRF. Potential flood may specially be generated due to PRA functionalities introduced by other features (such as PRA state transitions between active and dormant states).

16.7 PRA area ranges (Feature f10904-15)

This feature supports large number of area cells or macro/home eNBs to a single presence reporting area (PRA), therefore, single PRA can cover large reporting area with minimum configurations.

The feature allows the MME to provision large number of areas (cells or macro/home eNBs or tracking areas) to an existing PRA with a single command. The MME operation personnel needs to quickly add a large number of cell sites or tracking areas to an existing PRA. The standard based PRA functionality may be used for public safety use case and in crisis situation the quick provisioning of large areas is needed.

The MME allows provisioning of large areas by defining separate lists of area ranges to include and exclude on the PRA. This feature allows defining ECGI, macro and home eNB ranges.

16.8 MME support for scaling PRA limits (Feature f10904-17)

This feature enables the operator to provision multiple tracking areas codes (TACs) in a presence reporting area (PRA) with a single command.

The feature increases the number of area identifiers per each CN predefined PRA as below:

- tracking area identifiers (0..1499)
- macro eNB identifiers (0..3499)
- home eNB identifiers (0..3499)
- ECGIs (0..10499)

MME supports a limit of 50 000 of the combined number of TACs, eNBs, and ECGIs across all PRAs.

 **Note:**

The number of areas supported for UE-dedicated PRAs are not impacted.

16.9 PRA optimizations and additional timers (Features f10904-20 and f10904-30)

This feature defines further optimizations into the presence area reporting functionality for dual connectivity supporting IPv4 and IPv6 radio transport layer address (TLA).

For these features, `praDcConnectedIn` and `praDcConnectedOut` timers are introduced to ensure sequential secondary node addition/removal will not cause additional signaling due to back and forth reporting when the UE was in ECM-CONNECTED state, and `praDcIdle` timer is introduced to define a timer for presence reporting area (PRA) functionality for optimizing dual connectivity related reporting when the UE was previously in ECM-IDLE state. Timers are started in MME when the radio user plane endpoints have changed, for example, either a secondary node is added, removed or user plane is established as part of a handover procedure. If another sequential user plane updating procedure occurs before the timer expires, or UE context is released before the timer expires, the MME does not report any PRA status update towards the S-GW/P-GW.

For IPv4 based DC PRA, whenever the following conditions are fulfilled:

- optimized segment or range-based reporting is enabled (gParm `praDcIpv4` has value `dcPraIpv4OptIdleConn` or `praDcSegment` has the value `dcSegmentOptIdleConn`)
- the segment or range based reporting has previously been requested for some PDN of the UE
- the UE triggers Service Request message
- the MME detects a change on the inside/outside status that the MME has previously reported for the PDN
- the UE is in ECM-IDLE state (before receiving the Service Request)

then the MME starts the `praDcIdle` timer. The MME stops the timer on receipt of any trigger to update the RAN transport layer addresses (Initial context setup response as part of service request/control plane service request/intra MME TAU or path sw request/handover request acknowledge/E-RAB modification indication). If any of the above triggers updates on the PRA status so that no PRA report is required, the MME does not send any PRA status update.

In case a status update is still required, or the timer expires, the MME reports the PRA status within the next Modify Bearer Request/Create Session Request or sends a standalone Change Notification Request. If the UE context is released or suspended when the timer is running, the MME stops the timer and does not send the PRA report towards the S-GW/P-GW.

Note:

The MME does not suppress the initial inside report, that is, the very first 'inside' report after PRA start for a PDN connection. Note that the feature needs to be enabled alone to not suppress the initial inside report.

16.10 PRA dual connectivity reporting for IPv4 gNBs (Feature f10904-22)

This feature provides an option to utilize IPv4 addresses for gNBs in dual connectivity presence reporting area (PRA) functionality.

Feature *PRA reporting for transitions from eNB to gNB (f10904-07)* initially defined similar functionality when the RAN uses IPv6 addressing. This feature functionality follows the same logic, however, with some small additions applied on both IPv4- and IPv6-based RANs. Similarly, for both IPv4- and IPv6-based gNBs, PRA functionality is used to indicate when the UE is using a secondary gNB node (UE is inside) or not (UE is outside). MME uses provisioned subnet definition to analyze whether a provided RAN IPv4 endpoint belongs to an eNB or a gNB.

Note:

If the MME receives action 'start' but no IP address range is mapped with `cmm praDCSegmentMapping`, the MME reports that the UE is outside the presence reporting area.

16.11 MME support for optimizing standard PRA reporting (Feature f10904-28)

This feature optimizes the 3GPP standard based PRA reporting by omitting the initial outside report and defining timers to restrict PRA reporting, if the UE is bouncing in and out of the PRA. The feature is controlled by the `praStdSuppressInitialOut` and `praStdSuppression` global parameters.

When the MME receives PRA action 'start' from S-GW/P-GW and the global parameter `praStdSuppressInitialOut` is set to `No` (default value of the parameter), the MME sends the PRA report (PRA information) immediately, regardless of the UE's presence inside

or outside of the area.

When MME receives PRA action 'start' from S-GW/P-GW and the global parameter is set to `Yes`, the MME does not send any initial report (PRA information) if the UE is currently outside the area. The MME only sends the first report when the UE is or has arrived inside the area.

Additionally, the feature introduces two configurable timers to control the PRA report suppression: the PRA suppression timer and the PRA suppression cancel timer. The MME suppression of overly frequent PRA reports for 3GPP standard based PRA is controlled via the global parameter `praStdSuppression`. When this parameter is set to `Yes`, the MME suppresses a subsequent PRA report within the PRA suppress time period, unless the PRA status stays the same for the PRA suppress cancel defined time period.

16.12 MME support for new PRA action on 5GS to EPS mobility for DC PRA (Feature f10904-35)

With this feature, the MME supports receiving new PRA action during 5GS to EPS mobility and the inter-MME mobility procedures.

Upon receipt of the new PRA action start, the MME starts reporting the UE presence for the corresponding DC PRA. The MME supports the previously existing DC PRA optimization timers when reporting. Specifically, on 5GS to EPS HO procedure, if the UE is already "inside" when the MME receives the PRA action start, the MME starts the corresponding optimization timer `praDcConnectedIn` and reports the initial inside status at the expiration of the optimization timer. The MME starts the optimization timer in this case to ensure that the race condition scenario is handled properly. Also, the MME hands over any previously started DC PRA reporting between the old and the new MME during the inter-MME mobility procedure. The new MME starts reporting for the received DC PRA and always provides the initial status towards the S-GW/P-GW when it receives the PRA action from the old MME.

16.13 MME support for receiving new PRA action during additional procedures (Feature f10904-34)

The MME supports receiving a new PRA action during additional messages and procedures.

The MME supports receiving a new PRA action for the dual connectivity (DC) PRA on the following additional GTP messages:

- GTP Create Bearer Request

- Modify Bearer Response
- Update Bearer Request
- Change Notification Response

Upon receipt of a new PRA action, the MME starts or stops PRA reporting accordingly. When the MME starts the PRA reporting, the MME updates new initial status on PRA information on the following conditions after considering whether to report the initial status depending on optimization setting:

- either any next applicable GTP message that is sent during the procedure (Create Bearer Response/Create Session Request/Modify Bearer Request/Update Bearer Response, if any of these to be sent)
- or a standalone Change Notification Request message (if no message to be sent during the same procedure that can carry the PRA information)

After this, the MME continues reporting upon any next DC PRA status change. The MME supports the current optimization settings

(`dcSegmentBasic/dcSegmentOpt/dcSegmentOptIdleConn`) and related optimization timers (`praDcIdle`, `praDcConnectedIn`, and `praDcConnectedOut`) to optimize the PRA reporting if the PRA reporting is supported.

The MME supports receiving the GTP messages above with a new PRA action for DC PRA during the following procedures:

- dedicated bearer setup (Create Bearer Request)
- default/dedicated bearer modification (Update Bearer Request)
- intra-MME/inter-MME handover/TAU (Create Session Response/Modify Bearer Response)
- handover/TAU from 5GS with the N26 interface (Create Session Response/Modify bearer response)
- any standalone PRA report response (PRA report. For example, the PRA information is sent in the Change Notification Request message or the new PRA action comes inside the Change Notification Response message)
- PDN setup with Request Type "Handover" from the ePDG (Create Session Response)

The MME also supports a new PRA action received for the standard PRA during the following procedures:

- handover/TAU from 5GS with the N26 interface (Create Session Response/Modify bearer response)
- PDN setup with Request Type "Handover" from the ePDG (Create Session Response)

After receiving a new PRA action, the MME continues reporting any status changes for the

standard PRA and supporting also the previously developed reporting optimization.

17. 5G support

Dual connectivity provides support for 5G NSA deployment options 3A/3X.

17.1 MME support for dual connectivity (Feature f10904-01)

The feature extends radio coverage to 5G new radio (NR) with EPC core in support of 5G Non-Stand Alone (NSA) option 3A/3X or LTE coverage via small cells, when enabled. Without the feature, the EPC core, per Rel12 DC feature definition, is unaware of the extended radio type whether it is LTE (via small cells) or 5G NR.

The feature provides early introduction of 5G with EPC core (MME and S-GW/P-GW) to enable new services with higher throughput and/or lower latency requirements.

Dual connectivity involves two kinds of NBs (master and secondary), in providing radio resources to a given UE with active radio bearers, while single S1-MME termination point exists for an UE between a MME and the E-UTRAN.

The secondary NB could either be an E-UTRA eNB (small cell) for which the 3GPP Rel12 original feature was introduced or be a NR 5G gNB to support 5G NSA options 3A/3X.

The master eNB, at which the S1-MME terminates, performs all necessary S1-MME related functions (as specified for any serving eNB), such as mobility management, relaying of NAS signaling and E-RAB handling, and manages the handling of user plane connection of S1-U.

The feature supports a new E-UTRAN-initiated S1AP E-RAB modification indication procedure to the secondary gNB or eNB. The MME initiates a modify bearer request procedure with secondary gNB/eNB S1-U tunnel IDs toward the S-GW to switch the S1-U paths of the connected UE to the gNB/eNB termination point.

The MME supports the E-UTRAN initiated UE context modification procedure.

On receipt of an UE Context Modification Indication with CSG Membership Information, the MME verifies the CSG Membership and responds with the UE Context Modification Confirm (CSG Membership Status) message.

17.2 MME support for NSA option 3A/3X EDCE5 enhancements (Feature f10904-08)

The feature supports 5G new radio via dual connectivity also known in 3GPP as EDCE5, including per UE PLMN services control of access to 5G NR when used as a secondary RAT, per UE subscription based access control to 5G NR with MME local override options, and others.

The support includes:

- per UE PLMN services control of access to 5G NR when used as a secondary RAT
- per UE subscription based access control to 5G NR with MME local override options
- extension of EPS QoS range including AMBR from 4.29 Gbps up to 4 Tbps on S6a, S1AP and NAS interfaces
- 5G UE radio access capability handling in MME and over S1AP
- 5G UE additional NR security capability
- enhanced S-GW/P-GW selection with +nc-nr for Nokia S-GW/P-GW selection mode 2
- bearer setup with QCIs 80, 82, and 83 to support applications with lower latency requirement
- 5G capable UE handling during IRAT between 2G/3G and LTE
- various performance measurement (PM) counts for 5G capable UEs
- CLI command to show subscriber count of allowed 5G UEs
- QoS bitrates adjustment above or below 4.29 Gbps, when NR UEs move between MMEs or between GERAN/UTRAN and LTE, based on old/new node support for DCNR

To allow provisioning of the higher UE AMBR, APN AMBR, and GBR bearer maximum/guaranteed bit rates supported by 5G technology, the following values are extended to allow up to 4 Tbps:

- `failopenProfile`
 - user equipment aggregate maximum bit rate downlink
 - user equipment aggregate maximum bit rate uplink
- `failopenProfileApnConfig`
 - access point name aggregate maximum bit rate downlink
 - access point name aggregate maximum bit rate uplink
- `gbrQciQosProfile`
 - guaranteed dedicated bearer uplink bit rate
 - guaranteed dedicated bearer downlink bit rate
 - guaranteed dedicated bearer maximum uplink bit rate
 - guaranteed dedicated bearer maximum downlink bit rate
- `imsiRangeService`

- UE aggregate maximum uplink bit rate
- UE aggregate maximum downlink bit rate
- `lteTo2G3GQosMapping`
 - apn AMBR for uplink rate in kilobits per second
 - apn AMBR for downlink rate in kilobits per second
- `plmn`
 - Max UE AMBR uplink rate
 - Max UE AMBR downlink rate
- `qosProfile`
 - APN aggregated maximum bit rate uplink for default bearer
 - APN aggregated maximum bit rate downlink for default bearer
 - guaranteed dedicated bearer uplink bit rate
 - guaranteed dedicated bearer downlink bit rate
 - guaranteed dedicated bearer maximum uplink bit rate
 - guaranteed dedicated bearer maximum downlink bit rate
- `qosProfileBackTc`
 - Quality of Service (QoS) default maximum bit rate for uplink for background class (in kbps)
 - Quality of Service (QoS) default maximum bit rate for downlink for background class (in kbps)
- `qosProfileConvTc`
 - Quality of Service (QoS) default maximum bit rate for uplink for conversational traffic class (in kbps)
 - Quality of Service (QoS) default maximum bit rate for downlink for conversational traffic class (in kbps)
 - Quality of Service (QoS) default guaranteed bit rate for uplink for conversational traffic class (in kbps)
 - Quality of Service (QoS) default guaranteed bit rate for downlink for conversational traffic class (in kbps)
- `qosProfileInteractTc`
 - Quality of Service (QoS) default maximum bit rate for uplink for interactive traffic class (in kbps)
 - Quality of Service (QoS) default maximum bit rate for downlink for interactive traffic class (in kbps)
- `qosProfileStreamTc`
 - Quality of Service (QoS) default maximum bit rate for uplink for streaming traffic class (in kbps)
 - Quality of Service (QoS) default maximum bit rate for downlink for streaming traffic class (in kbps)

- Quality of Service (QoS) default guaranteed bit rate for uplink for streaming traffic class (in kbps)
- Quality of Service (QoS) default guaranteed bit rate for downlink for streaming traffic class (in kbps)
- uePlmnServices
 - LTE UE aggregate maximum uplink bit rate
 - LTE UE aggregate maximum downlink bit rate

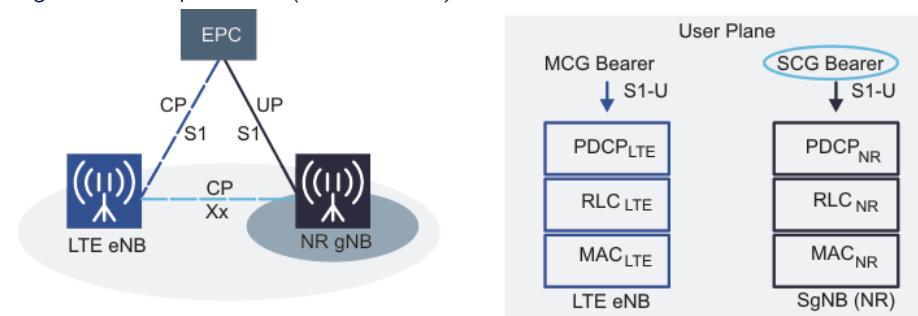
17.3 Secondary RAT usage reporting for 5G NSA option 3X (Feature f10904-03)

This feature supports secondary RAT usage reporting for 5G dual connectivity NSA option 3X. The feature is enabled per UE PLMN.

Dual connectivity

Dual connectivity involves two NBs, master and secondary NBs, in providing radio resources to a given UE (with active radio bearers), while single S1-MME termination point exists for an UE between a MME and the E-UTRAN. The secondary NB can either be an E-UTRA eNB (small cell) or a NR 5GNB to support NSA option 3A/3X as depicted in the figures.

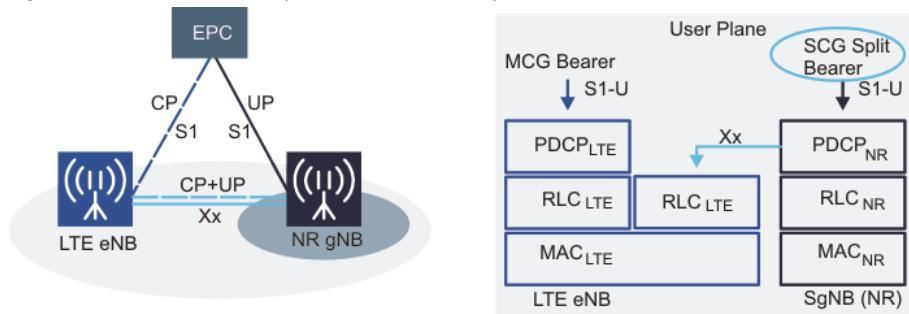
Figure 142: Option 3a (SCG bearer)



In the 3a option,

- S1U is anchored at the gNB
- Mobility signaling between LTE and NR is visible to EPC due to S1 path switch
- EPC needs to support E-RAB modifications
- S1-U is not split and it is delivered over NR
- There is no additional load to LTE eNB, no flow control is needed
- Xx interface is used for control plane traffic only
- UE mobility interruption (NR to LTE): impact is due to S1 path switch from gNB to eNB

Figure 143: Option 3x (SCG split bearer)



In the 3x option,

- S1U is anchored at the gNB
- Mobility signaling between LTE and NR is visible to EPC due to S1 path switch
- EPC needs to support E-RAB modifications
- S1-U is split at the gNB
- LTE eNB transmits a fraction of the user data
- Xx interface needs to support CP and split user traffic, flow control, and strict latency requirements

When a secondary RAT can be used in conjunction with E-UTRAN, the HPLMN or VPLMN operator may wish to record the data volume sent on the secondary RAT.

Provisioning

MME supports local configuration, per UE PLMN services, to enable or disable volume reporting for secondary RAT when the dual connectivity feature is enabled. The provisioning requires creating an enhanced dual connectivity profile which includes

- `irPgw` = true/false: whether P-GW is intended recipient of Secondary RAT Usage Reports
- `irSgw` = true/false: whether S-GW is intended recipient of Secondary RAT Usage Reports

MME also supports a configurable timer `secondaryRatUsageReportingDelay` to wait for Path Switch Request. It is used to delay sending the Secondary RAT Usage Data Report when a X2 handover procedure follows the receipt of a S1AP Secondary RAT Data Usage Report.

Supported procedures

MME supports eNB-initiated Secondary RAT Data Usage Report procedure. The purpose of this procedure is for the eNB to periodically or during handover provide Secondary RAT Usage Report on the used NR resources. Handover flag is only set during handover

procedures.

MME supports Secondary RAT Usage Report List IE in the following S1AP messages over S1-MME:

- E-RAB MODIFY RESPONSE
- E-RAB RELEASE RESPONSE
- E-RAB RELEASE INDICATION
- E-RAB MODIFICATION INDICATION
- UE CONTEXT RELEASE REQUEST
- UE CONTEXT RELEASE COMPLETE
- UE CONTEXT SUSPEND REQUEST
- SECONDARY RAT DATA USAGE REPORT

MME supports Secondary RAT Data Usage Report IE along with Secondary RAT Type = NR and associated handling in the following S11 messages:

- Create Session Request. MME includes Secondary RAT Data Usage during the following procedures:
 - X2-based handover with S-GW relocation (`irSgw` = false)
- Modify Bearer Request. MME includes Secondary RAT Data Usage during the following procedures:
 - X2-based handover with or without S-GW relocation
 - S1-based handover with or without MME or S-GW relocation
 - E-UTRAN-initiated E-RAB modification
 - S1-based handover with MME relocation
- Modify Access Bearers Request. `irPgw` is set to false since request message is only intended for S-GW.
- Change Notification Request. The trigger for the Change Notification, regardless of ULI change, is receiving of Secondary RAT Data Usage from eNB in the following procedures:
 - Connection suspend
 - S1 release
 - E-UTRAN to UTRAN Iu mode or GERAN A/Gb mode inter-RAT handover
 - MME to 3G-SGSN combined hard handover and SRNS relocation
 - eNB periodic reporting of secondary RAT data usage with no other S11 signalling to the S-GW (Handover flag is not set)
 - RAU
- Forward Relocation Complete Acknowledge (MME relocation)
- Delete Session Request. MME includes Secondary RAT Data Usage during the following procedures:
 - UE-initiated detach
 - MME-initiated detach

- HSS-initiated detach
- UE or MME requested PDN disconnection
- S1/X2-based handover with S-GW relocation (`irPgw` = false)
- E-UTRAN to UTRAN Iu mode or GERAN A/Gb mode inter-RAT handover
- MME to 3G-SGSN combined hard handover and SRNS relocation
- RAU
- Delete Bearer Response
 - P-GW-initiated bearer deactivation
- Delete Bearer Command. MME includes Secondary RAT Data Usage during the following procedures:
 - MME initiated dedicated bearer deactivation
- Release Access Bearers Request. MME includes Secondary RAT Data Usage during the following procedures:
 - Connection suspend (`irPgw` = false)
 - S1 release (`irPgw` = false)

17.3.1 Secondary RAT usage reporting procedures

Descriptions of procedures used for secondary RAT usage data reporting.

Secondary RAT usage data is provided in a new IE of an existing S1AP message

If the Secondary RAT Usage Report is provided by an S1AP message from eNB to MME and the provisionable per serving PLMN Volume Reporting for Secondary RAT flag is enabled and at least the intended receiver S-GW (IRSGW) flag or intended receiver P-GW (IRPGW) flag is set, the MME will transfer the secondary RAT usage data to the S-GW and P-GW (for example, during S1 release procedure).

Figure 144: Secondary RAT usage report is provided by S1AP E-RAB-RELEASE-RESPONSE

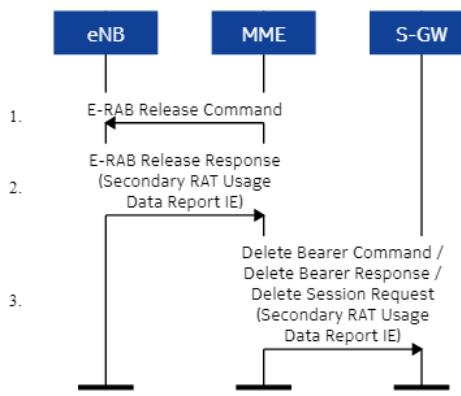


Figure 145: Secondary RAT usage report is provided by S1AP E-RAB-RELEASE-INDICATION

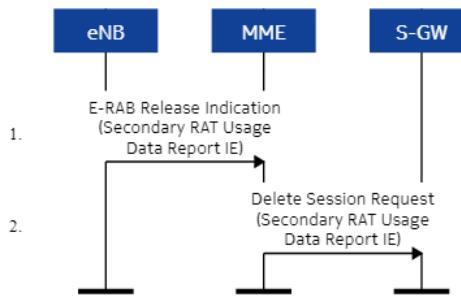


Figure 146: Secondary RAT usage report is provided by S1AP E-RAB-MODIFICATION-INDICATION

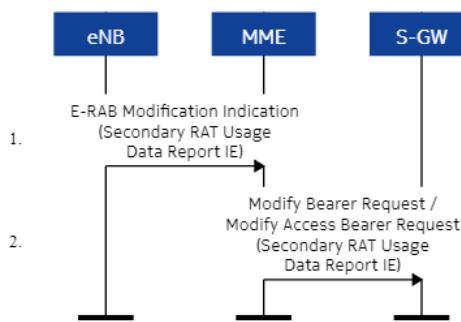


Figure 147: Secondary RAT usage report is provided by S1AP UE-CONTEXT-RELEASE-REQUEST

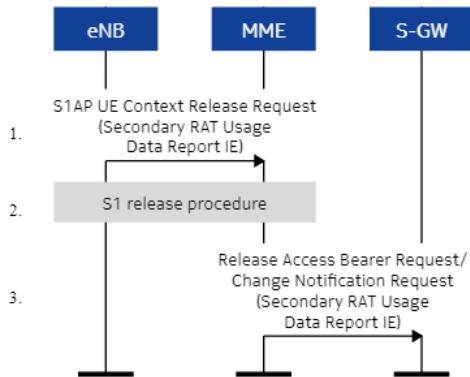


Figure 148: Secondary RAT usage report is provided by S1AP UE-CONTEXT-RELEASE-COMPLETE

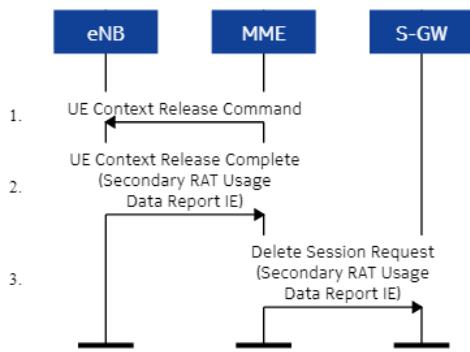
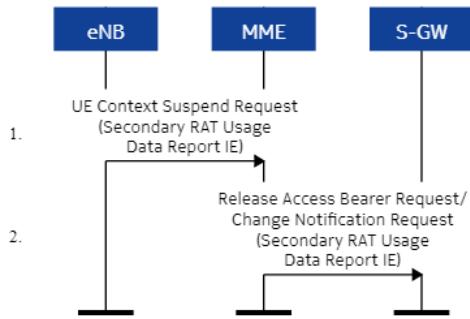


Figure 149: Secondary RAT usage report is provided by S1AP UE-CONTEXT-SUSPEND-REQUEST



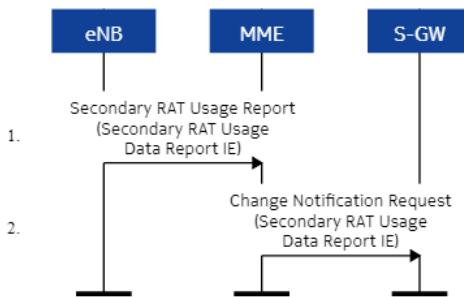
Secondary RAT usage report is provided by S1AP message S1AP SECONDARY-RAT-USAGE-REPORT

The eNB, if it supports dual connectivity with a secondary RAT, using unlicensed spectrum aggregation in the form of LAA/LWA/LWIP, and it is configured to report secondary RAT usage data for the UE, depending on certain conditions, it sends a RAN usage data report message to the MME including the secondary RAT usage data for the UE. The RAN usage data report includes a handover flag to indicate when the S1AP message is sent triggered by X2 handover. The secondary RAT usage data is provided by S1AP SECONDARY-RAT-USAGE-REPORT.

The MME will process the S1AP SECONDARY-RAT-USAGE-REPORT only if the serving PLMN provisionable Volume Reporting for Secondary RAT flag is enabled and either or both the intended receiver S-GW (IRSGW) flag or intended receiver P-GW (IRPGW) flag is set.

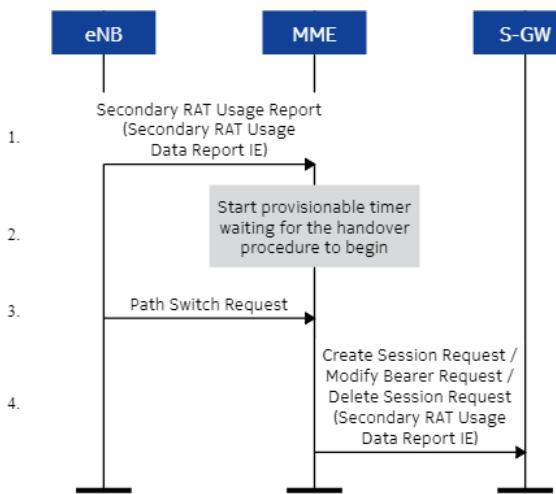
Upon receipt of the S1AP SECONDARY-RAT-USAGE-REPORT, if the handover flag is not present, the MME immediately forwards the Secondary RAT Usage Data Report to the S-GW via the S11 CHANGE-NOTIFICATION message.

Figure 150: Handover flag not present



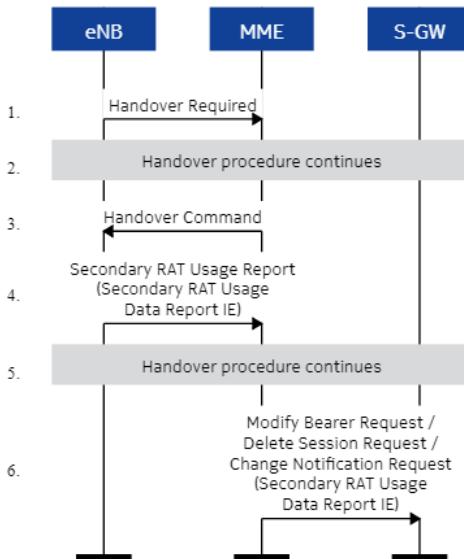
Upon receipt of the S1AP SECONDARY-RAT-REPORT, if the handover flag is true, the MME will start a provisionable timer awaiting for a X2 handover procedure to be triggered by the eNB. If the timer expires before receiving the S1AP PATH-SWITCH-REQUEST, the MME immediately forwards the Secondary RAT Usage Data Report to the S-GW via the S11 CHANGE-NOTIFICATION message. If the S1AP PATH-SWITCH-REQUEST is received before the timer expires, the MME forwards the Secondary RAT Usage Data Report to the S-GW via the S11 CREATE-SESSION-REQUEST, MODIFY-BEARER-REQUEST, DELETE SESSION REQUEST, and/or CHANGE NOTIFICATION message, depending on the X2 handover procedure.

Figure 151: Handover flag is true



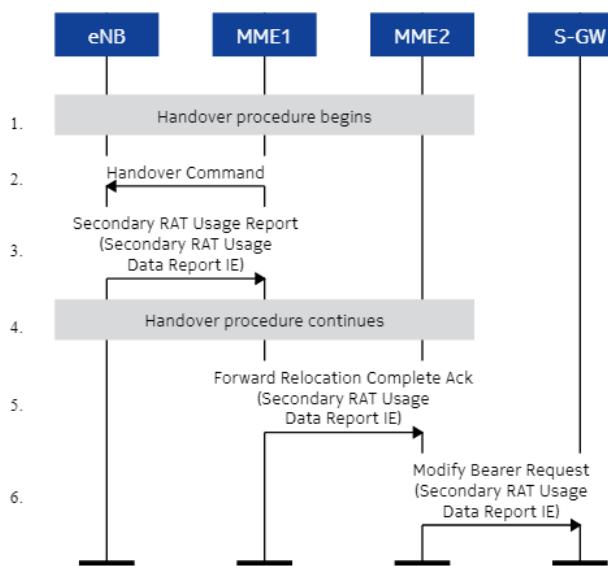
Upon receipt of the S1AP SECONDARY-RAT-REPORT during an ongoing handover procedure, the MME forwards the Secondary RAT Usage Data Report to the S-GW via the S11 MODIFY-BEARER-REQUEST, DELETE SESSION REQUEST, and/or CHANGE NOTIFICATION message, depending on the handover procedure.

Figure 152: Ongoing handover procedure



Upon receipt of the S1AP SECONDARY-RAT-REPORT, the Secondary RAT Usage Data Report will be forwarded to the target MME via the S10 FORWARD-RELOCATION-COMPLETE-ACK message and the MME then forwards it to the new S-GW via the S11 MODIFY-BEARER-REQUEST message.

Figure 153: MME relocation



17.4 MME support for 3GPP 5G dual connectivity EDCE5 enhancements (Feature f10904-02)

This feature extends 3GPP 5G dual connectivity EDCE5 support by enhancing P-GW/S-GW selection with NR capability to include GW selection mode 1 support.

Feature *MME support for dual connectivity* is a 3GPP Rel12 EPC feature that was originally introduced to support extended LTE coverage via small cells and is now being adopted to augment LTE coverage with extended 5G NR coverage via EPC core. This type of LTE deployment with dual connectivity to 4G and 5G radios is what referred to in 3GPP as Non-Stand Alone (NSA) option 3/3A/3X.

This feature adds support for:

- UE subscription based access control indication via HSS
- UE capability indication of 5G NR support
- Increased subscribed UE/APN-AMBR beyond 4.29 Gbps and up to 4 Tbps
- Increased S1AP UE-AMBR bit rate up beyond 10 Gbps and up to 4 Tbps
- Increased EPS QoS bit rate for GBR and non-GBR
- Enhanced S-GW/P-GW selection for 5G NR UEs

17.5 Treating UE as supporting DC-NR based solely on HSS ARD "NR as Secondary RAT in E-UTRAN Not Allowed" bit (Feature f10904-24)

This feature allows the MME to select the S-GW/P-GW only based on the HSS access restriction data (ARD).

When this feature is enabled and the HSS ARD allows NR to be the secondary RAT for a UE, the MME select a S-GW/P-GW with nc-nr flag in DNS entry for the UE, regardless of the UE's network capability of DC-NR.

17.6 Indication of DC-NR support in Attach/TAU Accept message even when UE is not allowed 5G3x service (Feature f10904-31)

This feature allows the MME to send DC-NR support indication to the UE in the Attach/TAU Accept message even if the MME has determined the UE is restricted 5G3x service and regardless of the UE's support of DC-NR indication to the network or not.

The feature is controlled via the `dcnrIndToUe` parameter of the `enhancedDualConnectivityProfile` command. When the feature is enabled, the MME sends DC-NR support indication to the UE in the Attach/TAU Accept message even if the MME determines that the UE is DC-NR access restricted, regardless of the UE's network capability of DC-NR. However, the MME will still indicate UE 5G3x restriction to the eNB.

The MME uses the restriction criteria defined in the below features to determine the UE DC-NR restriction and whether the DC-NR restriction indication is sent to the UE.

- *MME support for 3GPP 5G dual connectivity EDCE5 enhancements (Feature f10904-02)*
- *MME support for NSA option 3A/3X EDCE5 enhancements (Feature f10904-08)*
- *Treating UE as supporting DC-NR based solely on HSS ARD "NR as Secondary RAT in E-UTRAN Not Allowed" bit (Feature f10904-24)*

17.7 MME support for N26 LTE Interworking - 5G (Features f13501-03 and f13501-05)

This feature introduces MME support for N26 LTE interworking. The N26 interface is an inter-CN interface between the MME and 5GS AMF to enable interworking between EPC and the NG core network.

The N26 interface supports a subset of the functionalities that are supported over S10 interface.

The following mobility procedures between the AMF (Access and Mobility management Function) and the MME using the N26 interface are supported:

- EPS to 5GS idle mode mobility procedure
- 5GS to EPS idle mode mobility procedure
- EPS to 5GS handover procedure
- 5GS to EPS handover procedure

For the UE to be able to move from EPS to 5GS network, during attach or TAU procedure, the N1 mode flag within the UE network capability IE should be set to `N1 mode supported`. Additionally, when the UE retrieves the subscription data from the HSS, the core network restrictions AVP allows access to 5GC and the access restriction data AVP allows NR (New Radio) in 5GS.

During PDN establishment, the MME selects a P-GW that is SMF+PGW-C compatible. For the MME to proceed with such a selection, the APN (that forms the P-GW FQDN) that is resolved through DNS, should have interworking 5GS indicator set in the APN configuration AVP which is received as part of subscription data from HSS. If this indicator is set, the MME sends NAPTR query to DNS server and selects only the records that have the `+nc-smf` character string in their app-protocol name. If there are no such records, then the MME fallbacks to non SMF+PGW-C compatible P-GWs.

When UE moves from EPS core network to 5GS, the MME includes in the Context Response (IRAT TAU) or Forward Relocation Request (IRAT HO) only the PDNs that are eligible for N26 interworking, as described above. If a PDN does not have this characteristic, the MME deletes the PDN towards the S-GW/P-GW at the mobility completion.

In case of IRAT attach or IRAT TAU, where GUTI is generated from AMF, the MME resolves AMF IP through DNS with the following AMF FQDN format to retrieve IMSI from the old AMF:

```
pt<AMF Pointer>.set<AMF Set Id>.region<AMF Region  
Id>.amfi.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

In case of IRAT HO from EPS to 5GS, the MME resolves target AMF IP through DNS server using the following 5GS Tracking Area Identity (TAI) FQDN:

```
tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.  
5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

In case of 5GS to EPS idle mode mobility or HO procedure, the MME detects that the UE comes from 5GS from the F-TEID of S11/S4 S-GW GTP-C received in Forward Relocation Request (HO) or Context Response (TAU). In this case, the IP of S-GW will have value 0.0.0.0.

This means that in a 5GS to EPS idle mode mobility or in a handover scenario, the MME will always trigger S-GW relocation.

Finally, in HO scenarios from EPS to 5GS and vice versa, the MME will always trigger indirect tunnel establishment with S-GW.

17.7.1 N26 interworking procedures

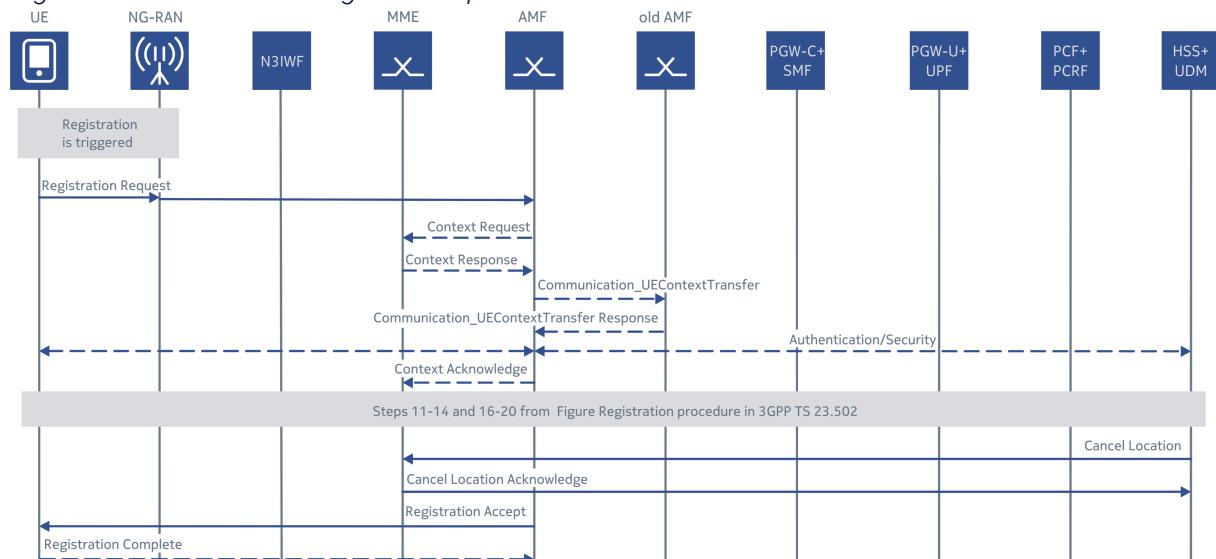
Below are presented the supported mobility procedures between MME and AMF.

17.7.1.1 EPS to 5GS idle mode mobility procedure

MME supports the registration procedure that is performed during the EPS to 5GS idle mode mobility procedure for single-registration UE(s) using the N26 interface.

The registration procedure as defined in 3GPP TS 23.502 is presented below.

Figure 154: EPS to 5GS registration procedure



- **Registration Request**

The UE sends the Registration Request message with registration type set to Mobility Registration Update, including the 5G-GUTI as it has been mapped from EPS GUTI (as the old GUTI). The native 5G-GUTI (if available) can be set as additional GUTI indicating that the UE is removing from EPC. The additional GUTI is provided in both the idle and connected state, if available.

- **Context Request/Context Response and Context Acknowledge**

These steps are not performed when the registration procedure is part of the EPS to 5GS

handover procedure.

- Context Request

This message is only performed for idle mode mobility. The target AMF derives the MME address and 4G GUTI from the old 5G-GUTI and sends Context Request to MME, including the EPS GUTI as mapped from 5G-GUTI and the TAU request message according to 3GPP TS 23.401. The MME validates the TAU message.

- Context Response

Provided that the Context Request message has been sent, the AMF converts the received EPS MM Context into the 5GS MM Context. The received EPS UE context includes the IMSI, the ME Identity, the UE EPS security context, the UE Network Capability, and EPS Bearer context(s). The EPS Bearer context includes for each EPS PDN connection, the IP address and the FQDN for the S5/S8 interface of the PGW-C+SMF and APN. The Context Response message includes also the UE NR security capabilities if the source MME has received this information during the last AMF to MME mobility procedure or from the UE during the attach/TAU procedure.

- Context Acknowledge

Provided that the Context Response message has been sent and the AMF accepts to serve the UE, then the target AMF sends the Context Acknowledge message to the MME according to 3GPP TS 23.401.

- Cancel Location/Cancel Location Acknowledge

In case of cancellation, the cancellation type is MME-Update procedure. For the PDN connections which have not been released in a standalone P-GW, the MME initiates PDN connection release procedure. In addition, the source MME needs to de-register the UE from the serving MSC/VLR as the UE is no longer reachable for SGs services as described in 3GPP TS 23.401 , chapter 5.3.3.1 (steps 13 to 14 and steps 18 to 19).

17.7.1.2 5GS to EPS idle mode mobility procedure

MME supports the 5GS to EPS idle mode mobility procedure using N26 interface as specified in 3GPP TS 23.502.

When the UE moves from the 5G Core network (5GC) to the EPC and it is in idle state, then the UE performs either a tracking area update or an initial attach procedure.

The UE performs the tracking area update procedure in any of the following cases:

- Both the UE and the EPC support attach without PDN connectivity.
- The UE has at least one PDU session for which the session continuity is supported during interworking (for example, the UE has EPS bearer ID and the received EPS QoS parameters are mapped).

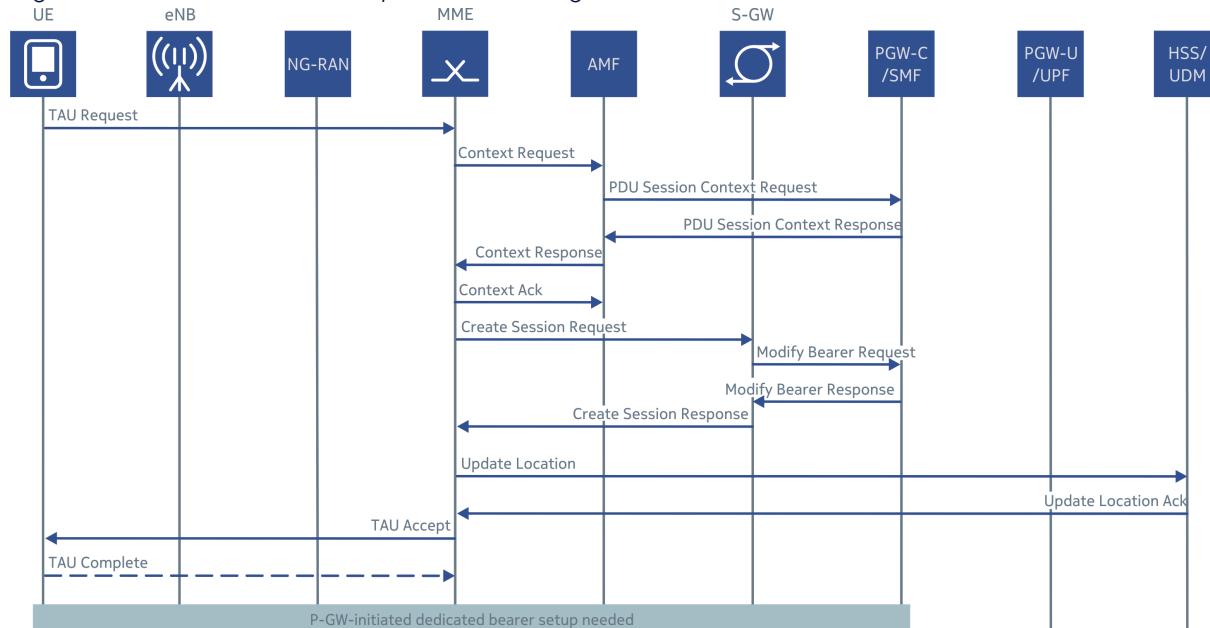
The UE performs an initial attach procedure in any of the following cases:

- The UE is registered without a PDU session in the 5GC.
- The UE is registered only with a PDU session for which session continuity is not supported during interworking to EPC and either the UE or the EPC does not support attach without PDN connectivity.

In accordance to the aforementioned criteria, the UE performs a tracking area update procedure in E-UTRA/EPS when it moves from NG-RAN/5GS to E-UTRA/EPS coverage area. The procedure includes the setup of the default EPS bearer and dedicated bearers in EPC. Reactivation of the EPS bearer(s) is also possible, if required.

The 5GS to EPC TAU procedure is shown in the figure:

Figure 155: 5GS to EPC TAU procedure using the N26 interface



■ Tracking Area Update Request

The TAU Request message is integrity protected using the 5GS security context available in the UE. The UE includes a GUTI, that is mapped from 5G-GUTI, in the old GUTI IE in the Tracking Area Update Request message. In addition, the UE includes the old GUTI type IE with GUTI value set to 'Native GUTI', and the UE status IE with a 5GMM (Mobility Management) registration status (for example, UE Status IE set to 'UE is in 5GMM-REGISTERED state').

■ Context Request

MME indicates in the Context Request message that it supports attach with or without PDN and non-IP PDN.

■ Context Response

Provided that the target access is allowed, the AMF responds with a Context Response

message including the mapped MM context (including the mapped security context) and the SM EPS UE context (default and dedicated GBR bearers) to the MME.

If the verification of the integrity protection fails or the target access is restricted, the AMF returns an appropriate error cause. If the AMF replies with a Context Response message with or without any active PDN(s), even in case when the target MME has indicated that it supports attach without PDN, then the target MME does not perform any signaling with S-GW/P-GW. The Context Response message also includes the UE NR security capabilities that target MME stores in database and then forwards it to the target AMF during the next registration or handover procedure.

- **Update Location Request**

The MME creates sessions to the target S-GW and updates the location with an Update Location request message that is sent towards the HSS

- **Tracking Area Update Accept/Complete**

The MME can provide to the eNB a PLMN list in the Handover Restriction List IE, having taken into account the last used 5GS PLMN ID and the Return preferred indication. It is possible that the MME does not release the signaling connection with the UE, based on the indication received in the TAU trigger that the UE is moving from 5GC (that is because the PGW-C+SMF can initiate dedicated bearer setup procedure).

After the TAU procedure completion, the dedicated bearer setup can be triggered by the PCRF+PCF. The latter can also provide the mapped QoS parameters, if PCC has been deployed. This procedure is specified in 3GPP TS 23.401, chapter 5.4.1 *Dedicated bearer activation*.

The MME can also initiate the update of the QoS parameters if the received QoS differ from the subscribed parameters.

17.7.1.3 EPS to 5GS handover procedure

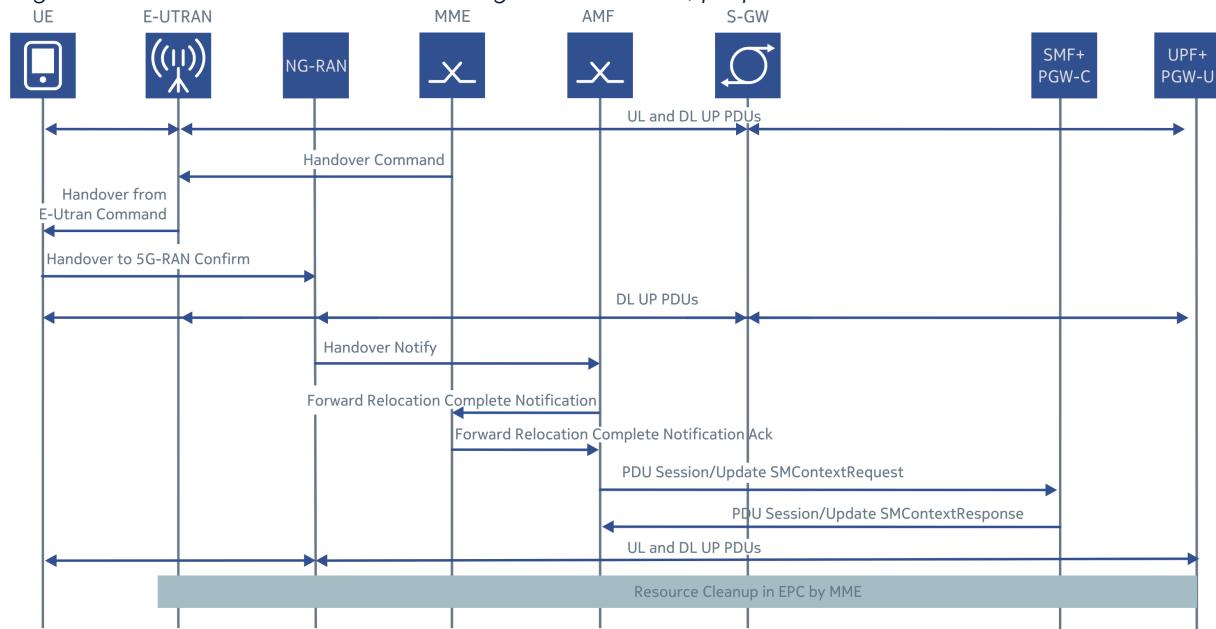
MME supports the EPS to 5GS handover procedure using the N26 interface for single-registration mode UE(s) as specified in 3GPP TS 23.502.

The procedure involves a handover to 5GS and a setup of QoS flows in 5GS.

In the case of handover to a shared 5GS network, the source eNB selects a PLMN that is going to be used in the target network. A supporting MME provides the AMF, through the N26 interface, an indication that the source EPS PLMN is the preferred PLMN.

The handover preparation steps are described below:

Figure 156: EPS to 5GS handover using N26 interface, preparation



■ Handover initiation/Handover required

The procedure includes the S1-based handover procedure as described in 3GPP TS 23.401 (chapter 5.5.1.2.2, steps 1 and 2).

■ Forward Relocation Request

The procedure includes the handover as described in 3GPP TS 23.401 (chapter 5.5.1.2.2, step 3) with the following modifications:

- The MME UE context includes the IMSI, the ME Identity, the UE security context, the UE Network Capability, and the EPS Bearer context(s).
- The Direct Forwarding Flag indicates indirect forwarding.
- The MME EPS Bearer context(s) includes for each EPS PDN connection the IP address, the FQDN for the S5/S8 interface of the P-GW-C+SMF and the APN. It also includes for each EPS bearer the IP address and the CN tunnel info at the UPF+PGW-U for uplink traffic.

■ Forward Relocation Response

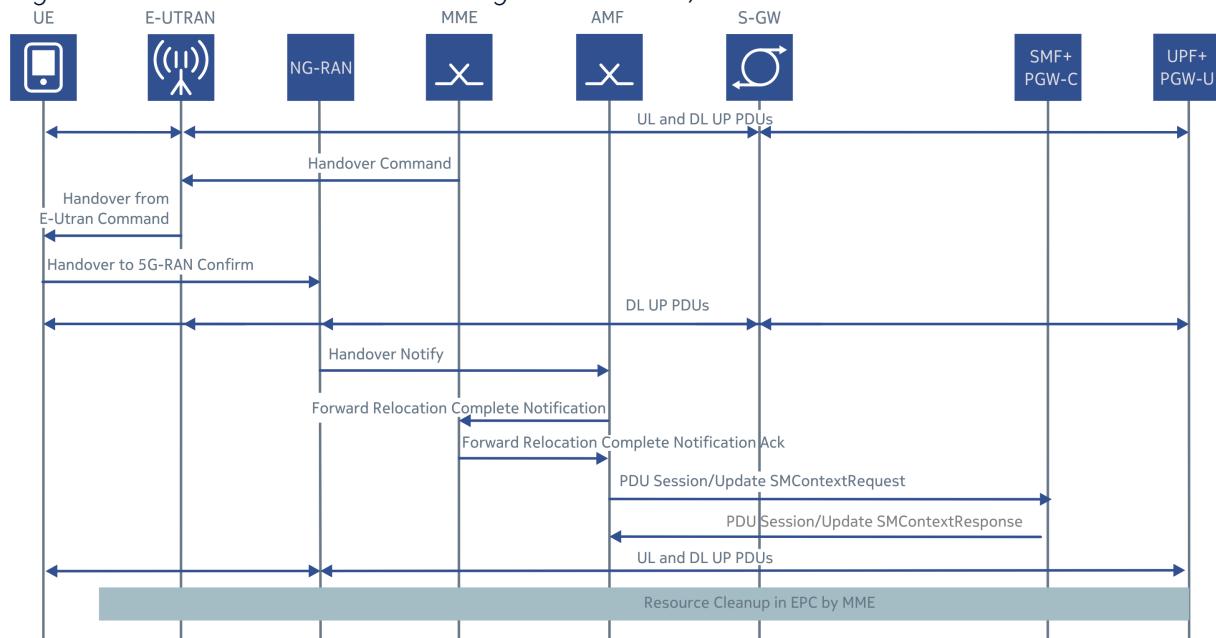
The AMF sends the Forward Relocation Response message to the source MME including the Cause, the Target to Source Transparent Container, the Serving GW change indication, the CN Tunnel info for data forwarding, the EPS Bearer setup list, the AMF Tunnel Endpoint identifier for Control Plane, the Addresses and the TEIDs. The EPS bearer setup list is the combination of EPS bearer setup lists provided from different P-GW-C+SMF(s). The AMF can also send Forward Relocation Response message indicating handover rejection (for example, the target NG-RAN didn't accept the handover).

■ Create Indirect Data Forwarding Tunnel Request/Response

The procedure includes the step as described in Figure S1-based handover in 3GPP TS 23.401, chapter 5.5.1.2.2 (S1-based handover, normal).

The handover executions steps are shown in the figure:

Figure 157: EPS to 5GS handover using N26 interface, execution



- Handover Command/Handover from E-UTRAN Command

The MME sends the Handover Command message to the source eNB as described in 3GPP TS 23.401 (chapter 5.5.1.2.2, steps 9 to 11).

- Forward Relocation Complete Notification

The AMF knows that the UE has reached the target side and it informs the MME by sending the Forward Relocation Complete Notification message.

- Forward Relocation Complete Notification Acknowledge

The MME sends the Forward Relocation Complete Notification Acknowledge message as described in 3GPP TS 23.401 (chapter 5.5.1.2.2, step 14).

- UE Context Release Command/Complete

For the PDN connections which are anchored in a standalone P-GW, the MME initiates PDN connection release procedure. (3GPP TS 23.401, chapter 5.5.1.2.2).

If indirect forwarding has been used, then the timer's expiration (started after the Forward Relocation Complete Notification Acknowledge message) triggers the SMF+PGW-C to release temporary resources used for indirect forwarding. The latter resources are allocated in the preparation stage. Additionally, the source MME needs to de-register the UE from the serving MSC/VLR as the UE is no longer reachable for SGs services.

Particularly for old resource release at the source MME, the latter uses the existing GTP `s10rmUeDataAtSrcMme` timer configuration to safeguard the deletion of the old resources at the source MME when handover is completed.

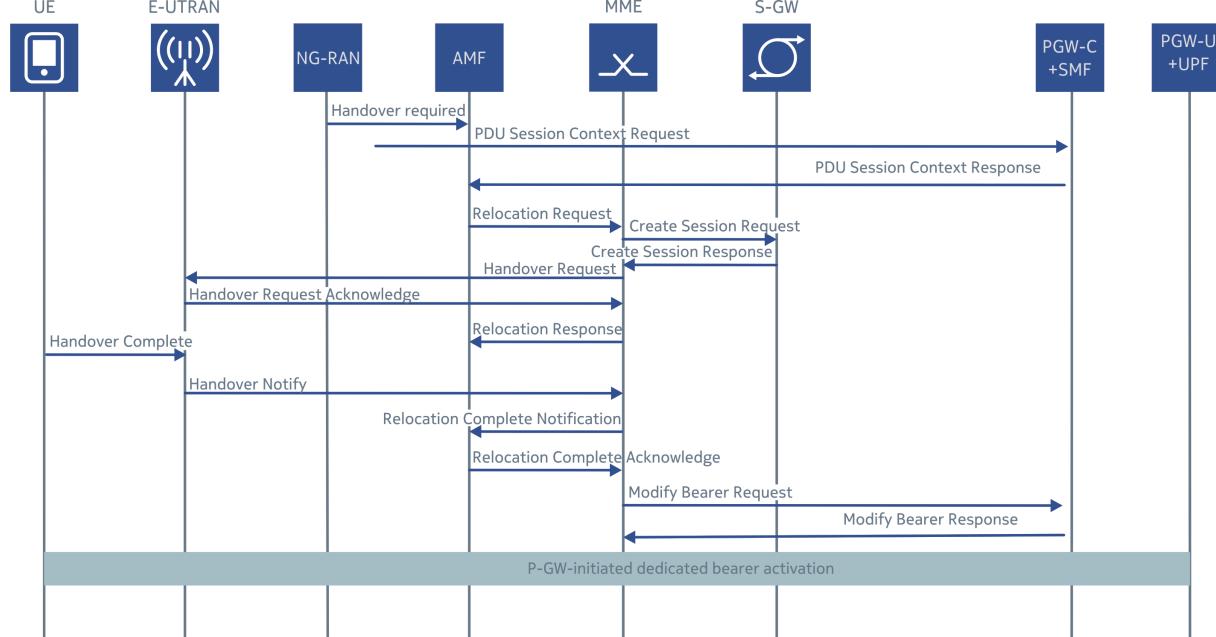
17.7.1.4 5GS to EPS handover procedure

MME supports the 5GS to EPS handover procedure using the N26 interface as defined in 3GPP TS 23.502.

The procedure involves the handover to EPC and the setup of default EPS bearer and dedicated bearers for GBR (Guaranteed Bit Rate) QoS flows in EPC. Reactivation of dedicated EPS bearers is also possible and it is performed by the P-GW, at the successful handover completion, at the target EPC.

The 5GS to EPS handover procedure is shown below in the figure:

Figure 158: 5GS to EPS handover procedure using N26 interface



- **Forward Relocation Request**

The AMF sends a Forward Relocation Request message to the target MME as defined in 3GPP TS 23.401 (chapter 5.5.1.2.2). The message includes the MME UE EPS PDN connection(s) and may include the UE NR security capabilities that the target MME stores in a local database and forwards it to the target AMF in the next registration or handover procedure. Note that the Handover Request message towards the target eNB includes the UE AMBR IE. The subscribed/used UE-AMBR can be included in the MME Context from the AMF.

- **Forward Relocation Response**

It is possible that the target MME may not implement a handover request (for example because the target eNB cannot allocate any of the requested radio bearers). In such a

case, the target MME sends a Forward Relocation Response message including an appropriate error cause and the handover procedure ends at this point.

In case the N26 feature is disabled at the target MME, then the latter will send a Forward Relocation Response with cause code Relocation Failure.

- Handover command

The AMF sends the Handover command to the source NG-RAN.

- Forward Relocation Complete Notification/Forward Relocation Complete Acknowledge

The AMF receives the Forward Relocation Complete Notification message from the MME when handover is completed from the target eNB. The AMF replies to the target MME with the Forward Relocation Complete Acknowledge message.

- Modify Bearer Request

The MME sends the Modify Bearer Request message to the target serving GW for each PDN connection, including the PDN connections that need to be released (3GPP TS 23.401, chapter 5.5.1.2.2).

- Modify Bearer Response

The Modify Bearer Response message is exchanged as defined in 3GPP TS 23.401, chapter 5.5.1.2.2. At this step, the UP path is established for both the default and the dedicated GBR bearers among the UE, the target eNB, the S-GW and the PGW-U+UPF. The PGW-C+SMF uses the EPS QoS parameters as they have been assigned for the dedicated EPS GBR bearers during the QoS flow establishment. The PGW-C+SMF maps all the other IP flows to the default EPS bearer.

P-GW may initiate Create Bearer Request procedure to set-up non-GBR dedicated bearers.

17.7.2 Support of UE usage type for selecting the target AMF

The MME supports the subscribed UE usage type for selecting the target AMF during EPS to 5GS handover procedure.

When the 5GS interworking feature is enabled at the MME and PLMN level and considering that the UE supports N1 mode, then the MME applies the following actions relevant to DCN:

- Indicates to the HSS that the DCN is supported and stores in local database the subscribed UE usage type (UUT), if this is received from the HSS as part of the subscription.
- Uses the subscribed UE usage type to discover the target AMF as part of EPS to 5GS handover using N26 interface.
- Forwards the subscribed UE usage type, if this exists in the local database, to the AMF in the Context Response or Forward Relocation Request message.

The AMF is selected based on the target 5GS TAI received from the source eNB. The 5GS TAI includes the 5GS TAC, the MNC and the MCC. The S-NAPTR procedure for finding a candidate set of AMFs for a target 5GS TAI will start at the 5GS TAI FQDN having at least the Service Parameters of "x-3gpp-amf:x-n26". When there is subscribed UE usage type, the procedure for an MME to find a candidate set of target AMF(s) makes use of the Service Parameters as follows: "x-3gpp-amf:x-n26+ue-<ue usage type>".

During the AMF selection, if the DCN feature is enabled, the records with '+ue-<uut>' extension in their app-protocol with 'x-n26' and app-service 'x-3gpp-amf' are prioritized. If there are no records that matches to UE usage type received from the HSS, then the MME checks if the `ueUsageSgwFallbackSelection` parameter of the `uePlmnServices` command is enabled. If it is enabled, then the MME selects an AMF that does not support the '+ue-<uut>' extension, otherwise the handover to 5GS procedure is aborted.

17.7.3 Return Preferred indication

A Return Preferred indication is specified in the Forward Relocation Request and Context Response messages to indicate a preferred return of the UE to the last visited EPS or 5GS PLMN at a later access change to an EPS or 5GS shared network.

During the mobility (connected/idle) from EPS network towards 5GS, the AMF receives from the MME an indication of 4G preferred PLMN to indicate the preferred return of the UE to the last used EPS PLMN, at a later handover, back to the 4G shared network. The AMF stores the last visited EPS PLMN info in the local UE context and sends it to the serving gNB as part of the mobility restriction list.

During the mobility (connected/idle) from 5GS network towards EPS, the AMF sends to the target MME an indication of 5G preferred PLMN to indicate the preferred return of the UE to the last visited 5GS PLMN, at a later handover, back to the 5G shared network. The MME stores the last visited EPS PLMN info in the local UE context and sends it to the serving eNB as part of the handover restriction list.

The indication of the Last NG-RAN PLMN identity is propagated from MME to the target eNB node in the Initial Context Setup Request, Handover Request, and Downlink NAS Transport.

This functionality is controlled via `4g5gRetPrefPlmn` global parameter.

17.7.4 N26 interworking with DCN and DCNR features

MME supports interworking between N26 and DCN/DCNR features.

Provided that any UE supports the N1 mode or the DCNR capability and has a particular UE usage type subscribed, the MME must be able to resolve any node (that is, S/P-GW) using the features that are supported by the UE and the MME/PLMN.

When the UE supports the N1 mode and it is DCNR capable, the GW selection incorporates both the nc-nr and nc-smf service parameters. Note that, when multiple network capabilities are embedded in the +nc-<network capability>, then they must be separated by the symbol ":" (for example, +nc-nr.smf.).

When searching for a network node having a particular network capability within a certain Dedicated Core Network (DCN), the character strings +nc-<network capability> and +ue-<ue usage type> are appended to the app-protocol name (for example, x-s5-gtp+nc-<network capability>+ue-<ue usage type> or x-s5-gtp+ue-<ue usage type>+nc+<network capability>).

MME prioritizes DCN feature DNS records (+ue-<uut> in app-protocol x-s5-gtp or x-s8-gtp and ap-service x-3gpp-pgw) against DCNR feature DNS records (+nc-nr in app-protocol x-s5-gtp or x-s8-gtp and ap-service x-3gpp-pgw) and DCNR feature DNS records against N26 feature DNS records (+nc-smf in app-protocol x-s5-gtp or x-s8-gtp and ap-service x-3gpp-pgw) in NAPTR response for apn fqdn query towards DNS. This means that if all the above features are enabled, then during PDN establishment, the MME will select between records that do have +ue-<uut>+nc-nr.smf extension else if fallback parameter for DCN and DCNR are enabled then SMF-PGW-C or standalone P-GW will be selected. The MME fallbacks by default to standalone P-GW if no record with +nc-smf extension in app-protocol is received.

17.7.5 Inter-system cause value mapping

The N26 interface supports the following cause value mappings.

Cause value mapping from S1AP cause to NGAP cause

The MME supports propagating the S1AP cause received from the source eNB (during inter-system handover) to the target AMF node by using the S1AP IE that is included in the Forward Relocation Request message. Also, MME supports reading, identifying and sending the NGAP cause value received from the source AMF (during inter-system handover) through the S1AP IE that is included in the Forward Relocation Request message. The following cause value mapping is used:

For the inter-RAT handover procedure from LTE (that is, served by MME to NG-RAN), the AMF maps the S1AP cause in the GTPv2 Forward Relocation Request message to an NGAP cause as it is shown in the table below. The AMF sends this NGAP cause in the NGAP

Handover Request message to the NG-RAN.

Table 71: Cause value mapping from S1AP cause to NGAP cause

Handover Required (S1AP cause)		Handover Request (NGAP cause)	
Group	Value	Group	Value
Radio Network Layer Cause	Time critical Handover	Radio Network Layer Cause	Time critical Handover
Radio Network Layer Cause	Resource Optimisation Handover	Radio Network Layer Cause	Resource Optimisation Handover
Radio Network Layer Cause	Reduce Load in Serving Cell	Radio Network Layer Cause	Reduce Load in Serving Cell
Any other value		Radio Network Layer Cause	Handover Desirable for Radio Reasons

For details, see *3GPP TS 36.413* and *3GPP TS 38.413*.

Cause value mapping from NGAP cause to S1AP cause in case of failure

The table below defines the cause value mapping that is performed by the AMF when it receives the NGAP Handover Failure message from the NG-RAN. This mapping is only needed if the inter-RAT handover fails in NG-RAN. For inter-RAT handover from LTE (that is, served by MME to NG-RAN), if the handover fails in accessing the NG-RAN, then the AMF maps the NGAP cause in the NGAP Handover Failure message to the S1AP cause (that is included in the Forward Relocation Response message) by using the following mapping. The AMF uses the S1AP cause in the GTPv2 Forward Relocation Response message to MME.

Table 72: Cause value mapping from NGAP cause to S1AP cause in case of failure

Handover Failure (NGAP cause)		Handover Preparation Failure (S1AP cause)	
Group	Value	Group	Value
Radio Network Layer Cause	No Radio Resources Available in Target Cell	Radio Network Layer Cause	No Radio Resources Available in Target Cell
Radio Network Layer Cause	Encryption and/or integrity protection algorithms not supported	Radio Network Layer Cause	Encryption and/or integrity protection algorithms not supported
Miscellaneous Cause	O&M Intervention	Miscellaneous Cause	O&M Intervention
Any other value		Radio Network Layer Cause	Handover Failure In Target EPC/eNB Or Target System

For details, see 3GPP TS 38.413 and 3GPP TS 36.413.

Cause value mapping from NGAP cause to S1AP cause

The table below defines the cause value mapping that is performed by the AMF when it receives the Handover Required message from the NG-RAN. For the inter-RAT handover from NG-RAN to LTE (served by MME), the AMF maps the NGAP cause in NGAP Handover Required message to a S1AP-based cause by using the mapping below. The AMF uses this S1AP cause in the GTPv2 Forward Relocation Request message to MME.

Table 73: Cause value mapping from NGAP cause to S1AP cause

Handover Required (NGAP cause)		Handover Request (S1AP cause)	
Group	Value	Group	Value
Radio Network Layer Cause	Handover Desirable for Radio Reasons	Radio Network Layer Cause	Handover Desirable for Radio Reasons
Radio Network Layer Cause	Time Critical Handover	Radio Network Layer Cause	Time Critical Handover
Radio Network Layer Cause	Reduce Load in Serving Cell	Radio Network Layer Cause	Reduce Load in Serving Cell
Any other value		Radio Network Layer Cause	Resource Optimized Relocation

For details, see *3GPP TS 38.413* and *3GPP TS 36.413*.

Cause value mapping from S1AP cause to NGAP cause in case of failure

Below table defines the cause value mapping that is performed by the AMF when it receives the Forward Relocation Response message from MME. This mapping is only needed if the inter-RAT handover fails in LTE. For inter-RAT handover from NG-RAN to LTE (served by MME), if the handover fails in accessing the LTE then the AMF maps the S1AP cause received in the GTPv2 Forward Relocation Response message to an NGAP-based cause as it is shown in the table below. The AMF sends this NGAP cause in the NGAP Handover Preparation Failure message to the NG-RAN.

Table 74: Cause value mapping from S1AP cause to NGAP cause in case of failure

Handover Failure (S1AP cause)		Handover Preparation Failure (NGAP cause)	
Group	Value	Group	Value
Radio Network Layer Cause	No Radio Resources Available in Target Cell	Radio Network Layer Cause	No Radio Resources Available in Target Cell
Radio Network Layer Cause	Encryption and/or integrity protection algorithms not supported	Radio Network Layer Cause	Encryption and/or integrity protection algorithms not supported
Radio Network Layer Cause	No Radio Resources Available in Target Cell	Radio Network Layer Cause	No Radio Resources Available in Target Cell
Miscellaneous Cause	O&M Intervention	Miscellaneous Cause	O&M Intervention
Any other value		Radio Network Layer Cause	Handover failure in target 5GC/ NG-RAN node or target system

For details, see 3GPP TS 36.413 and 3GPP TS 38.413.

17.7.6 Emergency bearer over the N26 interface

The MME supports propagating and accepting the emergency bearer over the N26 interface.

The MME does not check the 5GS interworking allowed flag in the HSS subscription data for the emergency APN since the latter is not part of the UE subscription. The operator should ensure that the provisioned PGW-C IP address or the FQDN designate the combo pgw-c+smf, otherwise the emergency bearer will fail at the target node. Note that the 5GS Interworking Indication IE should be set in Create Session Request during emergency PDN connection setup for N1 capable UE when the feature is enabled at the MME.

17.7.7 Security context establishment

The MME supports mapped security context or security context reestablishment in N1 mode to S1 mode mobility, as specified in 3GPP TS 24.301.

During inter-system change from N1 mode to S1 mode in EMM-IDLE mode, if the UE is operating in the single-registration mode and:

- When the tracking area update procedure is initiated for mobility from 5GS to EPS, the UE will transmit a Tracking Area Update Request message integrity protected with the current 5G NAS security context and the UE will derive a mapped EPS security context. The UE will include the key set identifier eKSI indicating the 5G NAS security context value in the Tracking Area Update Request message.
- if the attach procedure is initiated and the UE has received an 'interworking without N26 interface not supported' indication from the network and the UE has a valid 5G NAS security context, the UE will send an Attach Request message integrity protected with the current 5G NAS security context and the UE will derive a mapped EPS security context. The UE will include the eKSI indicating the 5G NAS security context value in the Attach Request message.

During the inter-system change from N1 mode to S1 mode in 5GEMM-CONNECTED mode, the secure exchange of NAS messages is established between the MME and the UE by:

- the transmission of NAS security related parameters encapsulated in the AS signaling from the AMF to the UE triggering the inter-system handover. The UE uses these parameters to generate the mapped EPS security context; and
- after the handover, the transmission of a Tracking Area Update Request message from the UE to the MME. The UE will send this message integrity protected using the mapped EPS security context, but unciphered. From this time onward, all NAS messages exchanged between the UE and the MME are sent integrity protected and ciphered using the mapped EPS security context.

17.7.8 MME support for release 16 direct data forwarding (Feature f13501-07)

This feature supports 3GPP release 16 direct data forwarding in 5GS to EPS and EPS to 5GS handover procedures over the N26 interface.

When the direct forwarding path is available between the NG-RAN and the E-UTRAN, the MME may apply the direct tunnel forwarding function. The MME continues supporting the indirect tunnel if the direct tunnel is not available.

During 5GS to EPS and EPS to 5G handover procedures over the N26 interface, direct or indirect data forwarding applies for the downlink data performed as part of the handover, based on configuration in the MME.

When the global parameter `n26DirectFwd` is set to `Yes`, direct data forwarding is enabled over the N26 interface in 5GS to EPS and EPS to 5GS handover procedures.

When the global parameter `n26IndirectFwd` is set to `Yes`, indirect data forwarding is enabled over the N26 interface in 5GS to EPS and EPS to 5GS handover procedures.

When both the parameters are enabled, direct data forwarding has preference over indirect data forwarding in case the RAN and 5G also support direct data forwarding.

17.8 CMM support for Ethernet PDU for mobility across N26 interface (Feature f20102-01)

This feature supports 3GPP standard specified Ethernet PDUs on the AMF and the MME for handover and idle mobility procedures over the N26 interface.

This feature affects mainly the AMF, since the existing configuration is reused in the MME. This feature enables the AMF to control handling of Ethernet PDUs during mobility over the N26 interface. As target nodes, both the AMF and the MME indicate in the Context Request message if Ethernet PDUs are supported. Based on the indications received in the Context Request message, the target node includes Ethernet or non-IP PDUs in the context transferred to the source node. However, the AMF is not aware of the type of PDU session and so the AMF only passes the indication that Ethernet or non-IP PDUs are supported to the SMF, which responds accordingly.

For the case of connected mode mobility:

- the MME as the source node, such as in EPS to 5GS handover, always propagates Ethernet or non-IP PDUs to the target AMF.
- when the AMF serves as the source node, such as in 5GS to EPS handover, there is a configuration option to define if Ethernet or non-IP PDUs are supported by the target node.

Ethernet PDUs are supported end to end by the core network elements (such as the MME, the SP-GW, the AMF, the SMF, and the UPF) in order to achieve session continuity for the Ethernet PDUs over the N26 interface.

18. Availability/reliability

Reliability is provided by overload control, recovery from unexpected transaction combinations, optimized signaling and load balancing features.

18.1 Overload control

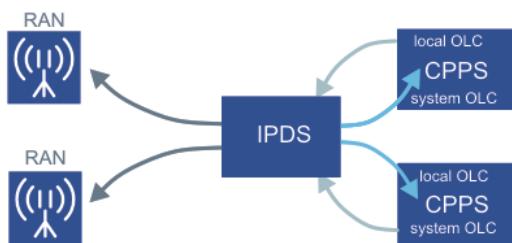
Memory, central processing unit (CPU), busiest core, and busiest process thread are monitored on the load balancer IP director services (IPDS) and control plane processing service (CPPS) virtual machines (VMs).

Overload conditions that are measured on individual IPDS and CPPS VM instances are forwarded and aggregated on IPDS, and then fed back to CPPSs that determine the right level of progressive shedding action to take.

There are multiple thresholds of escalating the MME reaction to the overload condition:

- Minor: Alarm, reduce overload control (OLC) averaging window
- Major: Progressive message shedding (idle UE procedures)
- Critical: Incremental progressive message shedding (idle and connected mode UE procedures)

Figure 159: Overload control



Enhanced attach storm strategy

The MME supports two thresholds for attach storm: a lower threshold at which IPDS instructs CPPSs to reject attaches and the higher attach storm threshold at which IPDS drops attaches. Thresholds are calculated based on the number of active CPPSs or the number of CPPSs that can be provisioned.

The lower threshold provides statistics and protection for peer nodes whereas the higher threshold protects the MME.

Delete bearer storm (monitor Delete Bearer Request (DBR) – silently drop beyond threshold)

This function provides an MME DBR threshold to protect the MME from overload because of excessive DBRs from S-GWs. Field experience at relatively low subscriber load has shown that various scenarios can result in S-GW mass delete of bearers that in scenarios at higher capacity or with multiple S-GWs might overwhelm the MME signaling capacity. Similar to the HSS attach rate threshold, this eOLC function prevents the MME overload through procedure drops with subsequent S-GW retries spreading out the event duration providing the MME time to process the spike in load.

DDN storm (monitor DDN – silently drop beyond threshold)

Safety-net limit allows up to 1600 DDNs per CPPS per second. Thus a CMM containing 10 CPPS supports 16000 DDNs per second.

Feature *CMM support for flexible size CPPS/DBS for MME/TA/AMF on Openstack (f80005-10)* increases the limit to 1920 DDNs per CPPS per second for an MME configured with 12 vCPUs per CPPS.

The threshold protects the MME from DDN storms that can put the CPPS or IPDS into CPU overload. When the DDN rate on the S11 interface exceeds the prorated limit, the algorithm forces the MME to drop additional DDNs exceeding the limit on a per second basis. While this results in S-GW retries, it protects the MME from overload because of an excessive DDN load.

Paging restriction in overload

This function is an overload control mechanism that restricts the use of more aggressive paging methods during a major overload on the MME. A restricted paging type is introduced, which only allows a single page attempt and a paging method of the last seen eNB or the last seen eNB list. This overload control mechanism is introduced to avoid S1 Paging message fan-out from the use of more aggressive paging methods, such as the last seen tracking area (TA), while in overload. By automatic switching to the restricted paging type during a major overload, the number of S1 Paging message generated by the MME application is dramatically reduced.

CPPS UE context manager object size (monitor list size and reject procedures beyond threshold)

This function monitors the number of UE context manager objects per CPPS and rejects call processing procedures beyond the threshold. A UE context manager object is created for every call processing procedure executed on the CPPS. While typical concurrent procedures are approximately 1000, the CPPS is dimensioned to support up to 24 000. Delay in execution of procedures because of time-out of peer nodes or internal delay can result in an increased number of concurrent procedures. No response at all from the HSS during an attach storm driven overload can, for example, consume up to 60% of the context manager objects before attach rate overload control starts dropping attach requests.

CPPS session input queue size (monitor queue size, drop procedures that require new context manager objects)

This function monitors the size of MME CPPS session manager input queue, which is typically very small (~50 messages). If there are delays in creating UE context manager objects for new procedures, this queue can be backed up. Upon reaching the overload threshold, the IPDS drops all requests for any new procedures (except Service Request as network-originated service requests are embedded procedures within larger paging request procedures).

IPDS memory overload (monitor, and switchover at extended period over critical overload threshold)

On IPDS, memory used is established at system initialization and grows very little with additional traffic load (IPDS uses about 12% of memory at 40 000 transactions/s). If IPDS memory is critically overloaded, the IPDS is switched over to its standby peer.

Additional overload control functions

The MME provides proprietary per call measurement data (PCMD). PCMD processing can be stopped to provide more CPU for call processing.

PCMD includes data from the CMM and eNBs and is collected on each active CPPS during evolved packet system mobility management (EMM) and evolved packet system session management (ESM) procedures. CPPSs send PCMD to the Network Element Cluster Controller (NECC) VM at the end of a procedure for logging onto disk.

For PCMD shedding purposes, an MME overload trigger is calculated as one of the following:

- IPDS input core CPU above overload threshold
- IPDS packet processing core above overload threshold
- IPDS average CPU above overload threshold
- IPDS busiest thread CPU above overload threshold
- all active CPPS instance average CPU above overload threshold
- all active CPPS instances busiest thread CPU above overload threshold

The MME enables the operator to select any of the four methods of PCMD treatment under overload through provisioning.

Related descriptions

- [CMM support for flexible size CPPS/DBS for MME/TA/AMF on OpenStack - Delivery](#)
(Feature f80005-10)

18.1.1 Overload notification to eNBs (Feature m10702-01)

The *Overload notification to eNBs* feature provides progressive network-level overload control when individual MMEs become critically overloaded.

There can be extreme situations where procedure rejection by the MME might cause central processing unit (CPU) overload. This can happen if eNBs ignore procedure rejection because of overload and keep offering heavy load to the MME. To help, under these situations, the MME has defined the concept of the MME wide overload when CPU usage is far beyond critical threshold. The MME overload is defined as follows: If the IP director services (IPDS) input core CPU is >75% or packet processing core CPU is >95%, or if the IPDS interface CPU or thread CPU is >95%, or if all the CPPSs have CPU or thread CPU >95%.

The MME overload is deliberately set higher than any other resource overload to trigger all other overload mitigation schemes (procedure rejection at major and critical overload) before the MME declares the MME overload.

Once the MME overload is triggered, the MME sends an Overload Start message to a randomly selected 5% of eNBs. If the MME overload persists or increases, the Overload Start message is sent to an additional 5% of eNBs in phases of 30 seconds until CPU falls below the MME overload threshold. The Overload Start message instructs eNBs to only permit RCC establishment for emergency sessions to the MME. The MME sends the Overload Stop message to eNBs in phases of 5% of eNBs that have received the Overload Start every 30 seconds once MME CPU is < 80%.

18.1.2 MME enhancements to overload control (Feature m10711-01)

The **MME enhancements to overload control feature changes the logic used to select messages or procedures to shed when the MME goes into major and critical overload. Progressive message shedding can be achieved with less service impact.**

The prior logic used the messages associated with procedures that generate the highest signaling load to maximize the impact of shedding and minimize the number of procedures aborted because of shedding.

The new logic uses procedures used by idle users during major overload, and only escalates to using procedures that affect connected users during critical overload.

Messages shed during a major overload change from attach, tracking area update (TAU), service request, paging, SGS paging, S1 handover, inter radio access technology (inter-RAT) handover with the generic number (GN), inter-RAT handover with the UTRAN, inter-RAT handover with the GSM, and context request to attach, TAU, service request, paging, and SGS paging.

Additional messages shed during critical overload change from S1 release, detach, X2 handover, create dedicated bearer, modify bearer, deactivate dedicated bearer, packet data network (PDN) connectivity, and PDN disconnect to S1 release, detach, X2 handover, create dedicated bearer, modify bearer, deactivate dedicated bearer, PDN connectivity, PDN disconnect, S1 handover, inter-RAT handover with GN, inter-RAT handover with UTRAN, and inter-RAT handover with GSM.

When the MME gets into minor central processing unit (CPU) overload (80%), the MME can be provisioned to ask all eNBs to stop sending per call measurement data (PCMD) data messages. The MME asks eNBs to resume sending PCMD data messages 5 minutes after coming out of a minor overload.

18.1.3 Sending RAB to S-GW as part of safety net upon DDN for connected UE (Feature m10138-01)

The **Sending RAB to S-GW as part of safety net upon DDN for connected UE feature cleans up bearer resources on the S-GW when the MME drops DDNs because of an overload.**

The MME has a safety net to handle the case in which the MME receives a DDN for a UE that is in the ECM-CONNECTED state. Currently, the MME sends a DDN Ack (accept), then it sends

the UE Context Release Command (normal release cause code), and then the DDN Failure Indication after the UE Context Release Complete message is received.

This feature changes the behavior that the MME sends Release Access Bearers Request to the S-GW as part of this scenario based on a provisioned value.

When the provisioning flag is not set (default value), the safety net works as it did before the implementation of this feature. With the flag set, where flag values are Yes or No and the flag name is `sendRabUponEcmConnectedDdn`, the RAB should be sent after the DDN failure indication.

18.1.4 Enhanced overload control to rebalance CPPS load (Feature m10709-01)

The *Enhanced overload control to rebalance CPPS load feature provides faster auto rebalancing of resources across control plane processing service (CPPS) virtual machines (VMs)*.

This feature introduces a preferred treatment mechanism to balance the load on the CPPS instances based on the number of UE context entries.

This mechanism gives priority to the lighter loaded CPPSs during a UE distribution to balance the number of subscribers among the CPPSs. The preferred treatment mechanism is adjusted every second as new subscribers are assigned to the lighter loaded VMs.

This feature also provides the following enhancements:

- New objects to the list of resources are monitored by the overload control function. Access point name (APN) usage and bearer resources are budgeted and when a CPPS exhausts either of them, it is no longer selected by the CPPS selection function as the recipient for new UE attaches.
- When usage thresholds for the new resources are exceeded, `ISS_softwareAllocatedResourceOverload` alarm is raised. The preferred treatment is used in scenarios where no imbalance is present. Round robin is the approach used by the CPPS selection.

When an imbalance is present, for example, because of the addition of a new CPPS in an in-service MME, the CPPS selection uses the preferred treatment where the least loaded CPPS is selected more often.

When the imbalance is no longer present, the CPPS selection function returns to the round robin distribution method.

The mechanism is especially useful during CPPS VM growth when all new subscribers should

be assigned to the new call processing VM.

During normal operational load, this mechanism rebalances the subscribers on the distributed CPPS VMs within 48 hours.

18.1.5 Provisionable NAS cause code for throttling (Feature m10108-04)

The *Provisionable NAS cause code for throttling* feature provides provisionable non-access stratum (NAS) cause code (CC) to be sent in UE mobility management reject messages because of any MME overload or any throttling of UE mobility management requests.

The default NAS cause code is set to #22 Congestion. The MME includes T3346 timer with a value of 0 whenever it rejects a UE request with cause code #22.

This is a precursor to the implementation of T3346 timer handling.

This feature provides faster recovery from the overload that escalated to attach rejects because of congestion.

18.1.6 Offloading overloaded CPPSs and support for T3346 timer (Feature m10709-02)

The *Offloading overloaded CPPSs and support for T3346 timer* feature provides graceful, automatic rebalance of the MME node when the distributed control plane processing service (CPPS) resources become unbalanced in carrying call processing traffic.

This feature enables the offloading of UEs from CPPS instances during periods of central processing unit (CPU) overload (CPU consumption above 85%) to lightly loaded CPPS instances, when available, in the MME. This feature also supports inclusion of T3346 timer when a UE mobility management request is rejected by the MME because of overload conditions, including a CPPS overload with the non-access stratum (NAS) cause code #22 Congestion.

Before the implementation of this feature, when IP director services (IPDS) or CPPS went into CPU overload, the MME responded by rejecting fractions of mobility management and session management procedures. As the CPU overload was increasing or decreasing, the MME progressively increased or decreased the fraction of procedures it rejected. As part of this rejection mechanism, international mobile subscriber identity (IMSI) and globally unique temporary identity (GUTI) attaches were also candidates for rejection.

The MME support for offloading overloaded CPPSs is built upon this mechanism of rejection of IMSI and GUTI attaches during CPPS CPU overload, in order to relocate UEs to lightly loaded CPPS instances in the MME, when available. Only sufficient UEs are offloaded so that the CPPS in CPU overload are brought out of CPU overload.

This feature provides capabilities that build upon the existing MME overload control mechanisms:

- Offload of all IMSI and GUTI attaches targeted for rejection from CPPS instances in CPU overload to the lightly loaded CPPS instances when available. Lightly loaded target CPPSs have CPU consumption lower than 70% and room available in the UE context table (cache).
- IPDS targets a percentage of IMSI and GUTI attaches towards CPPS instances in CPU overload and instructs the CPPS to reject these attaches and then to delete the UE context. The deletion of the UE context is only done when there are lightly loaded CPPSs within the MME. The UE context is deleted irrespective of whether the NAS cause code #22 is provisioned.
- When the MME rejects an Attach Request, it includes in the Attach Reject message a T3346 timer and sets the NAS cause code to #22 Congestion (this assumes that the MME overload mobility management (MM) rejection NAS cause code is set to 2). This spreads the reattaches back to the MME so that MME gets enough time to delete the UE context cleanup associated maps. Under CPU overload, the MME can reject GUTI attaches. This feature takes advantage of the rejection and sets the stage for subsequent offloading of the UE to a lightly loaded CPPS within the same MME.
- When the UE subsequently retries the IMSI or GUTI attach, the MME does not find UE context, forcing the MME to assign a CPPS that is not in CPU overload and has room in the UE context table. The MME proceeds with the Attach Request by obtaining IMSI from the UE to establish its identity.
- The IPDS distribution of the UE to CPPSs is done in such a way that CPPSs never experience overload. However, if CPPSs experience overload because of some unforeseen reason and there are lightly loaded CPPSs available, following new CPPS growth or after a fault of a CPPS instance or virtual machine (VM) and its subsequent recovery, the scheme offloads a certain percentage of UEs until the CPPSs in CPU overload come out of overload.
- The UE offload rate depends on the attach rate experienced by the MME and also by the procedure rejection rate applied to the CPPS in CPU overload.
- The UE offloading activity is done until the source CPPS's CPU overload alarm state goes from major to minor. After that point, no more forced offloading using the above method is done and it is left to weighted CPPS selection to do further balancing.

This feature's additional use of T3346 is as follows:

- If the NAS cause code #22 Congestion is used to reject attaches, tracking area updates (TAUs), and service requests because of IPDS CPU overload, and/or CPPS CPU or CXN object overload, the MME also includes the backoff timer T3346 information element (IE) and sets the T3346 value. The UE is expected not to send any new requests until the expiration of the timer. The NAS cause code #22 is only sent if provisioned.
- The MME enables the provisioning of a separate minimum and maximum timer value for attach, TAU, and service request procedures. It randomly selects a timer value between the minimum and maximum timer values. This random selection is used to avoid clustering of UE requests. If timer values are not provisioned, the MME sets the T3346 timer to 0.

The benefit of this feature is only seen if a majority of the UEs in an operator network support the handling of T3346 timer. The benefit of this feature is also shown when CPPSs go into CPU overload and lightly loaded CPPS instances are present in the same MME.

18.1.7 Offloading 3GPP Rel 12 diameter overload control - phase 1 (Feature m11316-03)

The *Offloading 3GPP Rel 12 diameter overload control - phase 1* feature provides network-level overload control to prevent or minimize network signaling storms caused by individual node overload or failure.

This feature is the first phase of 3GPP Rel 12 Diameter overload functions and is limited to support the DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY error code rejected by DRA when the entire cluster behind the routing address (DRA) is overloaded and if the alternate HSS segment is overloaded as well.

In this phase, the MME does not include the overload control supported features towards the DRA.

Upon receiving DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY (5198) result code from DRA, the MME rejects Attach, Tracking Area Update (TAU), or Service Requests initiated by UEs by mapping the result code to the non-access stratum (NAS) cause code #42 Severe network failure (sent to UE). The cause code #42 is a provisionable option where the operator can select an evolved packet system mobility management (EMM) NAS cause code to send.

For initial and update requests, the MME rejects the procedure and does not retry the secondary connection; however, if the request times out, the MME follows the current behavior on time-outs.

For termination (detach) requests, if the request times out, the MME does not retry the secondary server; however, as per existing behavior, it cleans up the session information.

The MME does not retry regardless of procedures/messages. There is no impact on Notify Request (NOR) or Purge UE Request (PUR) retry, because NOR/PUR does not fail UE-initiated procedures and does not send a NAS cause code to the UE.

18.1.8 GTP load and overload control (Feature m10727-01)

The *GTP load and overload control* feature provides network-level load and overload control to optimize load across network elements and prevent or minimize network signaling storms because of individual node overload or failure.

This feature supports 3GPP Rel 12-specified GTP load and overload control. The feature supports GTP load factor in GTPv2C messages and uses the load factor to load balance sessions across the S-GW and P-GW in addition to using the static capacity information obtained in the name authority pointer (NAPTR) records. Overload control does not apply to the emergency packet data network (PDN) and eMPS users. Furthermore, this feature does not support the access point name (APN)-level load control and overload control.

GTP load vs overload

GTP supports both load and overload control, which are two distinct but complementary concepts.

Load control enables a GTP-C entity (for example an S-GW/P-GW) to send its load information to a GTP-C peer, for example an MME, evolved packet data gateway (ePDG), to adaptively balance the session load across entities supporting the same function, for example an S-GW cluster, according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

Overload control enables a GTP-C entity that is becoming or is being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance, including impacts to handling incoming and outgoing traffic.

GTP load/overload control principles

1. Each network element has internal protection mechanisms regardless of the load/overload mechanisms.

2. Emergency calls are not a subject to overload control.
3. Both load and overload control are used.
4. Load/overload functions are not supported across public land mobile network (PLMN) boundaries.
5. Both load and overload control are supported at an individual node level.
6. An MME overload is in scope and is supported.
7. A node under overload provides a mechanism to reduce the overload locally.
8. Load and overload capabilities, that is, receiving and sending, are configurable features, which are enabled/disabled at the node level independently.
9. A message throttling to the S-GW is compliant with the 3GPP TS 29.274 clause 12.3.9.3. The maximum bit rate (MBR) because of tracking area updated (TAU) and handover have highest priority; that is, these messages are the last ones to be throttled. As a result, relocation of the UE to a new S-GW is not valid as this basically results in overloading the other gateways (GWs).

Guidelines

The MME populates overload reduction (OLR) metric per the following guidelines:

- For the first OLR report, overloaded node reports provisioned OLR to the receiving node; provisioned OLR uses the hard-coded initial value.
- For the successive OLR reports, a feedback mechanism with a message rejection rate of an overloaded node allows to converge to the previous OLR and maintain the optimal traffic that can be processed in an overloaded situation. The recommended formula is as follows:

$$\text{New_Overload_Reduction_Metric} = \text{Prior_Overload_Reduction_Metric} + (1 - \text{Fraction_Successfully_Handled_by_Overloaded_Node}) * [100 - \text{Prior_Overload_Reduction_Metric}]$$

In relation to publishing the overload, the following are some of the recommended guidelines on publishing the overload for GTP node:

- The GTP node must send the overload at least before the validity timer expires and the overload condition persists. Additionally, it includes the overload message in every message that is a failure/rejection and it also includes the cause code of GTP-C congestion.
- If the overload is sent in a request and a response is received, do not send the same overload with the same sequence number if the receiving node sent a successful response. Note that the P-GW sends it multiple times, once per each session process. If successful response is not received, sending node includes the overload information in every message.

- Once out of the overload condition, the sender sets overload reduction metric as null, as defined in 3GPP TS 29.274.
- The MME associates the info properly to the right P-GW fully qualified domain name (FQDN).
- The MME decides whether it sends the message to the P-GW taking into account both the S-GW and P-GW overload information. The same applies in the reverse direction, for the P-GW-initiated message to the MME, where the P-GW takes into account the S-GW and MME overload information.

GTP-C load control

The GTP-C load control can possibly apply to GTP-C interfaces towards GTP-C entities responsible for network node selection.

Stage 2 (see 3GPP TS 23.401 clause 4.3.7.1a.1 and 3GPP TS 23.060 clause 5.3.6.1a) already requires support of load control on the S11/S4 and S5/S8 interfaces as follows:

- An S-GW can signal its load information to the MME for enhanced load balancing across S-GWs.
- A P-GW can signal its load information to the MME through an S-GW for enhanced load balancing across P-GWs.

The GTP-C load control is not supported in Rel 12 for the following GTP-C-based interfaces:

- S3, S10 (selection of the target MME during inter-CN handover, limited GTP-C traffic, minimize impacts to the MME)
- Sm, Sn (the MME / selection by a multimedia broadcast/multicast service gateway (MBMS GW), limited GTP-C traffic, avoid impacts to the MBMS GW)
- Sv (MSC-S selection in MSC pools by the MME, avoid impacts to legacy circuit switching (CS) products)
- Gn/Gp (avoid impacts to legacy Gn-SGSN/GGSN products and GTPv1-C).

GTP overload control

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance, including impacts to handling of incoming and outgoing traffic. Overload control information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes, can be used to reduce or throttle or both the amount of GTP-C signaling traffic between these nodes. As such, the overload control information provides guidance to the receiving node to

decide actions, which leads to mitigation towards the sender of the information. The GTP-C overload control feature continues to allow for preferential treatment of priority users (eMPS) and emergency services. Support of overload control on the S11/S4 and S5/S8 interfaces is as follows:

- The MME can signal an overload to the P-GW.
- The S-GW can signal an overload to the MME.
- The P-GW can signal an overload to the MME through the S-GW.

 **Note:**

The MME does not signal an overload to the S-GW as this is redundant with DDN throttling.

Traffic flood can possibly occur on the S3 and S10 interfaces, resulting from a large number of users doing TAU/routing area update (RAU), for example, overlaid radio access technologies (RATs) and failure of radio access network (RAN) node, MME load rebalancing, train moving across MME pools boundaries, and so on. Beyond mobility management procedures, RAN information procedures can also generate traffic on these interfaces, for example, for self-organizing network (SON).

Throttling signaling on these interfaces resulting from user's mobility, that is, inter-MME TAU, RAU, and handover, result in bad end-user perception (handover failure, loss of packet data network (PDN) connections) and must be avoided as much as possible.

The MME in overload can drop locally incoming RIM messages without causing GTP-C retransmissions. However, this can cause the RAN to retransmit the message.

The support of the overload control over S3/S10 can be beneficial, but it is not critical as for some other interfaces. It is therefore recommended that the MME returns a cause indicating a node overload when it cannot process a request, other than a RAN Information Relay message, but is still able to answer.

The GTP-C overload control is not supported in Rel 12 for the following GTP-C based interfaces:

- S3, S10 (see considerations above, minimize impacts to the MME and S4-SGSN)
- S11/S4 (from an MME to an S-GW, with the S-GW as a consumer)
- S5/S8 (from a P-GW to an S-GW, with the S-GW as a consumer)
- Sm, Sn (no overload scenario identified, limited GTP-C traffic, avoid impacts to the MBMS GW)
- Sv (no overload scenario identified, avoid impacts to legacy CS products)
- S101, S121 (no overload scenario identified, avoid impacts to legacy high rate packet

- data (HRPD) products
- Gn/Gp (avoid impacts to legacy Gn-SGSN/GGSN products and GTPv1-C protocol)

18.1.9 SCTP chunk throttling (Feature f12108-01)

SCTP chunk throttling feature prevents CPU overload resulting from SCTP control chunk flooding.

This feature supports SCTP chunk throttling. The throttling is invoked when a flood of SCTP packet is received on an interface. When the rate for a chunk type exceeds the defined threshold, the remaining chunks received within an interval are dropped and counters are pegged.

SCTP chunk throttling feature prevents CPU overload resulting from SCTP control chunk flooding by rate limiting the following ingress SCTP chunk types:

- INIT
- INIT ACK
- HEARTBEAT
- HEARTBEAT ACK
- ABORT
- SHUTDOWN
- SHUTDOWN ACK
- ERROR
- COOKIE ECHO
- COOKIE ACK
- ECNE
- CWR
- SHUTDOWN COMPLETE
- ASCONF
- UNKNOWN

This feature supports rate limiting as follows:

- The rate limit interval is 1 second.
- For each rate limited chunk type/group, a threshold is defined.
- For each rate limited chunk type/group, the number of chunks up to the threshold are forwarded for SCTP protocol processing.
- For each rate limited chunk type/group, if the threshold is crossed all remaining chunks within the rate limit period are dropped.

- Chunk/group specific MPH misc count is pegged for each dropped packet.
- Chunk/group specific PM count is pegged for each dropped packet.
- Alarm is generated.
- Alarm is cleared when the incoming rate for the chunk type is below threshold for 1 minute.

The mapping of SCTP chunk types to threshold is shown in the following table:

Table 75: Mapping of SCTP chunk types to threshold

SCTP Chunk Type	SCTP Chunk Value	Threshold	Throttle
DATA	0		No
INIT	1	INIT	Yes
INIT ACK	2	CONTROL GROUP	Yes
SACK	3		No
HEARTBEAT	4	HEARTBEAT	Yes
HEARTBEAT ACK	5	HEARTBEAT ACK	Yes
ABORT (T=0)	6	ABORT	Yes
ABORT (T=1)	6	ABORT	Yes
SHUTDOWN	7	CONTROL GROUP	Yes
SHUTDOWN ACK	8	CONTROL GROUP	Yes
ERROR	9	CONTROL GROUP	Yes
COOKIE ECHO	10	COOKIE ECHO	Yes
COOKIE ACK	11	CONTROL GROUP	Yes
ECNE	12	CONTROL GROUP	Yes
CWR	13	CONTROL GROUP	Yes
SHUTDOWN COMPLETE	14	CONTROL GROUP	Yes
ASCONF	193	CONTROL GROUP	Yes

SCTP Chunk Type	SCTP Chunk Value	Threshold	Throttle
UNKNOWN	15-63 64-127 128-191 192 194-255	UNKNOWN	Yes

Lowering a MME heartbeat interval may require raising the SCTP Heartbeat Acknowledge message threshold via gParms.

Lowering a remote (eNB S1MME) heartbeat interval may require raising the SCTP Heartbeat threshold via gParms.

18.1.10 Age out of S10 links based on actual usage (Feature f12118-02)

With this feature, unnecessary S10 links without traffic can be deleted.

MME uses `transactionOrientedLinkMoDeletionTimer` to delete S10 links that continue to heartbeat but have not carried any traffic for the specified time.

The S10 links can always be re-established as needed.

This functionality is identical to what is currently provided for Gn and S3 (SGSN links).

18.1.11 Paging overload control enhancements (Feature f10225-01)

This feature enhances paging overload by preventing excessive MME paging activity from driving the MME into critical overload.

The existing MME overload control (OLC) mechanism triggers restricted paging when CPU or memory consumption overload conditions are detected on the IPDS or the CPPS. Whenever restricted paging is activated by the OLC mechanism, the number of page attempts is limited to just one and MME paging is limited to use a paging method, such as `LastSeenENB`. For example, the MME only sends the Paging message to a single eNB for a page attempt.

This feature provides additional protection against overloads by addressing the following issues:

- Highly aggressive paging policy provisioning

Description: When the MME is configured to use aggressive paging methods, such as `LastSeenTAI`, for lower priority paging types, such as Basic, the resulting MME paging message traffic consumes a significantly larger slice of the MME's overall message capacity and may result in an overload condition.

Solution: If aggressive paging methods are used for lower priority paging types, the MME selects a less aggressive paging method, such as `LastSeenENB`, when protection from overload is needed. Protective action is taken when the following conditions are met:

- The MME is performing the first page attempt for a paging operation for a UE using one of the following paging types: Basic, CoverageEnhancement, PGWRestart, SxnRestoration, UeMonitLocationPaging, or UELB_PAGING.
- An aggressive paging method, such as `LastSeenTAI` or `LastSeenTAINBTAI`, was provisioned for the first page attempt in the `pagingPolicy` database of the current paging type.
- The MME paging fanout ratio, such as average number of eNBs paged per attempt, reaches a level that is considered excessive, such as average of 40 eNBs paged per page attempt.
- The measured MME paging message rate reaches 50% of the overall message capacity.
- The global parameter `pagingOverloadPrevention` is set to `Yes` (default value).

 **Note:**

This MME paging method selection override is reported via new PM counts and a new PCMD field.

- S1AP paging message queue backlog

Description: Large spikes in the paging message traffic can result in a large backlog of messages in the paging message queue on the IPDS. Such backlogs delay the transmission of paging messages by the MME and can cause major issues for overall MME paging support. This problem can also lead to the MME escalating to use of additional page attempts to reach a UE, which further increases the level of paging message traffic.

Solution:

- If the MME detects that the paging message queue depth has reached a level that takes two seconds or more to process, the MME restricts paging to only the Last Seen eNB even when the paging of multiple eNBs for a UE is present in the paging message queue. This action is taken to eliminate the backlog of messages in the paging message queue. Restricted paging is also activated for new page attempts
- If the MME detects that the paging message queue depth has reached a level that takes over six seconds to process, the paging message queue is cleared. This action is

only taken if the previous action was unable to reduce the paging message queue depth sufficiently.

18.1.12 MME support for APN level overload control (Feature f10701-01)

With this feature, the MME supports APN specific overload control and the overload is reported from the P-GW side.

The MME supports two options:

- The P-GW rejects a session creation with "APN congestion" and includes a back-off time during which the same P-GW is not selected for PDN connection establishments for this APN.
- The P-GW includes overload control information related to up to 10 specific APNs. If the MME receives overload control information related to specific APNs, the MME applies the overload control handling by considering the reported APNs together with the reported overload reporting metric and the period of validity related to the APNs. The MME may receive either the node level overload only, or the overload related to specific APNs only, or both.

18.2 Session restoration

The MME has implemented 3GPP node restoration functions, that is, the MME restoration, S-GW restoration, proxy call session control function (P-CSCF) restoration, and P-GW restart, according to standards.

Until a geo-redundant direct broadcast satellite (DBS) solution is available, the MME takes advantage of the session restoration server (SRS), a legacy remote UE context database solution from 9471 Wireless Mobility Manager, which, while it is not virtualized, provides an interim geo-redundancy option. The function and background of SRS is described in the *Session restoration server (SRS)* feature.

18.2.1 Evolved ARP and PDP context for dual stack (Feature m30108-01)

The *Evolved ARP and PDP context for dual stack* feature adds support for Dual Stack

packet data protocol (PDP) context and Evolved Allocation/Retention Priority. It provides better inter radio access technology (IRAT) handover success, avoiding the need for separate packet data networks (PDNs) for the two IP version types.

This feature supports handling of incomplete implementation of dual stack support in 3GPP TS 29.060, in which in a mobility use case there is no means of transferring the dual stack address between the old and the new network element in the PDP Context information element (IE). With this feature, the support for the PDP Context IE is amended to support the IPv4v6 dual stack end user address in mobility procedures.

Additionally, this feature supports optional IE Evolved Allocation/Retention Priority II functionality, which is to convey evolved allocation and retention priority (E-ARP) between SGSNs. The MME needs to support E-ARP so that GTPv1 is aligned with ARP in GTPv2, which, if not supported, causes ARP mapping misalignment.

This feature does not require SRS.

18.2.2 UE notification on specific PDN disconnection while the UE is in the idle state (Feature m10139-01)

The UE notification on specific PDN disconnection while the UE is in the idle state feature helps to avoid unnecessary network detach and to maintain other services of the UE while enabling reconnection for a single service.

This feature introduces support for the new Reactivation requested cause code by the MME. If the UE is in ECM-IDLE and the last packet data network (PDN) connection is not being deleted and the Delete Bearer Request received from the S-GW contains the Reactivation requested cause that was sent by the P-GW, the MME immediately informs the UE in both ECM-CONNECTED and ECM-IDLE states about the bearer deactivation, maps the S11 cause into a non-access stratum (NAS) cause value, and sends the NAS cause to the UE (especially required from Rel 10 onwards where cause values #8 Reactivation requested and #9 PDN reconnection to this access point name (APN) disallowed have been introduced). This results in the UE re-establishing the evolved packet system (EPS) bearer or PDN connection or both which the UE considers as necessary to re-establish.

With this feature, the MME enhances support when the Reactivation requested cause code is received in the Delete Bearer Request for the following scenarios:

- The UE is ECM-IDLE and the last PDN connection is not being deleted.
- The UE is ECM-CONNECTED and the last PDN connection is not being deleted.

In both cases, the MME informs the UE about the bearer deactivation, which allows the cause

value from the S-GW/P-GW to be transferred to the UE.

For the UE that is ECM-IDLE, when the MME receives a P-GW-initiated Bearer Deactivation with cause #8 Reactivation requested, and the last PDN connection is not being deleted, the MME initiates paging to inform UE of the Bearer Deactivation Request.

Upon becoming ECM-CONNECTED, following paging, the MME proceeds with the Bearer Deactivation Request. The S11 cause value #8 is mapped into NAS cause #39 Reactivation requested.

 **Note:**

Informing the UE of the PDN connection disconnect allows the UE to re-establish the EPS bearer/PDN connection upon becoming ECMCONNECTED following the paging. Paging is initiated through network triggered service request procedure in 3GPP TS 23.401 clause 5.3.4.3, from step 3a onwards.

For the UE that is in ECM-CONNECTED state, when the MME receives a P-GW-initiated Bearer Deactivation with cause #8 Reactivation requested, and the last PDN connection is not being deleted, the MME proceeds with the Bearer Deactivation Request. The S11 cause value #8 is mapped into NAS cause #39 Reactivation requested.

 **Note:**

Informing the UE of the PDN connection disconnect allows the UE to re-establish this EPS bearer/PDN connection. The MME partially complied with CR2477 before this feature. Only this ECM-CONNECTED case was supported.

CR2477 for 3GPP TS 23.401 includes two cases: P-GW-initiated Bearer Deactivation and UE/MME-initiated PDN disconnect. The UE/MME-initiated case includes updates that involve the MME detection and action upon PDN connections involving SIPTO. CMM does not yet support SIPTO. This part of CR2477 is not supported.

This feature does not require a session restoration server (SRS).

18.2.3 Enhanced S-GW restoration procedure (Feature m10538-08)

The **Enhanced S-GW restoration procedure** feature supports recovery of UE sessions when an S-GW fails or restarts without resorting to IMSI attach. All UE services are maintained even in case of S-GW failure.

With this feature, upon the detection of a S11 path loss or S-GW restart, the MME does not detach UEs associated with the failed S-GW. The MME retains the UE context and starts releasing the S1 connections of the connected UEs and starts allocating a new S-GW as soon as they become idle.

The MME starts S1 release of UEs in ECM-CONNECTED mode and as soon the S1 is released, a UE is assigned a new S-GW using the S-NAPTR procedure. The MME releases S1 of UEs in connected mode in the following order:

- UEs with emergency session in ECM-CONNECTED state
- UEs with emergency session in ECM-IDLE state
- UE in ECM-CONNECTED state with QCI=1 bearers
- UE in ECM-CONNECTED state with other GBR bearers
- UE in ECM-CONNECTED state without GBR bearers

The prioritized recovery of the UE in ECM-IDLE state is based on the provisioned list of APN and subscribed Restoration-Priority per APN. Home subscribers are always restored before roammers.

The prioritization is used for the following reasons:

- To allow all affected UEs to be reconnected to the network in a relatively short time, which is function of the speed of the S-GW relocations that the MME performs, based on implementation and the network load, so that downlink packets may be delivered to the UEs with minimum service interruption.
- Prioritizing the restoration of emergency PDN connections can enable the preservation of emergency calls in progress for authenticated and unauthenticated users, and can also enable PSAP to call back authenticated users with an emergency registration, but without an emergency call in progress.
- The restoration priority can, for example, allow to restore with a higher priority users with an IMS voice subscription over IMS users without an IMS voice subscription.

During this time, it is possible that an eNB may initiate S1 release of an ECM-CONNECTED UE. In this case, the MME proceeds with the request and as soon as the S1 connection is released, the UE is assigned a new S-GW. The MME scans through the entire UE context database and starts S-GW relocations once the restoration timer is expired. The newly selected S-GW may be the original S-GW if the restart has been completed. The MME handles any UE mobility management requests, that is, TAU or service request, as they arrive and, if the UE is associated with the failed or restarted S-GW, the MME first assigns a new S-GW to the UE and then proceeds with the procedure. This capability to re-locate UE to a new or restarted S-GW is already supported for TAU and this feature extends this capability to service requests irrespective of activation of the feature or not.

In the case of TAU that involves the MME or SGSN relocation, the MME indicates that the SGW change is required in the S10/S3 Context Response message. The new MME may try the old S-GW if it has not detected the S-GW failure. If the old S-GW does not respond, the new MME selects a new S-GW.

The MME's prioritization of ECM-IDLE UE recovery based on provisioned APN priority and the subscribed restoration priority is supported and it can be provisioned on a per-PLMN basis. The MME supports provisioning in order to support the prioritization of idle non-emergency UE recovery.

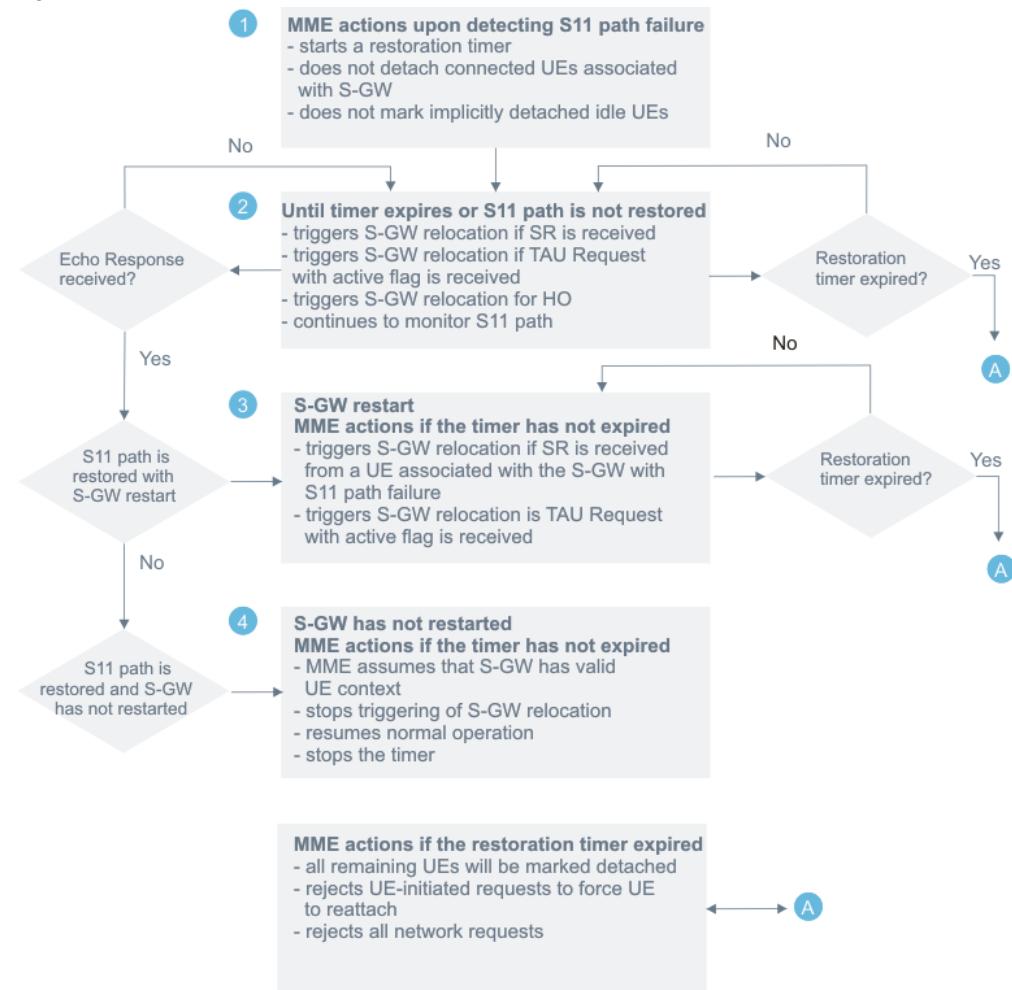
- APN-NI: APN Network Identifier as defined in 3GPP TS 23.007, clause 9.1.
- APN Priority: The MME uses the APN priority to prioritize the UE recovery based on the APN priority. The priority value ranges from 1 to 8. Priority level 1 has the highest priority and value 8 has the lowest priority. Any APN that is not in the list is assigned the lowest priority 8. This priority is used for a given subscriber if the subscriber has a PDN connection to an APN in the priority list at the time of failure.

Recovery consists of selecting an S-GW using the S-NAPTR procedure and recreating PDN sessions on the selected S-GW. All the PDN connections of the UEs are created on the selected S-GW. The selected S-GW may be a new S-GW or the old S-GW if it has been restarted. The subscribed restoration priority per APN received from the HSS is used to determine the relative restoration priority among PDN connections to the same APN.

The MME computes a normalized priority of a UE based on the provisioned APN priority and the subscribed APN restoration priority when the MME sets up a PDN connection. Once the normalized priority is computed, it is only recomputed whenever the MME handles any UE or network-initiated session management requests. So, any provisioning changes become effective only on a subsequent session management procedure. However, any updates to the APN restoration priority AVP for a UE take effect immediately.

The MME supports the enhanced restoration procedure when the `enhancedSgwRestorationProcedures` global parameter is enabled. The MME's actions for the UEs associated with the failed S11 path is shown in the figure.

Figure 160: MME's actions for UEs associated with a failed S11 path



A similar call flow is used for TAU Request messages used to relocate UEs to a new S-GW.

The following S-GW relocation scenarios are supported:

- The MME detects an S-GW failure, releases the S1 connection, and assigns UEs to a new S-GW.
- The eNB detects an S-GW failure and sends a request to release S1 connection before the MME.
- The MME receives a Service Request before a UE is relocated to a new S-GW.
- The MME receives a DDN before a UE is re-located to a new S-GW.
- The MME receives a TAU Request (with and without active flag) before a UE is relocated to a new S-GW.
- A TAU Request with the MME relocation
- S1 or X2 handover
- S1 handover with the MME relocation

The *Enhanced S-GW restoration procedure* feature does not require session restoration

server.

Related descriptions

- [Restricting S-GW relocation \(Feature f10166-01\)](#)

18.2.4 P-GW restart - S11 (Feature m10538-02)

The P-GW restart - S11 feature supports recovery of UE sessions proactively when a P-GW fails or restarts.

This feature supports MME capabilities to support S11 P-GW Restart Notification message and appropriate actions on impacted UEs, as specified in 3GPP TS 23.007. If the feature is supported by both the MME and S-GW, a P-GW Restart message is sent by an S-GW when it detects that the peer P-GW has failed and restarted. The MME supports the following capabilities:

- Provisioning on the MME to enable or disable the feature and enabling of paging idle UEs to restore sessions associated with a restarted P-GW.
- If the feature is enabled, the MME sends support of P-GW Restart Notification indication in Node Feature IE of GTPv2 Echo Request and Echo Response. If the feature is not enabled, the MME does not indicate the support of P-GW Restart Notification to the S-GW.

When an S-GW detects that a peer P-GW has restarted, the S-GW deletes all PDN connections associated with the P-GW and sends S11 P-GW Restart Notification message to the MME. Additionally, the S-GW may also send the message when the S-GW detects that the peer P-GW has failed and not restarted.

When the MME receives the P-GW Restart Notification with P-GW restarted or not, the MME deletes all the PDN connections associated with the S-GW and the restarted P-GW and the MME restores a PDN connection associated with the S-GW and restarted P-GW as follows. It is expected that the S-GW does not send another P-GW Restart Notification when P-GW is restarted if the S-GW has already sent a P-GW Restart Notification indicating that the P-GW has not restarted.

There are two actions taken by the MME: it responds with S11 P-GW Restart Notification Acknowledge to the S-GW and deletes all the PDN connections associated with the P-GW.

If a UE is connected, the MME sends for each UE S1-AP E-RAB Release Command with NAS message Deactivate EPS Bearer Context Request with ESM cause value #39 Reactivation requested if the UE has other bearers associated with other P-GWs. If the Deactivate EPS

Bearer Context Request includes ESM cause #39 Reactivation requested and the EPS bearer context is a default EPS bearer context, the UE sends PDN connectivity procedure to re-establish the PDN connection. If the deleted PDN connection is the last PDN connection, the MME detaches the UE using the detach profile introduced by earlier detach profile features. This feature introduces a new reason, a P-GW restart notification.

If a UE is in ECM-IDLE state and paging is enabled for PDN connection restoration, the MME pages the UE. When the UE responds with Service Request, the MME excludes the bearers of the PDN connections in the S1-AP Initial UE Context Setup. This triggers the UE to delete all the bearers that were not activated and send the PDN Connection Request message to reestablish the PDN connection. If the PDN connection deleted is the last PDN connection, the MME rejects the UE with cause value #10 Implicitly detached to force UE to re-attach. Again, the MME uses the detach profile in determining cause code to be sent and so on, except for the UE notification (paging). This feature's paging provisioning overrides the detach profile for the P-GW restart notification reason.

If there are multiple PDN connections (APNs) associated with a restarted P-GW or if there are multiple P-GW restarts, the MME prioritizes restoration of sessions in the following order by identifying UEs that have PDN connections on the restarted P-GWs:

1. Restore sessions for a UE in connected state for any mobility management procedure (like handover) and any procedure involving the restarted/failed P-GW as they occur as long as the MME is not in overload.
2. Explicitly or implicitly notify the UE in idle state that certain PDN connections have been deactivated when the UE initiates a mobility management procedure, such service request and TAU.
3. The UE in connected state with emergency PDN connection.
4. The UE in idle state with an emergency PDN connection.
5. The UE in connected state with GBR bearers.
6. The UE in connected state with non-GBR bearers.
7. Prioritize recovery of the UE in ECM-IDLE state based on the provisioned list of APN and subscribed Restoration-Priority per APN. Home subscribers are always restored before roamers.

The MME's actions to re-establish PDN connections are done in a provisioned period of time. Once the timer is expired, the MME stops the recovery of the PDN connections and deletes locally PDN connections of the left over UEs.

MME supports provisioning as follows:

- Enable/disable the feature globally; that is, the MME home network and all shared networks.
- Enable paging idle UEs so that the UE is notified that the PDN connection is deactivated.

This provisioning is done per MME.

- The UE with a provisioned APN-NI list, such as emergency APN, IMS, and Internet, and priority which indicates the preferential order of restoring the session. A maximum of 16 APNs can be provisioned. If an APN-NI list is not provisioned, then no attempt is made to re-establish any PDN connections associated with a P-GW restart.
- A timer for the maximum duration in which the MME would attempt to re-establish PDN connections. The MME starts the timer when it starts the reestablishment procedure. Once the timer expires, the MME stops the reestablishment attempts and deletes PDN connections associated with the PGW restart of the left over UEs.

The following default values are used:

- Notify ECM-IDLE UE: Default value is No. This feature's paging notification provisioning overrides this provisioning.
- Detach Type to be sent: Default value is Re-attach required
- EMM Cause to be included: Default value is Yes
- EMM cause code: #10 Implicit detach

The *P-GW restart - S11* feature requires the S-GW support. This feature does not require session restoration server.

18.2.5 P-CSCF recovery

MME supports three options for P-CSCF recovery. These features provide proactive recovery from a failed P-CSCF, resulting in better UE access to the VoLTE service. These features do not require Session Restoration Server (SRS).

As part of Supported-Features AVP, in the Update Location Request (ULR) message to the HSS, the MME indicates if it supports Proxy Call Session Control Function (P-CSCF) Restoration (only if P-CSCF recovery mode 2 or 3 is enabled).

If P-CSCF recovery is supported, it occurs as follows:

1. MME sends a Update Location Request (ULR) message to the HSS with a Supported-Features AVP via Feature-List-ID 2 and bit 16 in Feature-List if P-CSCF Recovery mode 2 or 3 is enabled.
2. If P-CSCF fails after a UE registered with IMS APN, when S-CSCF detects IMS connection failure based on timeout, S-CSCF will send a message to HSS about the P-CSCF failure.
3. The HSS initiates an IDR to the MME about the P-CSCF failure.
4. An IMS APN is identified by QCI 5 if IMS APN table is not defined or QCI 5 and IMS APN is defined and corresponding entry matched.

The global parameter `pcscfRecovery` specifies the mode of P-CSCF recovery. The P-CSCF recover modes are as follows:

Table 76: P-CSCF recovery modes

Recovery mode	Description
none (default)	No P-CSCF recovery. The MME ignores the bit in IDR-Flags AVP for P-CSCF recovery and the MME continues with the procedure.
mode 1	The HSS supports a proprietary P-CSCF recovery capability in which the HSS uses bit 31 in IDR-Flags to indicate P-CSCF recovery. The MME honors the request if the UE is in IDLE or CONNECTED mode. The MME informs the S-GW by sending a proprietary IE in Modify Bearer Request (Feature m11331-01)
mode 2	The HSS uses bit 8 in the IDR-Flags AVP for P-CSCF F recovery. The MME will honor the request whether the UE is in IDLE or CONNECTED mode. If the UE is idle, the MME pages the UE. Once the UE is in connected state, the MME will request the UE to deactivate and reactivate the IMS PDN connection. (Feature m11002-01)
mode 3	Indicates support for 3GPP-specified protocol configuration options (PCO). When P-CSCF has failed in IMS core network and the user is in IDLE or CONNECTED mode after IMS Registration, when notified by S-CSCF, the HSS initiates an IDR message to MME by sending the P-CSCF Restoration Request bit (Bit 8) set in IDR-Flags AVP. The MME sends the Modify Bearer Request to the P-GW (via the S-GW) for this associated PDN connection with a P-CSCF Restoration indication. Upon receipt of the P-CSCF Restoration indication by the P-GW, it checks whether the UE has indicated it that supports the Update bearer context at P-CSCF failure mechanism. If it is supported, the P-GW sends the Update Bearer Request to the MME with the list of available P-CSCF addresses within the PCO IE to update the destination UE (per the Update bearer context at P-CSCF failure mechanism). If it is not supported, the P-GW releases the IMS PDN connection by sending a Delete Bearer Request to the MME with cause code Reactivation requested. If this is the last PDN connection, the MME initiates a detach procedure based on the provisioned detach behavior profile. The detach behavior profile include parameters that specify the cause code to send, whether reattachment is required, whether the idle UE is paged, and whether a cause code is sent. (Feature m11331-03)

18.2.5.1 P-CSCF recovery - Option 1 (Feature m11331-01)

The **P-CSCF recovery – Option 1 feature** deals with a scenario where P-CSCF has failed when the user is in idle mode after IMS registration and, as a result, S-CSCF detects a failure based on timeout and initiates P-CSCF failure to the HSS.

The HSS initiates insert the subscriber data (IDR) procedure to the MME by sending a Rel 12-introduced AVP to the MME. As a result, the MME initiates the Modify Bearer Request with Private Extension IE set to P-CSCF Restoration required to the S-GW.

The Insert Subscriber Data (IDR) message sent from the HSS to the MME is a proprietary IDR based on a customer request. (Bit 31 in IDR Flags AVP is used for P-CSCF recovery.)

Usage of Indication Flags IE to notify the S-GW is replaced with the customer-requested specific Private Extension IE with P-CSCF Recovery data inside.

This feature is applicable for the Update Location Request/Answer (ULR/ULA) and Insert Subscriber Data/Answer (IDR/IDA) command pairs over S6a. The MME indicates in ULR message, as part of Supported-Features AVP, if it supports P-CSCF restoration which is used by the MME to notify the HSS that it is capable of receiving indication for the P-CSCF restoration.

If the MME does not support this feature, the HSS does not send the related information to the MME within IDR. If the HSS does not support this feature, the feature bit is ignored.

The HSS support is required for proprietary S6a functionality.

18.2.5.2 P-CSCF recovery - Option 2 (Feature m11002-01)

The **P-CSCF recovery – Option 2 feature** supports a version of P-CSCF recovery supported in 3GPP standards that addresses UEs in ECM-IDLE and ECM-CONNECTED mode in addition to the 3GPP option that addresses only UEs in the ECM-IDLE state introduced in the **P-CSCF recovery – option 1 feature**.

This feature deals with a scenario where P-CSCF has failed when the user is in an idle/connected mode after IMS registration and S-CSCF detects P-CSCF failure when trying to establish a terminating session based on timeout and notifies the HSS of a P-CSCF failure. The HSS, in turn, initiates an IDR procedure to the MME by sending Rel 12-introduced AVP to the MME. (Bit 8 in IDR Flags AVP.) Upon receiving IDR with Bit 8 in IDR Flags AVP, the MME detaches the IMS PDN.

For UEs in ECM-IDLE state, the MME pages the UE. Paging the UE if user is in IDLE state and releasing the identified PDN connection by executing explicit detach is controlled or based

on the existing MME provisioning parameter.

For UEs in the ECM-CONNECTED state, or when UEs in the ECM-IDLE state respond to the page, the MME releases the PDN connection towards the UE by executing PDN disconnection or detach procedure with NAS cause code Reactivation requested.

The MME also releases the same PDN connection towards the S-GW/P-GW by sending Delete Session Request message.

This feature is applicable for the Update Location Request/Answer (ULR/ULA) and Insert Subscriber Data/Answer (IDR/IDA) command pairs over S6a.

The MME indicates in ULR, as part of Supported-Features AVP, if it supports P-CSCF restoration which is used by the MME to notify the HSS that it is capable of receiving indication for P-CSCF restoration.

If the MME does not support this feature, the HSS does not send the related information to the MME within IDR.

If the HSS does not support this feature, the feature bit is ignored by the MME. The HSS identifies whether the MME supports HSS-based P-CSCF restoration based on feature support information provided by the MME.

As part of this feature, the MME supports Supported-Features AVP with:

- Vendor-ID AVP = 3GPP
- Feature-List-ID = 2
- Feature-Bit = 16

If the IDR is sent only for the purpose of requesting the execution of the HSS-based P-CSCF restoration procedures, the Subscription-Data AVP included is empty.

The MME determines if an APN is IMS-related by looking for QCI=5.

- If IMS-alias is provisioned and if QCI =5, it is considered to be IMS APN.
- If IMS-alias is not provisioned but QCI matches value 5, it is considered to be IMS APN.
- If APN NI contains ims (case insensitive) substring, it is considered to be IMS APN as well. The vendor is allowed to override ims alias with their own alias through the MME provisioning.

The MME executes the procedures for the HSS-based P-CSCF restoration, as described in 3GPP TS 23.380, sub-clause 5.4.

The *P-CSCF recovery – Option 2* feature requires HSS support. The S-GW/P-GW support is also required depending on the option.

18.2.5.3 P-CSCF recovery - Option 3 (Feature m11331-03)

The *P-CSCF recovery – Option 3* feature supports 3GPP Rel 12-specified protocol configuration options (PCO)-based P-CSCF restoration scenario. PCO-based P-CSCF restoration deals with a scenario whereby P-CSCF has failed in IMS core network when the user is in idle/connected mode after the IMS registration.

The HSS is notified by the S-CSCF and, as a result, the HSS initiates an IDR message to the MME by sending P-CSCF Restoration Request bit (Bit 8) set in IDR-Flags AVP. The S-CSCF in the IMS core may detect a P-CSCF failure when trying to establish a terminating session.

The MME sends accordingly a Modify Bearer Request to the P-GW for this associated PDN connection with a P-CSCF restoration indication.

The MME provides this indication to the P-GW via the S-GW. Upon reception of the P-CSCF restoration indication by the P-GW, it checks whether the UE has indicated that it supports update bearer context at P-CSCF failure mechanism.

- If it is supported, the P-GW sends Update Bearer Request to the MME with the list of available P-CSCF addresses within PCO IE to update destination UE, as per update bearer context at P-CSCF failure mechanism.
- If it is not supported, the P-GW releases the IMS PDN connection by sending a Delete Bearer Request to the MME with cause code Reactivation requested.

If this is the last PDN connection, the MME initiates a detach procedure based on the provisioned profile.

With this feature, VoLTE PDN reactivation can be avoided.

The *P-CSCF recovery – Option 3* feature requires UE, HSS, S-GW, and P-GW support.

18.2.6 PDN connection re-establishment after S-GW change (Feature f10103-01)

The *PDN connection re-establishment after S-GW change feature helps keep the shortest data delivery path and reduce S5 interface traffic by keeping S-GW and P-GW together whenever possible.*

During mobility procedures, like tracking area update or handover, the S-GW might be relocated based on the value of the new tracking area identity (TAI). The P-GW of ongoing PDN connection is never changed. This means that after the mobility procedure, the new S-

GW may be farther from the P-GW.

This feature allows configuring the MME to disconnect and re-establish the PDN connection in order to get the S-GW and P-GW closer. The existing PDN connections are disconnected by using procedures that avoid disturbing the traffic.

The purpose of this functionality is to keep the shortest data delivery path and to reduce S5 interface traffic by keeping the S-GW and P-GW together whenever possible.

The operator is able to configure two APN lists; one for voice traffic and one for data traffic. The operator is also able to configure how close to each other the P-GW and the S-GW are to trigger the PDN re-establishment procedure.

After the mobility procedure with the S-GW relocation is completed, the MME checks whether the APN of an active PDN connection is found in either of the two lists.

- If the APN is found in the voice APN list and if the P-GW and the S-GW are not close enough, the MME performs PDN re-establishment if the QCI=1 bearer is not active. If the QCI=1 bearer is active, the PDN re-establishment is performed immediately when the QCI=1 bearer is released. In both cases, the re-established is only started once the UE is moved to ECM-IDLE state. This is to prevent disruption to other traffic.
- If the APN is found in the data APN list and if the P-GW and the S-GW are not close enough, the MME starts a configurable timer when the UE is moved to ECM-IDLE state. If the UE goes to connected state when the timer is running, the timer stops and starts again when the UE goes again to idle state. When the timer expires, the MME performs PDN re-establishment.

PDN connection re-establishment based on the data APN list applies to home subscribers only.

This feature does not require session restoration server (SRS).

Related descriptions

- [PDN connection re-establishment after S-GW change with roammers and voice \(Feature f10103-02\)](#)
- [PDN connection re-establishment after S-GW change with roammers and voice enhancements \(Feature f10103-03\)](#)

18.2.7 PDN connection re-establishment after S-GW change with roammers and voice (Feature f10103-02)

PDN connection re-establishment based on the voice APN list applies to the roaming

subscribers if local breakout (LBO) has been enabled.

Related descriptions

- [PDN connection re-establishment after S-GW change \(Feature f10103-01\)](#)

18.2.8 PDN connection re-establishment after S-GW change with roammers and voice enhancements (Feature f10103-03)

The MME enhances PDN connection re-establishment after S-GW change by re-establishing IMS PDN connection immediately when QCI=1 voice bearer is not active or QCI=1 bearer is released for UEs in both ECM-IDLE and ECM-CONNECTED states.

Related descriptions

- [PDN connection re-establishment after S-GW change \(Feature f10103-01\)](#)

18.2.9 Session restoration FNS compatibility (f10713-01)

This feature allows the CMM, which has several Flexi Network Server (FNS) MMEs in the network, to be deployed with the mobile data backup server (MDBS). The MDBS is used for UE restoration data. The MME stores IMSI and the last visited TAI on the backup server. This feature only supports S-GW initiated network triggered service restoration (NTSR).

This feature allows the CMM to use FNS mobile data backup server (MDBS) UE restoration data, for example, the SRS. However, the UE context stored on the MDBS is limited compared to the one stored on the SRS. The CMM stores IMSI and the last visited TAI on the backup server. This is a FNS compatibility feature.

The RS10 interface carries Sz messages using IPv4.

The feature does not support any of the SRS supported restoration upon

- service request
- TAU request
- MT CS or SMS paging

Only a single MDBS can be supported per MME.

Either one of MDBS or SRS is supported per MME, but not at the same time.

18.3 Session restoration server

Features supporting session restoration server (SRS).

18.3.1 Session restoration server (SRS) (Feature m10538-01)

S1-MME or S11 link failures, or an MME failure are recovered at alternate MMEs in the pool through the MME restoration. With the SRS, recovery can take place without escalation to international mobile subscriber identity (IMSI) attach, which can lead to signaling storms. Operators can ensure voice service availability for end users.

Before the implementation of this feature, an MME or S-GW failure resulted in subscribers not receiving IP multimedia subsystem (IMS) terminating calls until other procedures like tracking area update (TAU) or service request made the UE reattach to the network. This reattachment added extra signaling over radio network and resulted in attach storms. Hence, enhanced restoration procedures are introduced to provide service resilience. The service resilience is provided for the MME or S-GW failure with or without restart to achieve restoration procedures with minimal increase in signaling that prevents UE from reattaching to the network.

The enhanced restoration procedures for the MME failure require availability of necessary UE context data to restore UE sessions either by the same MME after its restart or by another MME in the same pool as the failed MME. This necessary UE context data (restoration data) can either be stored on a persistent memory on the same MME or on an external server. Major drawback of storing restoration data in the same MME is that other MMEs do not have access to the data if the MME is down. Therefore, this feature uses an external SRS to store necessary UE context data required to restore UE sessions without reattachment.

The external server is a standalone MME with no 3GPP interfaces. The restoration data of a UE stored on an SRS by the MME (restoration client) consists of

- security context (non-access stratum (NAS) protection algorithm, NAS ciphering algorithm, NAS uplink and downlink counts, KASME, cipher key (CK), integrity key (IK))
- bearer context (bearer IDs, access point name (APN), S-GW/P-GW F-TEIDs, quality of service (QoS) parameters, for example)
- paging area (last seen eNB and tracking area identity (TAI))
- critical subscription data, such as access restriction data and RFSP Index

A restarted MME or another MME can retrieve the data using an IMSI or an S-temporary mobile subscriber identity (S-TMSI) as UE identity to restore UE sessions without reattachment. The MME updates UE restoration data for events like attach, packet data network (PDN) connectivity request, detach and TAU with and without the MME or S-GW relocation. Additionally, the MME failure requires the S-GW and P-GW to maintain UE context for a configurable period of time and the S-GW to send a DDN message with IMSI when it receives downlink data from the P-GW to other MMEs in the MME pool of the failed MME.

The enhanced restoration procedures for an S-GW failure with or without an S-GW restart consist of the MME and P-GW maintaining UE context for a configurable period of time and reconnecting the UE to a new S-GW or to the old S-GW if it has restarted as opposed to current scheme of detaching the UE upon S11 path failure.

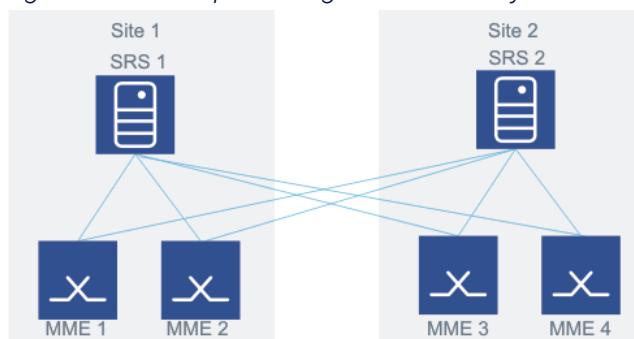
S-GW support is required for DDN with IMSI. Operators must also deploy an SRS node in the network.

18.3.2 MME support for SRS geo-redundancy (Feature m10538-10)

The *MME support for SRS geo-redundancy* feature provides added availability of the session restoration server (SRS) function so that even if a single site hosting the primary SRS node fails, session restoration is still possible. Operators can ensure voice service availability for end users.

This feature supports phase 1 of the SRS geo-redundancy in which two SRSs supporting an MME pool are deployed. The phase 1 architecture is shown in the figure and its main goal is to protect a site.

Figure 161: SRS phase 1 geo-redundancy architecture



The figure shows four MMEs of an MME pool that are deployed in two different sites for reliability. An SRS is deployed in each site. Each MME has an RS10 link to both the SRSs, but only one SRS can be configured as a primary SRS. An MME sends all its UE context updates to

its designated primary, but it retrieves the UE context from either SRS. MME1 and MME2 primary SRS is SRS2 and MME3 and MME4 primary SRS is SRS 1.

The architecture does not support synchronization of UE context across SRSs so that each SRS is a mirror image of the other. The following fault scenarios present how UE context is retrieved:

- Failure of an MME (for example, MME2)
 - Requests of UEs that are registered with MME2 are sent to other MMEs (MME1, MME2, and MME3) by the eNBs as they have lost the S1-MME interface to the MME2.
 - MME1, MME3, and MME4 retrieve the UE context from the SRS2 to restore UE sessions.
- Failure of an SRS (for example, SRS1)
 - MME3 and MME4 do not send any updates but they mark UEs that full update needs to be sent.
 - Once SRS1 is restored, MME3 and MME4 send full UE context updates to the restated MME.
- Failure of an SRS and MME, SRS and MME fail at the same site

Example: SRS1 and MME 1 failed. In this case, MME3 and MME4 are not able to send any updates to the SRS. However, MME2, MME3, and MME4 can retrieve context of UEs registered at MME1 from SRS2 that is the primary of the MME1.
- Failure of an SRS and MME, SRS and MME fail at different sites

Example: SRS1 and MME3 failed - In this case, MME1, MME2 and MME3 are not able to retrieve context of the UEs that were registered with MME3. This results in UEs to attach.

In this architecture, each SRS sends to MMEs that it is backing up the Echo Response message. This information is stored by each MME (basically this is MME code to its primary SRS mapping) so that the MME can send retrieve request to the right SRS. The MME determines where a UE is registered by using S-temporary mobile subscriber identity (S-TMSI) in case of service request, globally unique temporary identity (GUTI) in case of tracking area update (TAU) request, or globally unique MME identifier (GUMMEI) that is received in the Private Extension information element (IE) of the restoration DDN message (DDN with international mobile subscriber identity (IMSI)). The S-GW is enhanced to include the GUMMEI of the failed MME when it sends DDN message with IMSI to other MMEs in the pool.

New MME functionality

The MME always sends updates to the SRS provisioned as primary if two SRSs are provisioned.

If a single SRS is provisioned, the MME sends all the updates to the SRS and retrieves the UE

context from the SRS. If two SRSs are provisioned, then operators have to select an SRS as a primary SRS. If the primary SRS is down, no updates are sent to the other SRS. The other SRS is used only to retrieve the UE context.

The MME uses the MME GUMMEI received in the RS10 Echo Request message to build an MME to SRS mapping table. The MME uses this table to determine the SRS where UE context is stored for restoring UE sessions if UE is registered with another MME.

The MME obtains the MME code for a UE to retrieve context of a UE to be restored by using the following:

- S-TMSI for Service Request/Extended Service Request
- GUTI for TAU Request
- GUMMEI in Private Extension IE of DDN with IMSI for network-initiated recovery

If the MME does not receive GUMMEI in the Private Extension IE of the DDN message, the MME sends the S11 Downlink Data Notification Acknowledge message with cause Unable to page the UE. If the MME cannot retrieve the UE context, the MME rejects the UE request to force the UE to reattach.

S-GW support is required for DDN with IMSI. Operators also need to deploy an SRS node in the network.

18.3.3 Throttling ULR during UE restoration (Feature m10538-18)

Even though the use of session restoration server (SRS) avoids international mobile subscriber identity (IMSI) attach, because each UE session is restored on an alternate MME in the pool, there is still a surge of S6a traffic associated with Update Location Request (ULR) to inform the HSS of the new MME hosting the particular UE. The *Throttling ULR during UE restoration* feature throttles the ULR traffic to prevent S6a overload. With this feature, operators can ensure voice service availability for end users.

This feature enables the MME to throttle S6a ULR messages because of UE restoration to avoid an HSS/DRA overload. A UE restoration using SRS because of the MME restart or because of an eNB losing S1-MME link to the MME results in sending the ULR to the HSS to update location and also to obtain complete UE subscription data.

There is a possibility of these large numbers of ULRs causing overload conditions at the HSS/DRA.

To avoid the HSS/DRA overload, the MME monitors the rate of ULR because of the UE

restoration. If the rate of these ULRs exceeds a provisioned threshold, the MME delays the sending of the ULR. The delayed ULR is sent on a subsequent mobility management procedure if the rate of ULR because the restoration is below the threshold.

This feature can be enabled through provisioning, and ULR rate threshold can also be provisioned. The provisioning of the feature can only be done by a customer support team.

18.3.4 Service restoration enhancements (Feature m10538-22)

The Service restoration enhancements feature extends the scenarios where session restoration server (SRS) can be used to restore UE sessions. The feature provides enhanced session maintainability by storing more data in case of a previous MME failure. Operators can ensure voice service availability for end users.

This feature supports multiple UE restoration enhancements using the SRS:

- Support all bearers

Restoration data covers all packet data network (PDN) connections including the dedicated bearers.
- SGs-related information

This is used to restore UE SGs associations.
- Single radio voice call continuity (SRVCC) handover support

Adequate SRVCC information is stored on the SRS so that SRVCC handover can be supported for a restored UE.
- S102 interworking support

Adequate S102 information is stored so that S102 circuit-switched fallback (CSFB) and SRVCC handover for 1xRTT voice can be restored.

Support all bearers

Before the implementation of this feature, the MME restored only the default bearer from the provisioned restoration access point name (APN).

With this feature enabled:

- The MME sends all PDN connection information to the SRS.
- The MME sends both guaranteed bit rate (GBR) and non-GBR bearer information to the SRS.
- The MME includes GBR quality of service (QoS) parameters: QoS class indicator (QCI), allocation and retention priority (ARP), uplink/downlink maximum bit rate (MBR), and uplink/downlink GBR.

This change does not introduce new messages towards SRS or change the message structures.

SGs-related Information

The following information elements are added into RS10 protocol:

- SGs-Capabilities – SMS only Indication (Proprietary information element (IE))
 - 0 = SGs support is not limited to SMS (or UE has no SGs association)
 - 1 = SMS is only supported on the associated SGs
- SGs-State – State of the UE SGs association (Proprietary IE)
 - 0 = UE has no SGs association
 - 1 = Location Updated has been requested
 - 2 = UE has an SGs association

The new or restarted MME recovers SGs services as a part of the restoration service request (SR) procedure, if either SGs-State is not 0 or SGs-Capabilities indicates SMS-only.

The new or restarted MME recovers SGs services as a part of the restoration extended service request (ESR) procedure, if either SGs-State is not 0.

The new or restarted MME handles SGsAP-PAGING-REQUEST as shown if the CS restoration indicator bit of the Additional paging indicators IE is set.

Single radio voice call continuity (SRVCC) handover support

The MME and SRS support the following SRVCC parameters on the RS10 protocol:

- Mobile subscriber (MS) network capability

SRVCC bit SRVCC from UTRAN-HSPA/E-UTRAN to GERAN/UTRAN supported bit.
- Additional MM context for SRVCC

The IE consists of the Mobile Station Class Mark 2, Mobile Station Class Mark3, and supported codecs.
- Additional flags for SRVCC

The flag provides indication of whether UE supports IP multimedia subsystem (IMS)-centralized services or not.
- STN-SR

Session Transfer Number for SRVCC (see 3GPP TS 29.280 for the definition of the STNSR)
- C-MSISDN

Correlation mobile station international ISDN number (MSISDN)

S102 interworking support

The S102 infoware system (IWS) IP address information element on RS10 protocol is added to support recovery of S102 based 1xRT CSFB and SRVCC procedure:

In the update procedure, the MME updates the S102 IWS IP address to the SRS if the MME does:

- 1xRTT CS registration procedure
- S102 Redirection Command by the target MME because of the MME relocation
- S102 Redirection Command by the new or restarted MME because of the UE recovery

In the restoration procedure, the new or restarted MME sends S102 Redirection Command to the IWS obtained from the SRS as part of recovery service request, extended service request and TAU request procedures.

18.3.5 CMM support for resynch of SRS data (Feature f17008-14)

This feature allows an operator to trigger a primary restoration server synchronization or SRS resynchronization to recover the lost UE contexts in the primary database or SRS database after a CMM software upgrade.

Resynchronization enables a CMM to recover lost data after a software upgrade, so that the software upgrade can proceed in its SRS CMM buddy and the CMM for which it is a buddy.

This feature supports the following CNF in-service software upgrade (ISSU) scenarios:

- For a 5G and full-context 4G SRS, this feature supports pushing the SRS data from the buddy CMM to the CMM under software upgrade when the DBS instances are available. Data for the UEs that are active will already be pulled, but for inactive UEs, data must be pushed. Software upgrade should not be started on the buddy CMM that is being resynchronized until resynchronization completes.
- For a 5G and full-context 4G SRS, when a CMM (for example, CMM A) completes the ISSU, its buddy CMM (CMM B) must push the data for all of the UEs on CMM B to CMM A. Software upgrade should not be initiated on CMM B until after the resynchronization completes.

This feature supports the following VNF and CNF out-of-service software upgrade (OSSU) scenarios:

- For 5G, pushing the SRS data from the buddy CMM to the CMM under software upgrade

when the DBS instances are available. Data for the active UEs are pulled, but for inactive UEs, the data will need to be pushed. Software upgrade must not be started on the buddy CMM that is being resynchronized until the resynchronization completes.

- For 5G and full-context 4G SRS, when a CMM (CMM A) completes the OSSU, the buddy CMM (CMM B) must push the data for all of the UEs on CMM B to CMM A. Software upgrade should not be initiated on the buddy CMM until after the resynchronization completes.

18.3.6 MME support for enhanced backup of 4G UE context to the SRS for ISSU (Feature f17008-07)

If configured, an MME can back up and restore complete 4G UE contexts to and from its pre-configured SRS buddy in the MME pool.

This feature is applicable only to CNF deployments that are configured for in-service software upgrade (ISSU). Restoration is supported for all MME procedures, except for 4G IMSI Attach from the CNF's SRS buddy during and post ISSU.

When this feature is enabled, an MME (for example, MME-A) to which a 4G UE is attached sends an Update Request message to its buddy MME (for example, MME-B) to back up the UE's full context. The back up is performed so that if MME-A loses the UE's context due to ISSU rolling updates, the context can be restored from its buddy and the UE can be served without interruption. MME-B updates, restores, or deletes the UE's context over the NR10 interfaces (the same proprietary NR10 interface used by an AMF SRS). The MME monitors the NR10 interface by sending heartbeat messages to other MMEs in the pool.

This feature is controlled by the `supportFullUERestoration` global parameter.

- Update Request message

When a UE's context changes because of a procedure completion, the MME replicates the UE context by sending an Update Request message to its buddy SRS. If the UE's context is stored successfully in the buddy MME, the buddy MME sends the following success response:

```
HTTP status code 200_OK
```

- Restoration Request message

During an ISSU, UE context data can be lost during the CPPS and DBS rolling upgrades. When the serving MME receives signaling activity for a known UE, but the context cannot be found in the local cache or database, the MME seamlessly triggers context restoration

from its buddy MME and the incoming procedure continues without interruption.

- If the restoration request is successful, the buddy MME sends the UE context with the following status:

```
HTTP status code 200_OK
```

- If the context is not found, the buddy MME responds with the following status:

```
HTTP status code 404_NOT_FOUND
```

The serving MME requires the UE to re-attach or appropriate error handling is performed.

Since the UE is known to the MME, restoration is always performed with an IMSI or an IMEI, even if the incoming signaling is initiated using MME-allocated transient IDs. If the signaling activity is a 4G Attach with IMSI, no restoration is performed, and the attach continues.

- Delete Request message

When a UE's context is purged from the MME's cache and database, a Delete Request message is sent to the SRS buddy to remove the replicated context. The sending of the Delete Request message to SRS buddy is controlled by the `supportUeRestorationContextDeletion` global parameter.

18.4 Pool level redundancy (Feature f14109-06)

This feature provides support for MME pool-level redundancy.

On each CMM, DBS VMs are used for storing UE restoration contexts received from one other CMM in the same MME pool via the proprietary NR10 interface. Therefore, any CMM can provide both call processing and session restoration functionality. There is no longer the need to deploy a specialized session restoration server (that is, the WMM SRS using the RS10 interface).

18.4.1 Support for spread NR-10 links on multiple IPDS (Feature f72001-19)

With this feature, an operator can provision the NR10 interface in multiple IPDS pools. This feature helps increase the message rate across the NR10 interface. The messages and mechanisms that are used to update and fetch a UE's context remain the same. The CMM load balances the UEs across multiple NR10 links. Traffic for one UE is routed to the

same NR10 link.

18.4.2 MME support for pool redundancy record delete enhancements (Feature f14109-08)

This feature provides support for deleting the UE's context from the buddy MME, which acts as an SRS for an MME serving the UE.

Some scenarios, such as subscriber deletion or receiving a Cancel Location Request, result in deleting the UE context record at a serving MME, but not at the buddy MME, causing stale records to be left on the buddy MME. This feature minimizes the number of stale context records on buddy MMEs by deleting buddy context records when a serving MME deletes the UE context.

The serving MME checks if the buddy MME supports SRS context deletion by checking the version in NR10 heartbeat messages. If the buddy MME is on a version that supports SRS Context Deletion, then the serving MME sends delete context request to the buddy MME.

18.4.3 CMM support for inter-release pool redundancy versions (Feature f14109-09)

This feature adds support for pool redundancy across releases so that restoration records created by a CMM on Release N can be retrieved and used to successfully connect a UE from a CMM on Release N+1 and vice versa.

This feature is an extension of the existing 4G/MME and 5G/AMF pool redundancy feature and adds support for pool redundancy across CMM software releases so that restoration records created by a CMM on release N can be retrieved and successfully used to handle a UE by a CMM on release N+1 and vice versa. This feature is especially beneficial when software upgrades are performed on CMMs within the same pools. For a while, CMMs in the same pool may be running different software releases, therefore, it is important for CMMs to understand and process the data written by an older or newer software release. This understanding is accomplished by UE context evolution (upgrading or downgrading) at the time of writing to and/or reading from the session restoration server.

This feature introduces NR10 protocol versioning or apiFullVersion formatted as MAJOR.MINOR.PATCH between different releases. The apiFullVersion IE is exchanged via NR10 Heartbeat messages. In a CMM that supports both MME and AMF (that is, Quad Access configuration), separate MME and AMF NR10 links are used and MME NR10 traffic, including

HB messages, is segregated from AMF NR10 traffic; therefore, both NFs maintain their own independent apiFullVersion.

MME NR10 apiFullVersion begins with 1.1.0, starting in release CMM21. AMF NR10 apiFullVersion begins with 1.1.0, starting in release CMM20.5, and so in release CMM21 release it is 1.3.0. Any CMM release older than CMM21 (for MME) and CMM20.5 (for AMF) has, by default, an apiFullVersion 1.0.0.

The major version is incremented when incompatible changes are introduced to the non-HB NR10 protocol message set. An MME or AMF on a previous major version is unable to understand content data in the new major version. When a change to the major version occurs, the NR10 heartbeat message continues to be backwards-compatible since it is used to transmit the protocol version to all other network elements.

The minor and patch fields are changed when changes to the NR10 protocol are introduced, in such a way that upgrades and downgrades of protocol content still allow a lower version network element to understand the content. The minor version is changed at the CMM release level when a change to the UE context data requires upgrade or downgrade of the UE context data. For example, releases CMM21, CMM21 M1, CMM21 M2, and CMM21.5 each have a higher minor version than previous releases if UE context data changes in the respective release. The patch version is changed when a software patch is introduced that changes the UE context data in a way that requires upgrade or downgrade of that data when interacting with a lower release network element.

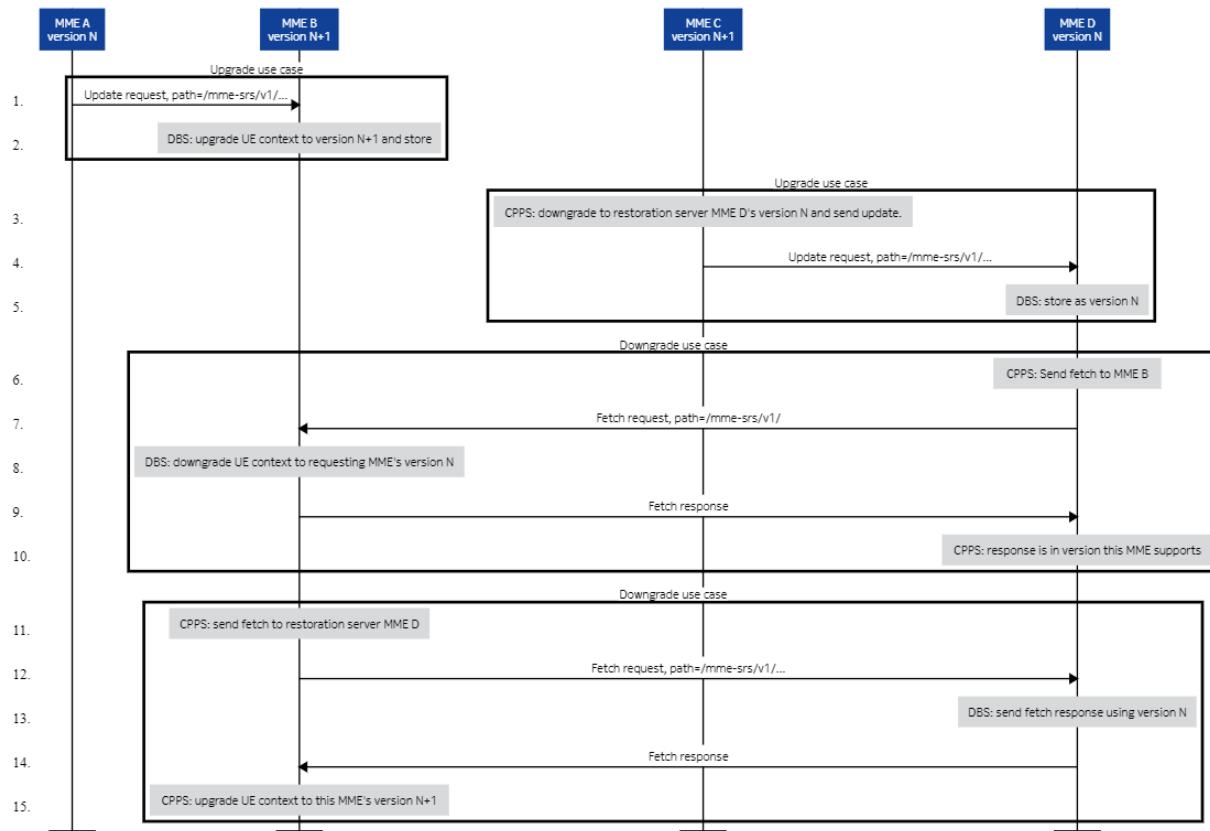
The UE context evolution is always performed in a stepwise fashion. For example, to upgrade from version N to N+2, two upgrades are performed, first from version N to N+1, then version N+1 to N+2. Furthermore, the NR10 data evolution is applied on a pair-wise interaction. When a pair of CMMs (MMEs or AMFs) with different software releases or NR10 protocol versions interact, the CMM having the newer protocol version is responsible for upgrading the UE context data received from an older CMM version to its own version. Similarly, a CMM having the newer protocol version is responsible for downgrading UE context data prior to sending to an older version CMM. Use of protocol version in pair-wise interactions only requires knowledge of another CMM's version when interacting with it.

Note:

- Any downgrading of UE context data can result in loss of new feature functionality. For example, if an AMF UE context is downgraded from version N+1 to N and checkpointed to restoration server as version N, when the UE context is then retrieved by an AMF on version N+1, the restored UE context will have new fields set to default values, which may differ from their values prior to checkpointing.
- For information about the supported transitions, see the *Release Compatibility Report*.

Figure *Pool redundancy upgrade and downgrade use cases* shows the upgrade and downgrade use cases between different releases.

Figure 162: *Pool redundancy upgrade and downgrade use cases*



18.4.4 CMM support for NR10 optimization enhancements - phase 1 (Feature f14109-13)

This feature optimizes the NR10 interface to increase capacity by not waiting for Acknowledge messages from the buddy CMM when sending Update Requests and Delete

Requests for the AMF and full Update Request and Delete Request messages for the MME.

This feature optimizes the NR10 interface to increase capacity. This feature is supported for VNF configurations with two IPDSs without L3NS.

Client AMF

The NR10 interface does not wait for an Acknowledge message from the server CMM when sending Update Request and Delete Request messages for the AMF. The client AMF includes “noack” in the path while sending Update and Delete Request messages to the server AMF. The client AMF also sends RST_STREAM to the server AMF after sending an Update or Delete Request message. The CMM does not wait for an update or delete response from the server AMF.

Server AMF

When the server AMF receives “noack” in the path of an Update or Delete Request message, then it does not send a response for that message.

Client MME

The NR10 interface does not wait for an Acknowledge message from the server CMM when sending full Update Request and Delete Request messages for the MME. If the gParm `supportFullUeRestoration` is also set to `true`, then the MME includes “noack” in the path when sending Update and Delete Request messages to the server MME. The client MME also sends RST_STREAM to the server MME after sending an Update or Delete Request message. The CMM does not wait for an update or delete response from the server MME.

Server MME

When the server MME receives “noack” in the path of an Update or Delete Request message, then it does not send a response for that message.

This feature is enabled using the gParm `inhibitPeerSrsResponses`.

18.4.5 CMM support for NR10 optimization enhancements (Feature f14109-14)

This feature adds support for partial updates over the NR10 interface for the MME.

When this feature is enabled using the global parameter `inhibitPeerSrsResponses`, the

first NR10 update that the MME sends to the buddy MME is a full update and all the subsequent updates are partial updates, which reduce the amount of data sent over the NR10 interface. If the buddy MME fails to process the partial update, the buddy MME periodically sends a new message over the NR10 interface to the client MME to indicate that partial update failed for all UEs. The client MME then marks these UEs. When the next procedure happens for those UEs, the client MME sends a full update to the buddy MME.

This feature provides the following enhancements in overload control for the NR10 interface:

- 4G IMSI-based throttling: for regular IMSI-based fetch in 4G when feature *MME support for enhanced backup of 4G UE context to the SRS for ISSU (Feature f17008-07)* is enabled, throttling starts when the CPU of the SRS crosses a threshold of 85% and when the own CPU is at 90%.
- 4G re-prioritization of SRS throttling. The following all apply for the MME when feature *MME support for enhanced backup of 4G UE context to the SRS for ISSU (Feature f17008-07)* is enabled:
 - At a predefined threshold of 75% SRS occupancy, the client MME throttles sending full updates to protect the MME acting as an SRS from having to shed its own call processing procedures. With this feature, the overload control (OLC) mechanism is enhanced to also consider the own CPU for throttling the full NR10 updates sent to the SRS.
 - When the SRS's busiest CPU crosses a predefined threshold of 80%, the client MME starts to throttle its partial updates to protect the MME acting as an SRS from having to shed its own call processing procedures. With this feature, the OLC mechanism is enhanced to also consider the own CPU for throttling partial NR10 updates sent to the SRS.
 - When this feature is not enabled, the MME sheds its fetch requests when its SRS crosses a CPU threshold of 80% and/or if its own CPU usage is above 85%. When this feature is enabled, the SRS threshold is 85% and the own threshold is 90% to ensure that fetches have highest priority in 5G.

18.5 Collision control

MME is designed to recover from unexpected transaction combinations and multiple messages of the same procedure. Mitigated collision scenarios improve network performance.

18.5.1 MME support for managed objects and enhanced collision handling (Feature m10508-01)

The *MME support for managed objects and enhanced collision handling feature provides enhanced algorithms for specific message collision scenarios.*

This feature provides enhanced algorithms for specific message collision scenarios as follows:

- The MME takes actions, as specified by item d in *3GPP TS 24.301 clause 5.5.1.2.7*, when the MME receives another Attach Request message from the UE while waiting for the Attach Complete message from the same UE on the same S1 connection.
- The MME takes actions, as specified by item e in *3GPP TS 24.301 clause 5.5.1.2.7*, when the MME receives more than one Attach Request messages from the UE on the same S1 connection before the MME sends the Attach Accept or Attach Reject for a pending Attach Request.
- The MME takes actions, as specified by item f in *3GPP TS 24.301 clause 5.5.1.2.7*, when the MME receives an Attach Request message from the UE in state EMM-REGISTERED. The MME invokes necessary EMM common procedures (GUTI reallocation, authentication, security mode control, identification, EMM information). The UE context and EPS bearer contexts, if any, are deleted and the new attach message is progressed.

 **Note:**

The action applies irrespective of whether the message is received on the same S1 connection or not.

- The MME takes the following actions when a TAU is received during the attach procedure on the same S1 connection:
 - The MME's actions if a TAU Request is received while waiting for the Attach Complete message from the UE are the following:
 - Timer T3450 is stopped.
 - The allocated GUTI is considered valid and the TAU procedure is executed.
 - The MME's actions if a TAU Request is received while waiting for the Modify Bearer Response message from the S-GW are the following:
 - The MME queues the request. The MME can proceed with common NAS procedures, such as AKA and SMC, if required in parallel while waiting for the Modify Bearer Response.
 - If another TAU Request is received while the TAU Request is queued, the MME discards the previous request and queues the most recent TAU Request only when

there is a difference in the IEs included in the NAS message. No abort counters are pegged and only peg AttTAU once.

Note:

The action applies irrespective of whether the message is received on the same S1 connection or not. The MME also supports queuing of TAU Request while waiting to receive the Modify Bearer Response.

- The MME aborts the attach procedure if a UE-initiated detach is received irrespective of the detach type and setting of the switch off bit.

Note:

The action applies irrespective of whether the message is received on the same S1 connection or not.

- The MME ignores any Service Request and Extended Service Request messages received during the attach procedure if received on the same S1 connection before the Attach Complete is received.
- The MME also ignores any Service Request and Extended Service Request received on the same S1 connection after receiving the Attach Complete, but before the Modify Bearer Request.
- If the Service Request and Extended Service Request are received on a different S1 connection, the attach procedure is aborted and the MME proceeds with the Service Request and Extended Service Request. The MME response depends upon the state of the UE at that point: If UE state is EMM-DEREGISTERED, the MME rejects Service Request and Extended Service Request. If the UE state is EMM-REGISTERED, the MME proceeds with Service Request and Extended Service Request.

Note:

A new S1 connection indicates that the UE might have lost the radio connection and established a new S1 connection.

- The MME rejects any S11 messages received before the transmission of the Create Session Request during the attach procedure. The MME ignores any S11 messages if received after the Create Session Request is sent and before the Modify Bearer Response is received.

i Note:

The strategy of ignoring messages during certain procedures is due to the following reasons: the MME does not queue the UE or network request. It is hard to determine whether the request is a valid request or not. If it is a valid request, the request is re-transmitted. The interval between the retransmissions may provide adequate time for the MME to complete the previous activity to accept the request for processing.

- The MME ignores any UE-initiated ESM messages received after the Initial Context Setup message and before the reception of the Modify Bearer Response except for the following cases:
 - The MME queues the following UE-initiated requests while waiting to receive the Modify Bearer Response. The MME proceeds with the request once the response is received.
 - Bearer Resource Modification
 - Bearer Resource Allocation
 - If the MME receives another Bearer Resource Modification or Bearer Resource Allocation while a request is queued, the MME discards the previous request and queues the most recently received request.

i Note:

Any ESM messages received before the authentication and security mode setup are rejected by the MME.

- If the MME requires to abort the attach procedure for any errors that occur before sending the Attach Accept, the MME sends Attach Reject. The MME uses the MME-initiated detach procedure for any errors that occur after sending the Accept.
- The MME queues any HSS request during the attach procedure except the Reset Request. The MME processes the HSS request after the completion of the procedure.
- If another Attach Request is received from the same UE on a different S1 connection, the current attach procedure is aborted and the new attach procedure is accepted and the MME treats this as a new attach.

i Note:

A new S1 connection may be a result of the UE losing its radio connection. The new S1 connection may be set up even before the old S1 connection is released due to the eNB timers to detect that the radio connection is lost. In this case, the UE is expected to re-request the procedure.

- The MME handles detach and attach message collisions as specified by item d in *3GPP TS 24.301 clause 5.5.2.3.5*.

i Note:

3GPP TS 24.301 specifies that the MME must accept an Attach Request before the completion of the detach procedure for the MME-initiated detach if the Detach Request message indicates that the re-attach is required.

i Note:

3GPP TS 24.301 specifies to accept the TAU message for the MME-initiated Detach.

- The MME handles detach and service request collisions as specified by item f in *3GPP TS 24.301 clause 5.5.2.3.5*. The MME ignores the Service Request message if the message arrives before the completion of the detach procedure.
- The MME rejects UE ESM messages and any S11 messages while detach is in progress.
- While waiting for Bearer Setup Response from the eNB, if the MME receives another Create Dedicated Bearer Request, the MME rejects the dedicated bearer activation to the S-GW with the cause value #73 Insufficient resources.
- If UE-requested bearer resource release results in bearer deactivation and if deactivation request is received in the MME while bearer activation procedure for the same bearer is in progress, deactivation procedure takes precedence. Activation procedure is aborted by the Bearer Resource Modification Reject message sent by the MME.
- If Bearer Activation Request is received after deactivation procedure has started, the activation procedure proceeds after deactivation procedure is completed. For deactivation triggered by Detach, deactivation procedure always takes precedence and activation procedure is aborted no matter its order by sending Bearer Modification Reject message.
- If any collisions of EPS bearer context deactivation procedure and modification procedure for the same bearer occur in the MME, deactivation procedures take precedence. Modification procedure is dropped silently if it is the same bearer id as the one in

progress, however, if it is a different bearer id, it is queued.

- The MME ignores any UE ESM (except the UE-initiated Detach and EMM) messages and also S11 network messages during X2 handover. If UE Detach message is received during the X2 handover, the MME aborts the procedure and progresses the detach.
- If needed to explicitly or implicitly detach the UE for any errors, the MME queues the Detach and proceeds with the detach after completing the handover.

 Note:

The detach type and cause code depend upon the type of error. Design changes the action to queue detach and proceed with it after completing the detach. This includes Detach due to HSS Cancel Location Request.

- The MME queues any HSS message received during X2 handover procedure except the Reset Request. The MME takes action on the HSS message after the completion of the message.
- If service request is received from the UE during X2 handover, the MME aborts the handover and proceeds with the service request.
- Upon receipt of a Cancel Location Request (CLR) from the HSS, the MME queues the CLR.
- Upon receipt of any NAS message other than Service Request from the UE while the paging procedure is in progress, no further page attempts are made for the current network-initiated service request and the MME sends a Downlink Data Notification Failure message to the serving gateway with a cause code of Service denied.
- Upon receipt of a Downlink Data Notification message while a UE-triggered service request procedure is in progress, the MME does not page the UE. It responds with a Downlink Data Notification Ack and proceeds with the UE-triggered service request procedure.

 Note:

The delay parameter for the Downlink Data Notification Ack must be calculated using same algorithm used for the network-triggered service requests.

- If the MME receives a request from the HSS (Cancel Location Request, Insert Subscriber Data Request, or Delete Subscriber Data Request) that requires call processing action, but the EMM and BSM (bearer session management) is busy processing another procedure, the HSS request is delayed by queuing the request. When the current procedure is finished, then CLR/IDR/DSR is processed.
- If the MME, while processing IDR with QoS changes, extracts new QoS, then it saves it to VLR, sends internal message to BSM, goes back to idle state and waits for Update Bearer Request from the S-GW. While waiting for Update Bearer Request, if a new request

arrives, it is honored; however, if bearer level updating is being processed, everything related to that bearer is blocked. For example, if bearer #5 is undergoing an update, everything related to bearer #5 at the bearer level is blocked.

- While handling CLR as the first request and another CLR request is received, the MME takes the following actions:
 - Set delete flag
 - Invoke call processing, if needed
 - Wait for call processing response
 - Send CLA to HSS
 - VLR delete
 - Ignore new procedures
- If the MME is busy processing purge UE, it sets the Delete UE in progress flag, it ignores the UE and eNB proxy, and rejects the HSS and SGW proxy. It clears the flag once the current procedure is finished and honors the new procedure.
- If the MME is busy processing a PUR request and a request to delete the VLR data (through CLI command) is initiated, the CLI request is delayed by queuing the request. When the current procedure is finished, the CLI request is processed.
- The MME sends the Downlink Data Notification Acknowledgement with a cause value requested accepted if the Down Link Data Notification (DDN) message is received during service request and extended service request procedure. All other S11 messages are ignored except a Delete Bearer Request of the last default bearer.
- If the MME receives the Delete Bearer Request for the last default, the MME aborts the service request/extended service request procedure and explicitly detaches the UE. The detach type used is re-attach not required and a cause value used is implicit detach.
- If a UE-requested Detach is received, the MME aborts the service request and extended service request procedures and progresses the UE-initiated detach.
- The MME aborts the service request and extended service request procedures if the MME implicitly needs to detach.
- The MME drops service request if received in ECM-CONNECTED state and it logs a message indicating that service request is received in ECM-CONNECTED state. In this case, the MME pegs both attempt counter and abort counter.
- If the MME receives extended service request while the UE state is set to the S-GW suspended state, the MME sends the Service Reject message with a cause value of implicit detach.
- The MME handles reception of the following messages, if received while service request and extended service request is in progress, as specified in 3GPP TS 24.301 clause 5.6.1.6:
 - Upon receipt of a Tracking Area Update Request message prior to the MME sending a Tracking Area Update Accept message for a previous Tracking Area Update Request

message for the same UE, the MME aborts the previously initiated procedure if there are differences in the information elements included in the messages. Processing will then proceed for the new request. However, if the message content of the two messages is the same, the later Tracking Area Update Request message is ignored. The MME pegs ABortTAU PM and AttTAU PM in this case.

- Upon receipt of a malformed Tracking Area Update Request message, the MME responds with a Tracking Area Update Reject message with one of the following reject causes based upon the type of issue found with the received message:
 - #96: mandatory information element error
 - #99: information element non-existent or not implement
 - #100: conditional IE error
 - #111: protocol error, unspecified
- The Tracking Area Update Reject message is encoded as specified in *3GPP TS 24.301 clause 8.2.25*.
- Upon receipt of another Tracking Area Update Request message before the Tracking Area Update Complete is received while processing a previous Tracking Area Update Request for the same UE and if this message is received after the MME sent a Tracking Area Update Accept message, the MME aborts the previously initiated procedure if there are differences in the information elements included in the messages. Process then proceeds for the new request. However, if the message content of the two messages is the same, the Tracking Area Update Accept message is retransmitted and the T3450 timer is restarted, if necessary, and no other processing is performed for the later Tracking Area Update Request message. Note that aborted or ignored Tracking Area Update attempts are pegged in TAU performance measurement counts as a failure of any kind.
- MME will ignore any UE ESM messages and any S11 messages from the network except a Delete Bearer Request of the last default bearer during the TAU procedure both in ECM-IDLE and ECM-CONNECTED state. If the MME receives a Delete Bearer Request for the last default bearer, the MME aborts the TAU procedure and explicitly detaches the UE. The detach type used is re-attach not required and cause value used is implicit detach.

 **Note:**

The probability of collisions is very low during this procedure. However, if received, ignoring the message results in re-transmission increasing the probability of processing the message.

- If internal errors cause the TAU procedure to be aborted, the MME immediately detaches the UE.
- The MME queues any HSS request during the TAU procedure. The MME processes the HSS request after the completion of the procedure except for the reset request.

- If the MME receives TAU message after the Context Acknowledge message and before the timer expires, the MME accepts the TAU Request, however, if Attach and Service Request is received, the MME rejects it.

18.5.2 Queuing network-initiated session request during mobility management procedures (Feature m10117-01)

The *Queuing network-initiated session request during mobility management procedures* feature enables queuing network-initiated session management requests during initial attach and IRAT handover and executing these requests at the completion of the procedure or at a point where eNB does not reject non-handover-related messages and/or communication with the UE is established.

The MME queues up to three network-initiated requests during attach and IRAT handover procedure. The only requests that are queued are Create Bearer Request, Delete Bearer Request, and Update Bearer Request associated with existing PDN connections. The MME simply drops any requests if it cannot queue the request either due to full queue or for any other reason. The MME drops any network-initiated procedures during an intra-LTE handover.

18.5.3 Extend queuing for all CSFB scenarios (Feature m10117-02)

The *Extend queuing for all CSFB scenarios* feature supports the re-sending of the S1AP UE Context Modification Request to an eNB, queuing of an SGsAP Paging Request message from the MSC, and the queuing and re-sending of a Downlink NAS Transport message and a CS Service Notification message.

This feature supports the re-sending of the S1AP UE Context Modification Request to an eNB after an S1AP UE Context Modification Failure message is received with the cause IE set to X2 handover triggered or S1 intra-system handover triggered.

This feature supports the queuing of an SGsAP Paging Request message from the MSC while the UE is undergoing an X2 handover or S1 handover. After the handover is complete, the SGsAP Paging Request is processed.

This feature supports the queuing and re-sending of a Downlink NAS Transport message and a CS Service Notification message while the UE is undergoing an X2 handover or S1 handover or when the eNB responds to an S1AP Downlink NAS Transport message with an

S1AP NAS Non Delivery Indication message with the cause IE set to X2 handover triggered or S1 intra-system handover triggered.

18.5.4 E911 collision scenarios (Feature m10112-04)

The *E911 collision scenarios* feature changes the current handling of collisions of UE-requested mobility management procedures and any network requests while waiting for a response to LCS-AP Location Request message to the E-SMLC.

For collisions where the UE is still connected, the MME proceeds with the received request and continues to wait for the response from E-SMLC. For other collisions in which the UE S1 connection must be released (excluding interactions with the feature *Homogeneous LCS Enhancements: Continuation of LCS Session after S1 Connection Release*), the MME sends LCS-AP Abort to the E-SMLC and waits for a response from the E-SMLC. For both the cases, the MME sends the Provide-Location- Answer (PLA) to the GMLC when it receives a response from the E-SMLC or upon t_{3x01} time out.

Related descriptions

- [Homogeneous LCS enhancements: continuation of LCS session after S1 connection release \(Feature m11000-02\)](#)

18.5.5 Enhanced queuing network-initiated session requests for X2/S1 HO (Feature m10117-04)

The *Enhanced queuing network-initiated session requests for X2/S1 HO* feature extends queuing capability during handover to include network-initiated bearer operations.

This feature is an extension of earlier collision control features. In those features, attach and IRAT handover procedures, CSFB procedures, SGs paging, and NAS downlink messages were queued if it was determined that the MME was processing an X2/S1 handover, or if the procedure was rejected with an indication from the eNB that a handover was in progress. This feature extends that queuing capability during handover to include network-initiated bearer operations.

The feature supports CRs that would enhance user experience for any network-initiated bearer requests during X2 handover. During X2 handover, if there is no S-GW relocation, the MME sends the requests to the target eNB.

With the implementation of this feature, bearer-related procedures that are affected by a

S1- handover in-progress are queued by the MME and replayed to the serving eNB at the completion of the handover procedure. This only applies in the situation where no MME change (standard behavior for X2 handover) and S-GW relocation are involved in the handover.

The objective of this queuing feature is to avoid procedure rejections that have the potential to result in poor user experience, such as delay in establishing or modifying a new bearer.

The MME queues the following network-initiated requests during X2 handover, S1 handover, and IRAT handover:

- Create Bearer Request
- Delete Bearer Request
- Update Bearer Request

 **Note:**

During S1 handover, queuing occurs only on the target MME side during scenarios with the MME relocation. Queued requests on the source side are dropped after handover completion. Queued requests on the target side are dropped on handover failures, in which the UE falls back to the source MME.

The MME supports a queue depth of three (3) when queuing network-initiated bearer requests.

The MME drops (without reject) any network-initiated bearer request that is received during an X2/S1 handover if the request results in the maximum supported queue depth being exceeded.

For the X2 handover, the dequeuing or dropping of queued network-initiated bearer requests is as follows:

- The MME processes (dequeues) any queued network-initiated bearer requests after the success of the X2 handover.
- The MME drops any queued network-initiated bearer requests after the failure of the X2 handover and drops any new requests exceeding the maximum queue depth.
- The MME processes (dequeues) any queued network-initiated bearer requests after the failure of an outgoing IRAT handover if the UE remains on the source MME.

For S1 handover, the dequeuing or dropping of queued network-initiated bearer requests is dependent on whether the S1 handover is an intra-MME or inter-MME.

In case of an intra-MME S1 handover, the MME processes (dequeues) any queued network-

initiated bearer requests after the completion (success or failure) of S1 intra-MME handover.

In case of an inter-MME S1 handover,

- the source MME drops any queued network-initiated bearer requests after the success of the S1 inter-MME handover.
- the source MME processes (dequeues) any queued network-initiated bearer requests after the failure of the S1 inter-MME handover if the UE remains on the source MME.
- the target MME processes (dequeues) any queued network-initiated bearer requests after the success of the S1 inter-MME handover.
- the target MME drops any queued network-initiated bearer requests after the failure of the S1 inter-MME handover.

18.5.6 MME collision handling of HO/TAU and ESM procedures (Feature m10117-05)

The *MME collision handling of HO/TAU and ESM procedures* feature provides several enhancements to the *MME collision handling of handover/TAU and ESM procedures*.

The collision handling of this feature improves the completion of the mobility management procedure with queuing of the ESM procedures. The collisions handled by this feature are the following:

- Delete bearer collisions with TAU/service request that follows an abnormal release of UE S1 connection.
 - An abnormal UE S1 connection release results in deactivating the GBR and while the MME is in the process of deactivating the GBR bearer, TAU/Service Request is received from the UE. The collision is handled as follows:
 - The MME does not delete the GBR while waiting for S1AP Release Request Complete message from the eNB or until S1AP UE context release timer (`ueContextRelease`) is expired. The S1AP UE context release timer's default value is 8 seconds.
 - If the MME has not started the S1 release procedure, it does not delete the GBR bearers.
 - If the MME has started the S1 release procedure, it waits for the completion of the procedure and then proceeds with the TAU/service request.
 - The deactivation of the GBR bearer is done as follows: the MME checks timer `deleteGbr` with range 0 to 20 seconds, and default value 0.
 - If the `deleteGbr` timer is set to 0, the MME deletes GBR bearers immediately after receiving the S1AP Release Request Complete message from the eNB or on the expiration of S1AP UE context release timer.

- If the `deleteGbr` timer is non-zero, the MME starts the `deleteGbr` timer immediately after receiving the S1AP Release Request Complete message from the eNB or on the expiration of S1AP UE context release timer. The MME does not delete the GBR bearers.
- The MME stops the timer for the following events if they occur before the expiration of the timer:
 - Service request and TAU
 - Paging
 - Attach and detach
 - If all the GBRs are deleted due to P-GW requests
- The MME deletes the GBR if the timer expires while the UE is in the ECM-IDLE state.
- The implementation prior to this feature was resulting in a situation where the MME and UE were waiting for responses to their requests resulting in not completing the UE TAU Request. These collisions are handled as follows:
 - If the MME determines that TAU Request will be received, then it waits for a configurable period of time before processing any network-requested ESM procedure.
 - During this X2/S1 handover TAU time interval, any network-initiated bearer requests received are queued.
 - Upon reception and completion of the TAU procedure or X2/S1 handover TAU timer expiry, the MME de-queues any network-initiated network request, if present, and processes them.
 - The MME queues up to three ESM requests from the network.
- ESM collision with a normal TAU Request (includes a combined TAU): The same handling scheme as described for the ESM collisions with TAU Request that follows X2/S1 handover is used.
- ESM collisions with X2/S1HO. Prior collision features handled ESM collisions during X2/S1 handover. This feature provides the following improvements:
 - Any network-initiated ESM requests are queued if the eNB rejects any E-RAB management messages with cause S1 intra-system handover triggered or X2 handover triggered.
 - In the case of S1 handover, the queued messages are only processed if there is no MME relocation.
 - The MME handles X2/S1 handover that may occur at three different stages of the ESM procedure as follows:
 - Stage 1: The MME has not sent the ESM request to the UE. In this case, the MME queues the request and processes the request after the completion of the handover.
 - Stage 2: The MME has sent the ESM request to the UE, but the MME has not heard

back from the UE and the supervision timer is still running. In this case, the MME puts the procedure on hold and proceeds with the X2/S1 handover. At the completion of the handover, the MME sends the ESM request again through the new eNB.

- Stage 3: The MME has received UE response, but it has not sent response to P-GW or it is waiting for the P-GW response. In this case, the MME sends the response and then proceeds with the handover.
- TAU Request collisions with S11 Downlink Data Notification (DDN) message:
 - Prior to implementation of this feature, when the MME was receiving a DDN while processing the TAU, the MME simply dropped the DDN. This behavior is supported.
 - With the implementation of this feature, when the MME receives a TAU Request while processing DDN message, three configurable options are supported:
 - Send DDN failure

This option preserves the current behavior. The MME sends the DDN failure with cause #89 and proceed with TAU.
 - Re-page

The MME stops paging and proceeds with the TAU Request. After TAU is complete and S1 release is done, the MME pages the UE. The MME uses the provisioned paging procedure just as original page used.
 - Treat TAU without the Active Flag set in the EPS Update IE as a TAU Request with the Active Flag set.

The MME treats the TAU Request without the Active Flag set in the EPS Update IE as a TAU Request with the Active Flag set and sends S1AP Initial UE Context Request to set up the bearers. This option basically eliminates the need to page the UE.
- TAU Request collisions with S11 Downlink Data Notification
 - Collision of S11 Delete Bearer Command sent by the MME to delete the voice bearer (QCI=1) in SRVCC handover and S11 Delete Bearer Request for the same bearer by the PGW. In this case, the MME queues the P-GW requests and responds appropriately after the completion of the Delete Bearer Command.
 - DDN collision with UE context release, that is, S1 release, procedure: the MME queues the DDN Request received if the MME is in the process of UE context release and proceeds with the DDN Request after completing the UE context release procedure. The UE context release may be triggered by the eNB or MME.

The feature covers the following UE-initiated session management procedures:

- Bearer resource allocation
- Bearer resource modification

The feature covers the following network-initiated procedures:

- Create bearer request
- Update bearer request
- Delete bearer request

18.5.7 PDN KPI improvement (Feature m10152-01)

The *PDN KPI improvement* feature improves the PDN Connectivity Request and PDN Disconnect Request KPIs by approximately 0.5%.

The MME's behavior for PDN Connectivity Request (the disconnect case is very similar) is as follows: The UE is in the ECM-CONNECTED state and sends PDN Connectivity Request to establish a default bearer. Normally, the MME performs the Create Session Request/Response exchange and then sends the eRAB Setup Request to the eNB and Activate Default Bearer Request to the UE. When the MME receives answers to these two requests, the MME informs the S-GW of the new S1-U data and the procedure is done.

The eNB dormancy timer can expire at any time while this procedure is being processed. When this occurs, the eNB sends the UE Context Release Request to the MME with S1AP cause User inactivity. The MME uses the release request as a trigger to abort the PDN request and then carries out the release procedure.

With the implementation of this feature, the MME looks at the S1AP cause in the Release Request and drops the request if it occurs while the PDN procedure is ongoing when the S1AP cause is User inactivity. The most common outcome with this change is that the PDN procedure is completed successfully before the eNB resends the UE Context Release Request, which can then be processed normally. In the unlikely event that the PDN procedure is still ongoing when the eNB sends the Release Request for the second time, the MME drops the request if the S1AP cause is User inactivity. If there is no response after the second try, the eNB sends eventually a Release Request with an error cause. Typically, the eNB uses S1AP cause Release due to reason generated in the E-UTRAN.

18.5.8 Collision of incoming delete bearer request procedure and ongoing update bearer request procedure (Feature f10159-01)

The operator can enable the MME to handle the collision of the incoming delete bearer request procedure and the ongoing update bearer request procedure.

When an S11 delete bearer procedure received by the MME collides with an ongoing

incoming S11 update bearer request procedure for the same EPS bearer:

- If the global parameter `collDbreqUbreq` is disabled (by default), the cause code in the response to the update bearer request procedure is set to reject, which means that the update bearer request procedure is rejected.
- If the global parameter `collDbreqUbreq` is enabled, the collision handling remains the same. The update bearer response procedure is still aborted, however the cause code within the update bearer response procedure will be changed from reject to accept.

This feature is not applicable for the scenario in which a delete bearer request collides with an update bearer request containing multiple bearers.

18.5.9 MME support for SRVCC HO and X2 HO collision (Feature f10502-01)

This feature supports collision of SRVCC handover with X2 handover. MME may receive Path Switch Request message when SRVCC handover is ongoing and before receiving Handover Cancel message but mostly after sending Handover Command message to the source eNB.

MME will proceed with SRVCC handover cancellation and after receiving PS to CS Cancel Notification message from the MSC, MME will proceed with the Path Switch Request.

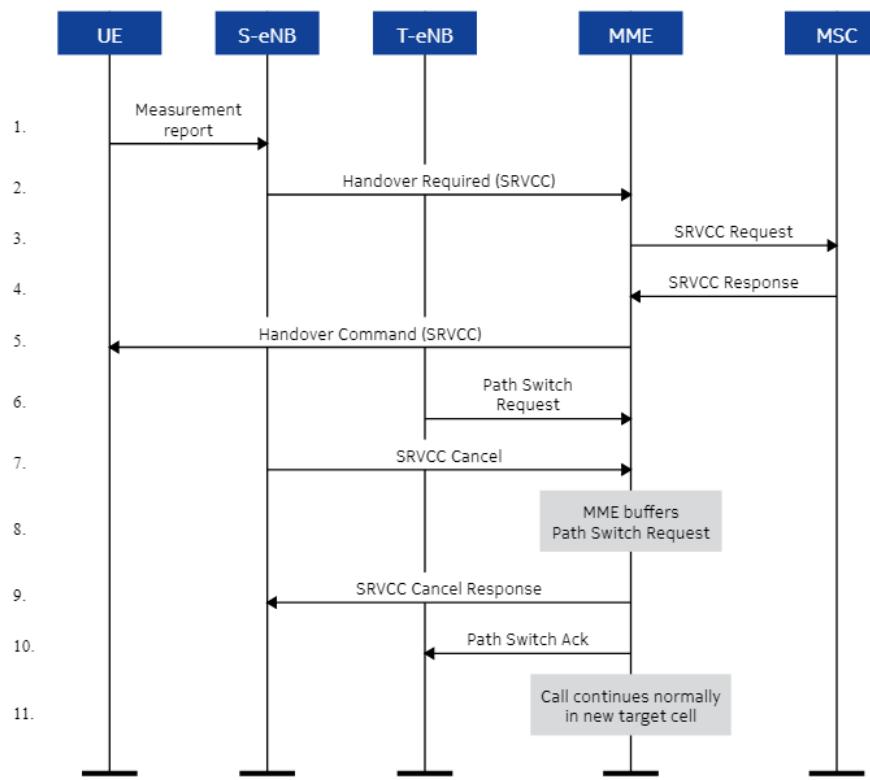
MME sends NAS notification message to UE through the target eNB. The notification message is sent to indicate to the UE that SRVCC handover is cancelled.

MME will send Handover Cancel Ack to the source MME.

MME sets the cause IE value of the SRVCC PS to CS Cancel Notification message sent to the MSC server as follows:

- 'Unspecified' if the handover is cancelled due to reception of a S1AP Initial UE message
- 'Handover/Relocation cancelled by source system' if the source eNB triggers the cancel
- 'Handover/Relocation cancelled by target system' if the handover is cancelled due to the reception of Path Switch Request message.

Figure 163: SRVCC HO - X2 HO collision handling



18.5.10 Improved handling of QoS modification collisions (Feature f13304-01)

This feature introduces a change to the MME's behavior during QoS modification collisions to prevent the MME from sending Update Bearer Response to the S-GW.

This feature addresses three identified collision scenarios:

- CSFB fail due to collision handling update bearer, UE not responding
- Update CSFB/QoS bearer modification scenario so CFSB completes
- Handling of incoming TAU colliding with Bearer Modification

When the feature is enabled through global parameter `qosModCollEnh` and the global parameter `sendSgw3gppS11cc` is set to `No`, the MME will not send Update Bearer Response to the S-GW in the above scenarios.

18.5.11 Send Delete Bearer Response with cause 110 during SRVCC collision (Feature f10502-03)

With this feature, the MME supports sending Delete Bearer Response with cause # 110 during SRVCC collision.

The feature is controlled by global parameter `srvccCollSendDbrCc110`. When the feature is enabled (the global parameter is set to `Yes`), the MME supports sending Delete Bearer Response with cause code 110 (Temporarily rejected due to handover/TAU/RAU in progress) during SRVCC collision.

By default, the feature is disabled.

18.5.12 CMM support for Origination Time Stamp IE and Maximum Wait Time IE to help P-GW to detect collisions (Feature f11504-01)

With this feature, the MME includes the Origination Time Stamp IE and the Maximum Wait Time IE in the Create Session Request message that is sent on the S11 message to gateways.

Due to node selection and geo-redundant nodes in the network, it is possible that the same PDN session can be created in two different network elements. Additionally, it is possible that the receiving nodes process the message after the sender has timed out on the message.

This feature enables the MME to include the Origination Time Stamp IE and the Maximum Wait Time IE in the Create Session Request messages sent to the S-GW. These IE indicate the maximum time that the MME is going to wait before giving up the message response and the procedure. The S-GW uses the same timestamp and maximum wait time.

The S-GW uses the same time stamp and maximum wait time to identify if the request is still a valid message and if the S-GW processes it. If the message is processed, the intermediate nodes replicate the time stamp and maximum wait time in messages generated by the node towards other peers. Each network element compares the timestamp with its own synchronized (NTP) time to ensure stale messages are not processed.

18.6 Signaling optimization

These features are designed for signaling load reduction.

18.6.1 Basic DPR/DPA (Feature m11301-02)

The **Basic DPR/DPA feature provides support for link establishment and resilience across Diameter interfaces.**

This feature provides basic support for Diameter peer exchange (DPR/DPA messages).

In Diameter protocol interactions, Disconnect-Peer-Request (DPR)/Disconnect-Peer-Answer (DPA) messages are handled as follows:

- When the peer node, for example, HSS, sends a DPR message to the MME, the MME answers the HSS with a DPA message, and will fail-over to another (secondary) HSS. The MME then expects the HSS to close the connection. After closing and a grace period longer than the DPR message timer (for example, 10 seconds), the MME attempts to reconnect with this HSS. If the HSS has not closed the connection within a 10-25 second interval, the MME re-initiates the connection.
- If the MME detects that the HSS link is being blocked (for example, using MME CLI command for link blocked, or for shutdown of remote end-point), the MME sends a DPR to the HSS, and waits the duration of the DPR message timer, for the HSS to respond with a DPA. When the DPA is received or times out, the MME gracefully closes the connection and completes the link blocking operation to this HSS.

The DPR message timer (`dprMsgTimer`) is configurable through the `diamProfile` command. The disconnect cause (`dprDisconnectCause`) sent by MME with DPR is configurable through the `rmtEndPtCfg` command.

The *Basic DPR/DPA* feature requires the *Diameter relay agent (DRA)* feature.

Related descriptions

- [MME support for basic DRA \(Feature m11307-01\)](#)

18.6.2 MME support for basic DRA (Feature m11307-01)

The **MME support for basic DRA feature provides support for load balancing and network overload assistance for S6a/HSS traffic.**

This feature introduces Diameter routing agent (DRA) functionality supported by the MME across the S6a interface. If a Diameter request is received by a DRA, the DRA determines the HSS identity based on the provided user identity and forwards the Diameter request directly to the HSS. In this case, the user identity to HSS resolution decision is communicated to the

MME in the Origin-Host/Origin-Realm AVPs of the response. The MME can store the determined HSS identity/name/realm and use it in further Diameter requests to the same user identity.

With this feature, the MME supports the following routing-related AVPs and routing-related errors, as specified in *RFC 3588, sections 6.1.8 and 6.4*.

- Origin-Realm
- Origin-Host
- Destination-Realm
- Destination-Host
- Proxy-Info
- Route-Record

The CMM supports up to three (3) Route-Record AVPs in the answer or request messages from the HSS/EIR/GMLC. The MME can receive and ignore up to three Route-Record AVPs in these messages. The MME echoes back Proxy-Info AVPs in the same order with the same Protect bit and it applies to both success and error MME answer messages.

With *Enhanced DRA support*, mixed mode of HSS and DRA is supported. The MME assumes the DRA only when the DRA support parameter is set on the remote end-point configuration, or HSS only when this parameter is set to False.

This feature works well with the *S6a retry different HSS* feature.

The *MME support for basic DRA* feature requires the Diameter routing agent (DRA).

Related descriptions

- [Diameter connections with load balancing \(Feature m11320-01, f11304-01\)](#)

18.6.3 Basic DRA for SLg interface (Feature m11309-01)

The *Basic DRA for SLg interface* feature provides support for load balancing and network overload assistance for S6a/HSS traffic.

This feature supports Diameter routing agent (DRA) for SLg interface. The feature includes:

- configurable flag to support DRA interface or direct connection to a GMLC
- support for routing-related AVPs and routing-related errors

The *Basic DRA for SLg interface* feature requires a Diameter routing agent (DRA) and a GMLC.

18.6.4 Enhanced DRA support (Feature m11303-01)

The **Enhanced DRA support** feature provides support for load balancing and network overload assistance for additional diameter nodes.

This feature extends the support for the *base Diameter routing agent (DRA)* feature by providing the following enhancements:

- DRA support for S13 interfaces
- Mixed-mode support for S6a, S13, SLg. With mixed-mode support, both DRAs and HSSs/EIRs/GMLCs are supported on the same MME at a per link basis.
- S13 retry capability (no retry is performed for SLg)
- S6a roaming DRA support

The *Enhanced DRA support* feature requires the *Diameter routing agent (DRA)* feature.

Related descriptions

- [MME support for basic DRA \(Feature m11307-01\)](#)
- [Diameter connections with load balancing \(Feature m11320-01, f11304-01\)](#)

18.6.5 Automatic neighbor relations (ANR) (Feature m10904-01)

The **Automatic neighbor relations (ANR)** feature helps automating the process of defining neighboring eNB IP addresses reducing the operations cost of managing eNB addition and maintenance in the network.

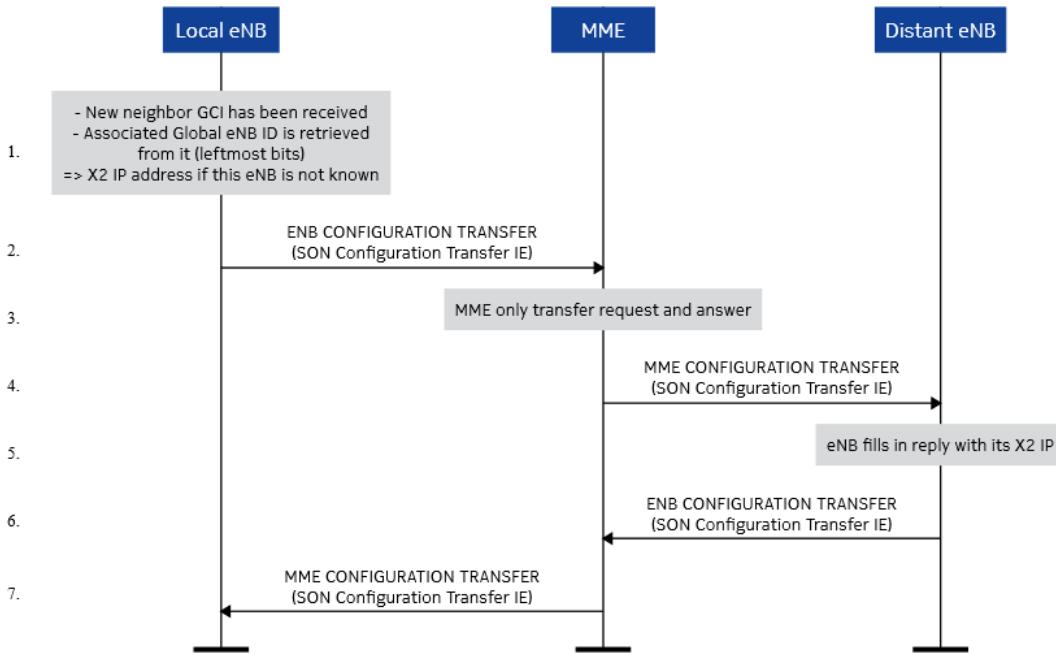
This feature supports exchange of S1-AP eNB Configuration Transfer Message between two eNBs to support the *automatic neighbor relation and optimization eNB* feature. An eNB obtains another eNB's IP address to set up X2 connection to the other eNB.

The *Automatic neighbor relations (ANR)* feature on eNB supports necessary capabilities to automatically generate neighbor relations to cells hosted by an eNB. A neighbor relation from a source cell to a target cell means that eNB controlling the source cell:

- knows the ECGI/CGI and PCI of the target cell
- has an entry in the neighbor relation table for the source cell identifying the target cell
- has the attributes in this neighbor relation table entry defined, either by OAM or set to default values. Examples of these attributes are target eNB IP address and SCTP ports.

The IP address of the eNB hosting a cell that is considered as a neighbor candidate is retrieved through two different S1 procedures involving the serving MME and the distant eNB itself. These procedures are described in 3GPP TS 36.413. The figure provides an overview of the process.

Figure 164: ANR



The call processing logic for ANR is as follows:

1. New neighbor relation has been (partially) defined: only PCI and ECGL of the potential neighbor cell are known. IP address of the hosting eNB needs to be acquired.
2. If S1 based solution has been selected, then ENB Configuration Transfer message is built, including Target Global eNB Id and TAI (extracted from the cell ECGL) and Source Global eNB Id and TAI.
3. SON Information Request IE is set to X2 TNL Configuration Info to request X2 IP address.
4. When the message is received by the MME, SON Configuration Transfer IE is transparently copied to the MME Configuration Transfer message that is sent to the eNB identified through received Target eNB-ID.
5. When the MME Configuration Transfer message is received by the target eNB, this one sends back ENB Configuration Transfer message to the MME. In this case, SON Information Reply IE that contains X2 TNL Configuration Info that carries the IP address is used.
6. As previously, when receiving the message, the MME transparently copies SON Configuration Transfer IE into the MME Configuration Transfer message that is sent to the source eNB.
7. Source eNB receives the message and extracts target eNB IP address from it.

This functionality is supported by both inter and intra-pool.

The *Automatic neighbor relations (ANR)* feature requires the eNB to support ANR.

18.6.6 S6a retry for NOR S6a messages (Feature m11323-01)

The *S6a retry for NOR S6a messages* feature provides an enhancement to support the retry for Notify Request (NOR).

Prior to the implementation of this feature, when the `s6aRetryDifferentHss` global parameter was changed to Yes, the MME only retried S6a Authentication Information Request (AIR) and Update Location Request (ULR) to secondary S6a link when the primary S6a link was reporting an error.

This feature provides an enhancement to also support the retry for Notify Request (NOR). The specific error scenarios where the retry handling is needed are the following:

- No response to request received in primary S6a link.
- The following error responses are received from the primary S6a link:
 - DIAMETER_TOO_BUSY
 - DIAMETER_OUT_OF_SPACE
 - DIAMETER_UNABLE_TO_DELIVER

The feature reduces unnecessary network signaling load.

18.6.7 S6a retry for PUR S6a messages (Feature m11323-02)

The *S6a retry for PUR S6a messages* feature supports an enhancement to support the retry for Purge UE Request (PUR).

Prior to the implementation of this feature, when `s6aRetryDifferentHss` global parameter was changed to Yes, the MME only retried S6a Authentication Information Request (AIR) and Update Location Request (ULR) to secondary S6a link when the primary S6a link was reporting an error. This feature supports an enhancement to also support the retry for Purge UE Request (PUR). The specific error scenarios where the retry handling is needed are the following:

- No response to request received in primary S6a link.
- The following error responses are received from the primary S6a link:

- DIAMETER_TOO_BUSY
- DIAMETER_OUT_OF_SPACE
- DIAMETER_UNABLE_TO_DELIVER

The feature reduces unnecessary network signaling load.

18.6.8 Error handling enhancements for PDN connectivity rejections (Feature m10140-01)

The *Error handling enhancements for PDN connectivity rejections* feature brings enhancements to PDN connectivity rejections when UE requests PDN connection for a network for which a PDN connection already exists and when there is a standalone PDN Connectivity Request (APN=x) for which the MME has an already established connection to the same APN with certain characteristics.

Prior to the implementation of this feature, the MME behavior, when a PDN Connectivity Request was received, was to check whether there was already a PDN connection to the network specified by the APN in the PDN Connectivity Request. When the received APN was the same as the APN of a PDN connection that has already been established for the UE, the MME was sending PDN Connectivity Reject with cause code #55 Multiple PDN connections for a given APN not allowed.

In addition to observing this during otherwise normal traffic conditions, there were cases in which a disruption in transport could cause a large increase in the frequency of occurrence of this failure mode. This suggests that some particular UE models experience difficulty on the bearer plane and they send a PDN Connectivity Request for the PDN connection they already have without first sending PDN Disconnect Request.

With the implementation of this feature, upon receipt of a UE requested PDN connection for a network for which a PDN connection already exists, the MME immediately deletes the previously established PDN connection and then honors the new UE requested PDN connection request.

Upon the receipt of a standalone PDN Connectivity Request (APN=x) for which the MME has an already established connection to the same APN, if the global parameter `dltPrevPdnConnOnNewReq` value is `Yes`, and that connection is not the only APN connection, the MME deletes the existing PDN session prior to processing the new PDN Connectivity Request.

Note:

An APN connection is considered the same by the combination of both the APN name and the IP address type (IPv4, IPv6). If the new PDN Connectivity Request cannot be queued or processed, the request is dropped.

Upon the receipt of a standalone PDN Connectivity Request (APN=x), the MME rejects the request if the UE has only one established PDN connection and that existing connection is the same APN received in the request. This behavior is observed even if the

`dltPrevPdnConnOnNewReq` global parameter is enabled.

Anticipated impact to the bearer setup KPI is approximately 0.4% absolute. For the subset of UEs that send a PDN Connectivity Request for the PDN connection they already have without first sending PDN Disconnect Request, the implementation of this feature allows these UEs to quickly re-establish internet service if there is a transient problem in the bearer path.

The feature reduces unnecessary network signaling load.

18.6.9 Barring access above UE procedure frequency count (Feature f10726-01)

This feature is used to detect abnormally-behaving UEs and to manage the signaling flood they may generate (either automatically or due to user action).

The feature is to minimize the harm of too frequent requests from the same misbehaving UE(s) for the operator by first trying to stop the UE attempts and by last starting to ignore any further unnecessary attempts.

The MME attempts to minimize the harm caused by the frequently attempting UEs by attempting to:

- prevent the UE from frequently retrying.
- slow down the retry frequency.
- drop the handling of the message as early as possible.

KPIs are not affected by the abnormally-frequently attempting UEs, for the operator can use feature specific counters to exclude feature detected cases from the KPIs.

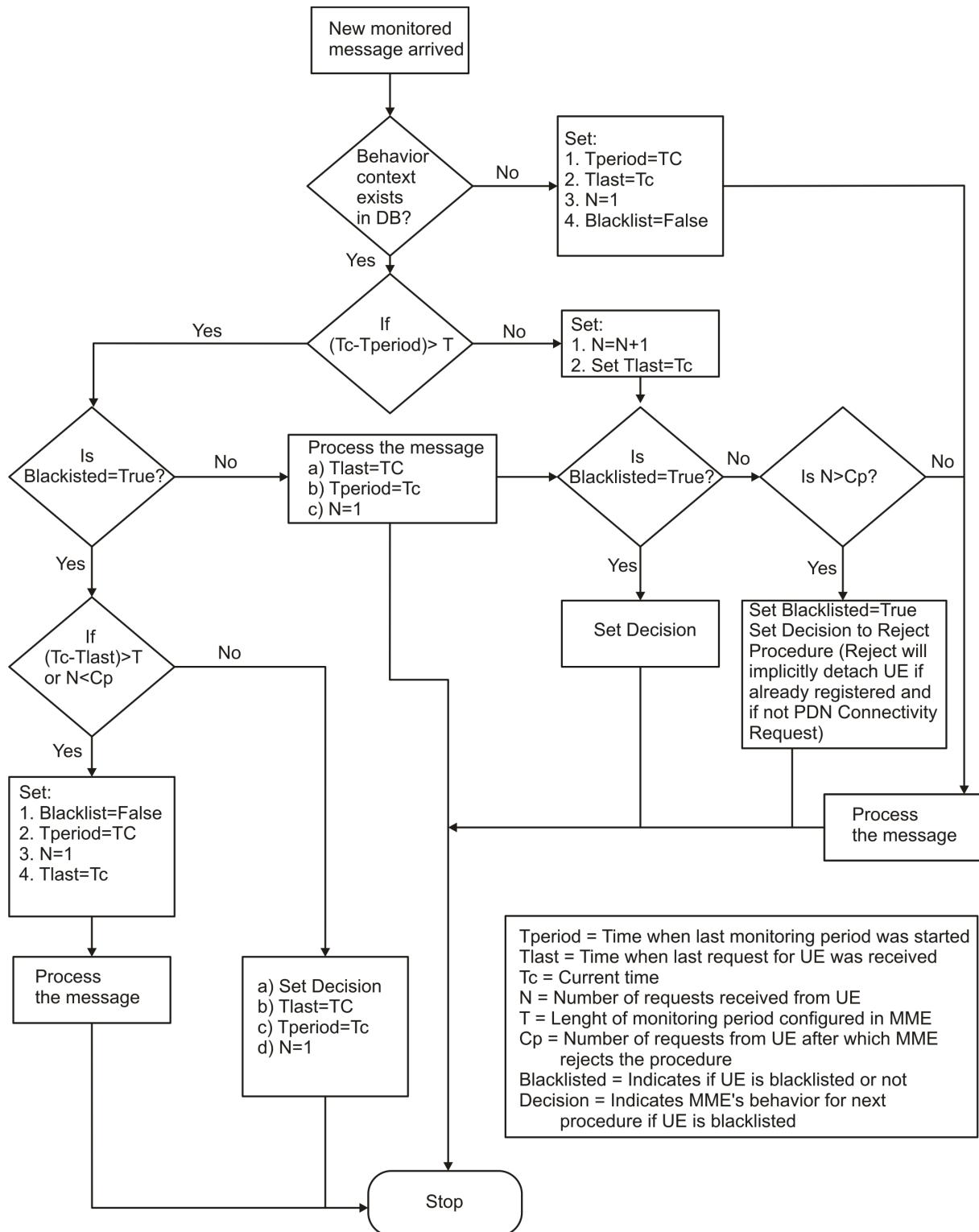
With this feature, attempts for attaches, standalone PDN connectivity requests and service requests (including also control plane service requests and extended service requests) from a single UE are counted into the MME internal UE specific counter and based on the sum of

the single UE attempts for (all of) those procedures during a time interval, the UE is possibly detected to behave abnormally (too frequent attempts) and is handled as described on further requirements.

Table 77: Behavior content

Behavior context data	Description
Tperiod	Indicates when the last monitoring period begins.
Tlast	Indicates when the MME receives the last procedure attempt.
N	Indicates the number of the procedures attempted by UE within a monitoring period.
Denylisted	Indicates whether the UE is isolated/denylisted.
Decision	Indicates how the MME will handle the next procedure request from the UE, the possible values are <ul style="list-style-type: none"> • reject procedure • detach • drop procedure

Figure 165: UE denylisting logic



18.6.10 S6a fault handling enhancement (Feature m11318-01)

The **Error S6a fault handling enhancement** feature reduces unnecessary new signaling load

towards the MME from attach requests when it is incapable of processing due to lack of an HSS node availability.

Prior to the implementation of this functionality, when there were no enabled S6a links, the MME's relative capacity was unchanged at the eNBs and a fraction of IMSI attach requests controlled by that relative capacity value was sent to the MME where the attempts failed.

With this feature, when the last enabled S6a link for the home PLMN transitions from enabled to disabled, and when this condition persists for more than 30 seconds, the MME sends Configuration Update messages to the eNBs with the MME relative capacity set to 1.

All traffic for all UEs that does not require S6a link continue to be processed.

Most of the S6a-related traffic (attach) result in the eNB redirecting the UE to another MME in the pool.

A small number of new attaches continue to fail on the MME with no S6a links. While this feature does not provide a special treatment when no S6a links are available to any of the MMEs in the pool, the network behavior under this condition is no worse than prior to the implementation of this feature.

The eNB treats relative capacity set to 0 as an indication that the MME is completely unavailable for service and redirects all traffic to other MMEs in the pool; hence value of 1 is used by this feature.

When there are no S6a links in the enabled state for the home PLMN and no one transitions enabled, and when there exists at least one S6a link enabled for the home PLMN for more than 30-45 seconds, the MME sends MME Configuration Update messages to the eNBs with the MME relative capacity set to its normal value.

The S6a HSS link update to the eNB capacity function is controlled through a first feature enablement parameter.

This feature detects scenarios where authentication challenge is optional (provisioned reauthentication frequency), and all S6a links relevant for the specific UE are down. In these cases, the MME skips the re-authentication step in order to provide service continuity.

Any other call processing activity that requires a transaction on S6a still causes procedure failures as prior to this feature implementation.

The S6a continuation of procedures with optional AKA function is controlled through a second feature enablement parameter.

18.6.10.1 S6a fault handling scenarios and parameters

When there are no enabled S6a links, the MME relative capacity is unchanged at the eNBs and a fraction of IMSI attach requests controlled by that relative capacity value is sent to the MME where the attempts will fail.

Home PLMN S6a links are links that are associated with HSS mapping rules (IMSI routing rules) that are keyed by the home network MCC and MNC. There may be one or more mapping rules. The set of S6a links described here are those associated with any rule keyed by the home MCC and MNC.

The following parameters control S6a fault handling:

Table 78: Parameters controlling S6a fault handling

Parameter	Scenario	Action taken
S6a HSS update eNB capacity (<code>s6aHssUpdateEnbCapacity</code>) is set to home HSS (<code>home</code>). This setting enables the detection of link availability and/or degradation of all the home PLMN HSS resulting in action to update eNB capacity parameters.	All home PLMN HSS are unavailable (the last home PLMN HSS link transitions from enabled to disabled) and while this condition persists and all home PLMN HSS link remain out of service during a wait period (~30 seconds).	The MME sends MME Configuration Update message to eNBs with the MME relative capacity set to one (1).
	No S6a links were previously in service, after the first home PLMN HSS link is restored into service (and it remains in service), and there is at least one home PLMN HSS link in service during a waiting period (~30 seconds).	The MME sends an MME Configuration Update messages to the eNBs with the MME relative capacity restored to its normal value.
S6a fault continue procedure with AKA optional (<code>s6aFaultContinueProcedureWithAkaOptional</code>) parameter is set to Yes. This allows some UE procedures to continue without using/requiring authentication vectors.	When all of the S6a links relevant to a single UE are down and an authentication challenge is about to be executed by the MME solely because of the PLMN security settings (implying that the AKA is optional).	Skip the AKA and continue the procedure. Any other call processing activity that requires a transaction on S6a will still cause procedure failures. Note that only the S6a links used to support the specific UE are relevant to this capability.

18.6.11 HSS signaling load reduction (Feature m11308-01)

With the HSS signaling load reduction feature the MME sends NOR at PDN session creation only when there is a P-GW change. Additionally, the MME suppresses the ULR when the MME already has subscription data for the UE.

This feature reduces the HSS signaling load, especially during attach storms.

Prior to the implementation of this feature, the MME sent Notify Request (NOR) to the HSS at every PDN session creation.

With this feature, the MME suppresses the NOR to the HSS if the P-GW FQDN stored in the VLR for the APN matches the P-GW FQDN selected for the current request for the same APN (initial attach or PDN connectivity procedures). Conversely, the MME sends NOR only when there is a P-GW change.

Additionally, when the UE attempted the LTE attach (IMSI or GUTI), the MME always performed S6a Update Location Request (ULR) to the HSS.

With this feature, the MME suppresses the ULR if the following conditions are true:

- The UE attaches with a local GUTI that the MME is successfully able to identify without using the NAS identity request procedure.
- The MME already has subscription data for the UE.
- In a shared network scenario, the PLMN for the TAI provided by the eNB matches the GUTI.

Both suppression policies are controlled by the setting of two independent HSS signaling load reduction parameters, global parameters `hssUlrReduction` and `hssNorReduction`.

18.6.12 MME support for KPI improvement (Feature m10911-02)

The **MME support for KPI improvement** feature specifies KPI improvements based on a critical support team's suggestions. There are several instances where the MME can make a change in the way it handles procedures that reduce failures.

Specifically, this feature supports the following:

- Purge the VLR for a particular UE after repeated procedure failures.
- Accumulation of failed procedures per subscriber counter.
- Upon no response to the HSS message Authentication Information Request (AIR) Or Update Location Request (ULR), the MME tries alternate HSS IP address even if the link is still up at the protocol level.

The feature reduces unnecessary network signaling load.

18.6.13 NAS CC to S-GW reject code mapping (Feature m10108-02)

The *NAS CC to S-GW reject code mapping* feature supports mapping of GTPv2 rejection indication cause codes to NAS ESM cause codes.

This feature supports re-mapping of two GTPv2 reject indication cause codes from the S-GW to MME over the S11 currently set to NAS ESM cause code #38 Network failure.

- Cause code #78 Missing or unknown APN, which is triggered by invalid APN received in the request in Create Session Request, maps to NAS ESM cause code #27 Missing or unknown APN.
- Cause code #93 APN Access denied - no subscription, which is triggered by Static address not allowed, APN selection mismatch and APN restriction violation, maps to NAS ESM cause code #33 Requested service option not subscribed.

18.6.14 Exclude destination host (Feature f11335-01)

This feature introduces a configuration change that controls the behavior whereby MME does not include the peer identity learned from the DRA in subsequent requests, and as a result, the destination host learned will not be sent in S6a or S13 requests to DRA (unless DRA destination host is provisioned for S6a or S13, which is non-standard).

When a DRA destination realm is provisioned, the same provisioned DRA identity will be sent in every (first and subsequent) request to the DRA.

MME can be configured to exclude the learned origin host as destination host in subsequent request messages to a DRA sent across S6a and S13. By default this capability is disabled.

Related descriptions

- [Exclude the vendor specific application ID \(Feature f11335-01\)](#)

18.6.15 Controlling sending of S1AP Connection Establishment Indication message (Feature f10410-01)

This feature supports a capability for the operators to choose MME handling of the S1AP Connection Establishment Indication message to be compliant with 3GPP stage 2 or stage 3 specifications.

Currently 3GPP stage 2 (23.401) and stage 3 specifications (36.300 and 36.413) do not

agree on when to send the S1AP Connection Establishment Indication message.

This feature introduces a global parameter to enable MME to support stage 3 requirements. If the global parameter `limitS1apConnEst` is set to `Yes`, the MME does not send the S1AP Connection Establishment Indication if it sends S1AP Downlink NAS Transport message. This rule will result in the MME not sending the S1AP Connection Establishment Indication message in attach and TAU request procedures.

MME sends the S1AP Connection Establishment Indication message in the CPSR procedure if the MME does not send any downlink data or the service accept message.

MME includes UE radio capability in S1AP Downlink NAS Transport message if the MME has the UE radio capability info.

18.6.16 Diameter routing message priority (Feature f11322-01)

Wireless networks can be restricted in different ways, such as by using multiple subscriber data management (SDM) cores and including of DRA in the network. Diameter overload indication conveyance (DOIC) implementation limits the conveyance of overload in SDM cores up to the immediate DRA layer that the SDM core is connected to.

The feature allows SDM clients, specifically MMEs/P-GWs and CSCFs, in communicating priority for a message.

This client provided priority will be utilized by DRA when making decisions related to diversion or throttling of the traffic, when SDM requests traffic reduction using DOIC.

The diameter routing message priority (DRMP) is communicated to SDM servers by DRA, if it is provided by the client.

If this feature enabled, a new AVP, such as DRMP, is added in S6a request messages (Authentication Information Request, Update Location Request, Purge UE Request, and Notify Request) sent out of the MME. The values for this AVP are read from configuration table configured through CLI, where DRMP value is defined for these request messages.

18.6.17 Further enhancements on HSS unavailability (Feature f11318-01)

This feature ensures service availability for some of the home users (and roamers treated as homers) even during HSS outage. The MME provides further enhanced functionality to

overcome HSS unavailability and ensures home subscriber access to the network whenever UE security context is still available. This feature enhances the functionality of feature S6a fault handling enhancement (m11318-01).

This feature overcomes HSS unavailability and ensures home subscriber access to the network as follows:

- On UE registration attempts (attach or TAU) inside the same PLMN, if the MME receives the security context (MM context) from the old MME or holds it already on its database, the MME is able to proceed and allow the UE to register.
- MME, however, delays the sending of ULR or NOR until the S6a link is available.
- On attach cases the MME uses a failopen profile instead of actual UE subscription data, if the actual APN configuration data is not available on the MME's local database An example is re-attach into new MME, when subscriber data is not available on the new MME. GTPv2 Identification Response does not provide any APN configuration data.
- If MME does not hold or get a hold of unused vectors or security context for the UE, it rejects the UE attempt.
- If the UE attaches with IMSI, it is assumed to have removed any previously existing security context and thus the MME accepts the UE registration only if the MME holds or is able to get a hold on an unused vector.
- During TAU performed after a previous IRAT handover, if there are no unused vectors left, the MME does not force re-authentication. MME follows PLMN security provisioning (authentication interaction percentage set for `IRATTAUpdate`) and if no authentication is to be run, MME continues using the mapped security context also after the TAU completion.
- If HSS does not reply to MME, or replies with an error code (DIAMETER_TOO_BUSY, DIAMETER_OUT_OF_SPACE or DIAMETER_UNABLE_TO_DELIVER), and the number of such occurrences exceeds a configurable threshold during a time interval, the MME marks the HSS as not available and considers the corresponding S6a link disabled for a configurable time interval.
- MME raises an alarm when an HSS gets denylisted. The alarm is cleared when the HSS is removed from denylist (after the configurable denylist timer has expired) or if any HSS-initiated request message is received.

The MME enhances HSS unavailability handling by

The functions can be enabled separately:

- delayed ULR and/or NOR sending
- HSS denylisting, including the trigger threshold and duration
- failopen profile and failopen APN configuration.

18.6.18 MME support for HSS unavailability recovery (Feature f11318-02)

With this feature, the MME continues with the attach/TAU procedure even when the HSS is unavailable by using the provisioned `failopen` profile which acts as a dummy subscription data until the HSS is available again. In addition, with the automatic and manual restoration modes, the MME tries to restore UEs which were using the `failopen` profile once the HSS is available again.

This feature includes additional-options-related HSS unavailability and the unavailability recovery. This feature enhances the functionality introduced in *Further enhancements on HSS unavailability (Feature f11318-01)* and adds restoration mechanisms.

The feature supports the following functions:

- Continues the procedure during the N26-based inter-IRAT mobility when the MME has security context/mapped security context and the MME can proceed without authentication.
- Provisions the number of authentication vectors per UE PLMN/serving PLMN combination.
- Enhances the `failopen` profile for serving the UEs during the HSS unavailability. A `failopen` profile can be provisioned per UE PLMN/serving PLMN combination. When defining per UE PLMN/serving PLMN, the `failopen` profile can contain a list of failopen APNs. Up to 50 failopen APN lists are supported, and up to 50 APNs are supported on all APN lists. The MME supports up to 16 APNs per APN configuration list. The `interworking5GsIndicator` parameter is additionally included on the failopen APN provisioning (compared to the legacy MME global failopen APN configuration).
- Provides options to restore the normal status and service for UEs that have been able to get or stay attached with special mechanisms during the HSS unavailability. The MME performs these actions once the HSS is back on service. The MME supports the automatic and manual mode to perform these restoration actions. The restoration actions include detaching the UEs that only have failopen-profile-based PDNs established and deactivating any failopen-profile-based PDNs for UEs that also have "normal" PDNs established. The rate of the manual restoration process can be provisioned by the operator.
- New parameter under the `failopen` profile is used to control whether the APN override based on failopen profile is allowed.
- Provides CLI options to output the subscriber counts (the `failopen` profile based on PDNs established).
- Provides corresponding PM counts and PCMD information.

18.6.19 CMM support for treat MIP6-Agent-Info in IDR as one entity (Feature f11336-01)

This feature supports treating the MIP6-Agent-Info AVP in Insert-Subscription-Data-Request (IDR) as one entity rather than individually modifiable elements. A global parameter is used to control the treatment.

The MIP6-Agent-Info AVP (defined in *IETF RFC 5447*) contains necessary information to assign an home agent to the mobile node: IPv4 address, IPv6 address, P-GW host, and P-GW realm. With current implementation, MME treats this information as four individual pieces data. If Insert-Subscription-Data-Request (IDR) has some of the four and does not have the others, MME preserves the missing ones, copying from the old VLR to new the VLR.

With this feature, MME can treat MIP6-Agent-Info AVP as a single piece of data. If IDR has one of IPv4 address, IPv6 address, or host (P-GW host and realm), other data is deleted.

When global parameter `treatMip6AgentInfoInIdrAsOneEntity` is enabled, MME treats MIP6-Agent-Info in IDR as one entity. By default, this functionality is disabled.

18.7 Load balancing

These features support network redundancy and sharing of traffic load.

18.7.1 MME S1 flex - basic pooling (Feature m10800-01)

The *S1 flex*, also known as *multipoint S1* or *MME pooling*, enables the connection of each eNB to all EPC nodes within a pool area (see 3GPP TS 23.401).

A group of MMEs serves an MME pool area connecting to several eNBs. The MME pool area is an area within which a UE may be served without the need to change the serving MME. The MME pool area is served by one or more MMEs (pool of MMEs) in parallel. The MME pool areas are a collection of complete tracking areas and may overlap each other.

Pool areas must be configured to the E-UTRAN. This information is also needed in the DNS.

The eNB selects an available MME for serving a UE at every UE transition from (RRC) idle to (RRC) connected mode. Selection is based on:

- Network topology: the selected MME serves the UE's location.
- The MME load: The eNB is responsible for the MME load balancing (within the pool).

Selection takes into account relative capacity of each MME.

- The UE state: For new attachments, selection is based on above conditions. For registered UEs, current serving MME is selected, unless the UE is in a border.

Each eNB is configured (through EMS) with the MME pool configuration.

If the UE has been allocated a GUTI, then the eNB selects the current serving MME (associated with the GUTI which identifies the current serving MME).

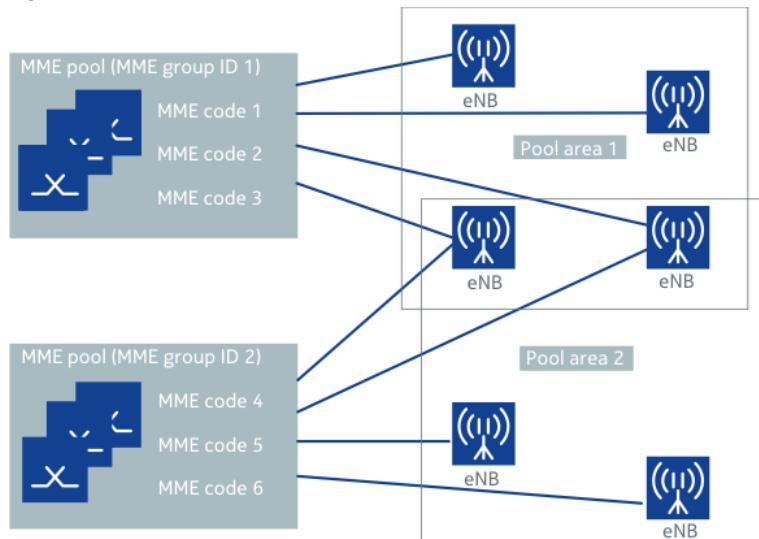
We assume that the eNB has the S1 connectivity to the serving MME, for example, as long as the eNB has the serving MME in its pool list. Otherwise, the eNB selects a new MME for the following cases:

- IMSI attach: Most likely after an UE power-up
- TAU or GUTI attach request from the eNB that does not have a serving MME associated with GUTI in its pool list.

Relative MME capacity weighted factor (0-55) is set by the MME within one MME pool and passed down to the eNB at S1-Setup.

- The eNB selects one MME based on received MME weighted factor.
- If weighted factor is the same among MMEs, the eNB selects the MME in round robin manner.
- The eNB does not select the MME from the other MME pool even though it might have IP connection to the neighbor MME pool in edge eNBs.
- The MME determines relative capacity based on the number of CPPS instances and their state: active and out of service.
- Whenever the number of CPPS instances changes for any reason, the MME sends changes to relative capacity to all the eNBs with S1 connections to the MME using Configuration Update message.
- The MME can override automatic updates of relative capacities to the eNB and use provisioned values. This capability is useful in case of maintenance activities.

Figure 166: Example of S1 flex implementation



The feature improves resilience, optimizes capacity, and reduces network load.

Using multiple MMEs within a single pool area increases the service availability, as other MMEs can provide services if one of the MMEs in the pool area is not available. The eNB can select another MME if the primary MME is not available. An MME pool also enlarges the served area compared to the service area of only one MME. The eNB selects the MME from the pool area on the basis of MME relative capacity in case the UE does not indicate any previously selected MME in the pool. Thus, there is some load distribution of the signaling traffic.

Load balancing takes place between multiple MMEs.

The S1 flex feature reduces signaling load on the S6a interface between the MME and HSS, as subscribers do not move as much between MMEs.

The *MME S1 flex - Basic pooling* feature requires the eNB support of S1 flex.

18.7.2 MME offloading (S1 flex - SON) (Feature m10800-01)

The *MME offloading (S1 flex – SON)* feature enables an operator to move subscribers between the MMEs that are in the same MME pool. Operators can add and remove an MME in a pool without interrupting ongoing sessions. Offloading helps solving MME overload situations. It also makes in-service software upgrades possible even when a node reset is required. User services remain uninterrupted during the MME maintenance.

This feature can be used to remove an MME from the pool for maintenance, for example.

- Removing a single MME from a pool (one to many move)
 - Based on standards-based procedures outlined in 3GPP TS 23.401 clause 4.3.7.3.
 - Paced to 75 UE/sec/CPSS or 2.7m/Hr (nominal). Relocation is done in parallel across all CPSSs.
 - ECM/EMM-CONNECTED UEs are marked for move once the active call is completed.
 - Emergency calls are preserved.
- Rebalancing pool traffic load to a new or recovered MME (many to one move). Single method is supported: percentage of load from all MMEs in pool relocated to a single target MME.

UE move granularity

ECM/EMM-IDLE and ECM/EMM-CONNECTED UEs are re-located dynamically as the move process walks the UE context database. The total percentage only of all registered UEs attached to an MME can be defined for the move process.

Call processing

Inter-MME UE relocation is performed with the help of the eNBs that have active S1 connection to the source MME and other MMEs in the pool that is targets of relocation.

At the beginning of UE relocation, the MME sends a Configuration Update message to each eNB with which it has an active S1 connection indicating that the source MME has 0 capacity. Upon receiving this Configuration Update message, eNBs do not send any new sessions to the source MME; instead they must send them to other MMEs within the same pool.

During relocation, the MME sends UE Context Release message with cause code Load balancing TAU required to each registered connected UE. When the UE comes back with a TAU, the eNB sends the UE to another MME within the pool. The S10 link between the source and target MME is used by the target MME to obtain UE context from the source MME.

During relocation, the MME pages idle UEs to bring them back to connected state and then releases the UEs using UE Context Release message with cause code Load balancing TAU required.

If a UE performs an ESM procedure during relocation, the UE is sent a context release with cause code Load balancing TAU required message after the completion of the procedure.

Inter-MME UE relocation is performed at a controlled pace in order not to overload the source MME. The pacing is based on the number of registered connected and registered idle UEs that are present in the MME. Sufficient time is given to page idle UEs. The maximum timeout value for a single page attempt is set at 60 seconds. The maximum number of page

attempts during inter-MME relocation is provisionable with a default value of 4 and a minimum value of 1.

Since the UE load on a typical MME (consumer traffic model) can be up to 5M UEs, this is a long procedure with the maximum allowed completion time (camp on timer) of 54 000 seconds with a default completion time of 5400 seconds.

The relocation procedure is divided into the following periods:

- CAMP ON during which UE relocation takes place.
- DRAIN is a grace period of 5 minutes provided during which the UEs that have started relocation can finish relocation gracefully.
- In case of 100% registered UE relocation, the MME aggregate service is locked at the end of the DRAIN period.
- Note that the completion time for the entire command is the time given in the command line + 5 minutes for a drain phase. The drain phase allows for graceful relocation of UEs for whom the relocation procedure has started just before expiration of time given by the operator to finish the procedure.

Requirements

The feature depends on the *MME pooling* feature.

The feature requires S10 interface support and the MME pool deployment with multiple MMEs in a MME pool.

18.7.3 Directed inter-MME subscriber move (Feature m10713-01)

The *Directed inter-MME subscriber move* feature introduces the use of GUTI re-allocation call flow for directed inter-MME UE move procedure where the destination MME for user move is explicitly defined.

In the MME offloading standardized by 3GPP, the eNB is responsible for selecting one of the other MMEs as the target MME. The MME under which the UE appears after the offloading is not defined.

This feature introduces the use of GUTI re-allocation call flow for directed inter-MME UE move procedure where the destination MME for user move is explicitly defined.

- Much more flexibility is provided on how load can be re-balanced across the pool.

- There are many more choices about which UEs to move.

One to one move

- The move is based on GUTI re-allocation method.
- The move involves a selection of a specific source and target MME.
- Volume of UEs to move is defined based on the provisioned selection criteria.
- Relocation is done in parallel across all CPPSs.
- ECM/EMM-CONNECTED UEs are marked for move once the active call is completed.
- Emergency calls are preserved.

One to many move

- The move is based on GUTI re-allocation method.
- The move involves a selection of a specific source MME.
 - Volume of UEs is based on the selection criteria, or all
 - When all, ability is provided to lock the MME aggregate service.
- Relocation is done in parallel across all CPPSs.
- ECM/EMM-CONNECTED UEs are marked for move once the active call is completed.
- Emergency calls are preserved.

The number of UEs to move can be expressed by number or percentage. In case an absolute number of UEs is specified and the UE filter covers several radio types, the number of UEs to move is distributed proportionally.

The selection of UEs is filtered through the following criteria:

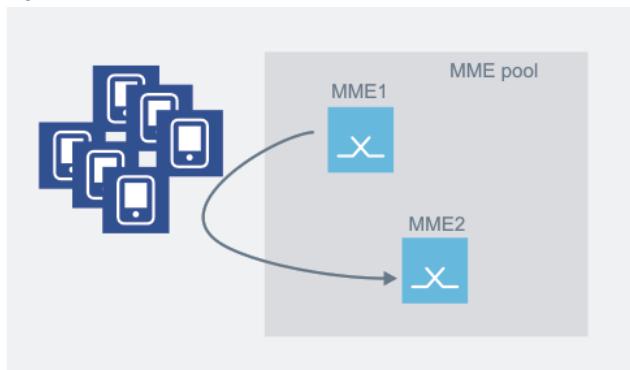
- UE state: active, idle, all
- mobile network
- IMSI range
- MSISDN range

Specifying number of UEs, other than all, is not supported in a combination with the following criteria:

- IMSI range
- MSISDN range

The directed move can be used to re-balance a specific UE or UE types and is particularly useful for operators to re-locate test devices onto a specific MME for a new SW version testing, for example.

Figure 167: Subscriber move based on IMSI/MSISDN range



The *Directed inter-MME subscriber move* feature requires MME pooling.

Related descriptions

- [MME S1 flex - basic pooling \(Feature m10800-01\)](#)
- [MME offloading \(S1 flex – SON\) \(Feature m10800-01\)](#)

18.7.4 S-GW draining (Feature m10131-01)

The *S-GW draining* feature enables operators to offload an S-GW for maintenance or load re-distribution. Note that this feature is now obsolete.

This feature provides a mechanism to move UEs off of an S-GW so that maintenance operations on that S-GW can be carried out without any service impact.

With this feature, sessions drain off of an S-GW through normal attach traffic instead of forcing UEs to another S-GW. To do this, the state of an S-GW link is changed to shuttingdown. When this is done, the link is still used for UEs that have an established session on the S-GW, but any new attach that normally would have been established on that S-GW is sent to other candidate S-GWs instead.

If S-GW restoration is enabled, instead of using normal attach, the MME proactively moves sessions to other S-GWs in the S-GW pool, typically resulting in no impact to HSS load, and full load of S-GW subscribers moved in about 30 minutes.

Expected uses for this capability are the following:

- Maintenance is required on an S-GW and the service provider does not want to have a spike of re-attach traffic when the S11 link is locked. The S11 link is therefore placed in the shutting-down state some time before the maintenance action starts. Field data suggests that 90% of sessions are drained within 3 hours.
- A service provider wants to operate their S-GWs in an N+1 sparing configuration. A given

set of tracking areas have two S-GWs associated with it through DNS data; one unique to the TA set, the other a single spare S-GW used for all TA sets. The spare S-GW is assigned a higher DNS order value so that it is normally not selected. The S11 link to the spare S-GW on every MME is set in the shutting-down state. During normal operation, all sessions are established on the S-GW unique to the TA set. If the S11 link to that S-GW becomes disabled, sessions are established on the spare. Once the unique S-GW link is restored to service, sessions begin to drain from the spare without any manual intervention. If the S11 link is in the shutdown administrative state, migration of UEs toward the higher priority S-GWs occur much more quickly than if the link is in the unlocked state. Since S11 links are usually dynamic links, it is possible that the operator may be required to manually place the S11 link into the shutdown administrative state. If the link is not in the shutdown state, migration of UEs toward the higher priority gateways still occurs but at a much slower rate.

18.7.5 Extending provisioned timer range for UELB (Feature m10702-04)

The *Extending provisioned timer range for UELB* feature enables operators to have a better control of UE load balancing through configurable rate control mechanisms.

This feature provides an option to make the UE load balancing drain timer interval dynamically set based on paging for UE load balancing parameters, which can result in much shorter waiting time at the end of the UE load balancing operation. The feature includes a provisonable parameter to slow down the UE load balancing operation to prevent surge in S6a traffic from overwhelming HSS/DRA capacity. With the implementation of this feature:

- The UE load balancing provisioning parameter governs the length of the drain step.
- The UE load balancing provisioning parameter allows throttling of the rate the UEs are moved away from the MME, in order to protect S6a resources from overload.

Customers who have experience using UELB to move individual UEs have noted that UEs must be moved serially and the drain period for UELB makes it very time consuming to move several UEs.

The current UELB drain period (hard coded at 5 minutes) was set with the largest volume of UEs moved and consideration for the longest possible time for any UE to be paged and complete the move process. The maximum interval to move an ECM-IDLE UE can be over 4 minutes, which is what leads to the current hard coded time interval.

It is more likely, however, that operators choose 1 or 2 attempts, and 3 - 6 second T3413

timer values for each attempt, resulting in an overall move interval closer to 15 seconds.

In order to ensure that the actual interval that is governed by the aforementioned parameters is never undershot, a dynamic drain interval is introduced that takes the product of the actual provisioned number of paging attempts used during UE load balancing, and the actual provisioned T3413 timer settings for those attempts, and adds 10% for procedure latency.

Operators may find that using the dynamically set drain interval significantly shortens the UE move operation for a single, or small number of UEs moved, while when moving the bulk or all UEs from an MME/SGSN, the static (5 minutes) drain interval ensures minimum service impact of the move operation.

With this feature, a provisioning parameter is introduced which enables or disables the dynamic drain interval for UE load balancing. When the parameter is enabled, it dynamically calculates the drain interval based on the UE page attempt during load balancing and the T3413 timer parameter values. When this parameter is disabled, a longer, maximum possible interval to complete the move for a UE is used (5 minutes) which ensures that all UEs have moved and all transient procedures have been completed prior to the UE load balancing operation completion.

Additionally, some customers have noted that the rate at which UEs are moved can result in a surge of load on the HSS/HLR. For example, when the MME sends an Update Location Request (ULR) for every moved UE, even with the overload protection through DRA, some load balancing TAU events can fail due to throttling at the DRA. Therefore, pacing is valuable with or without DRA. The same is applicable for the associated SGSN UE load balancing operation and impact to the HSS/HLR capacity depending on S4 or GN-SGSN.

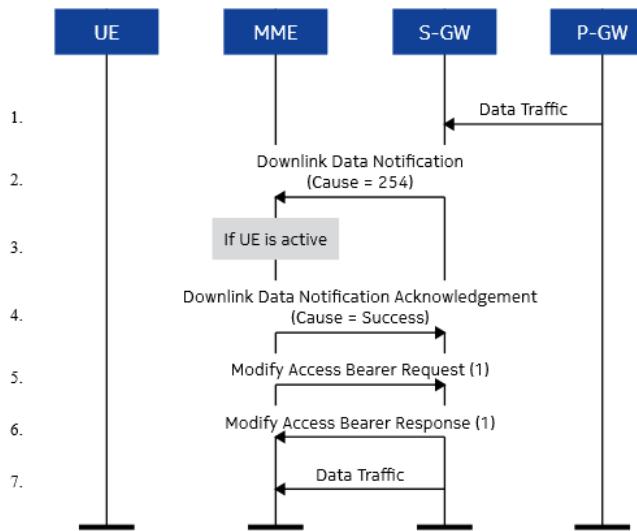
Prior to the implementation of this feature, the MME used a hard coded timer parameter to control the rate that the load balancing process walked through the UE context database to move UEs. The value of this parameter has been optimized to complete the largest UE move, draining all UEs from a fully loaded MME, within a standard maintenance window. When a smaller set of UEs are moved, or HSS/HLR/DRA capacity can be impacted, it is beneficial to slow the move rate down.

With this feature, a timer parameter is introduced, UELB deceleration fraction with a range of 10 to 100 percent in 10 percent increments with default value of 100% of the current maximum rate so that service providers can slow UELB down by a fixed fraction given by this parameter. The MME UELB process inverts the input parameter and multiplies by the hardcoded maximum move interval parameter.

18.7.6 S-GW geo-redundancy via ICR (Feature m10804-01)

The **S-GW inter-chassis redundancy (ICR)** allows a pair of S-GWs to be deployed in a redundant fashion so that in case of failure of a primary node, the secondary node can continue to service UEs without invoking node failure recovery actions by the adjacent nodes (the MME and P-GW).

Figure 168: S-GW geo-redundancy through ICR



The S-GW ICR allows the S-GWs to synchronize the UE, PDN session, and bearer state so that upon taking over the IP address of the primary S-GW, the secondary S-GW can restore full state upon switchover using slight modifications to its call flows. A successful switchover is transparent to the P-GW and MME.

When the S-GW receives control messages on S11, it sends DDN to the MME with special cause code #254 to restore S1-u DL path and the UE is ready to process control plane or data plane traffic. When the MME receives the DDN message with a special cause code, it responds with the DDN acknowledge message to the S-GW for connected UE; however, for the idle UEs, the existing approach is applied.

The MME also sends the Modify Access Bearer Request message to S-GW by sending all of the PDN session data in one message. The S-GW uses the normal DDN when the S-GW did not experience a geo-redundancy failover, that is, the S-GW that was involved in the attach or handover of that UE's PDN sessions. The S-GW sends the cause code #254 in the DDN packet only when the S-GW is newly active. This is an indication to the MME to respond with a Modify Access Bearer request if the MME is aware that the UE is already active. If not, the normal paging is followed.

The feature improves user experience through session continuity during S-GW failover.

This feature requires the S-GW to send special cause value #254 in DDN to the MME.

18.7.7 MME support for DDN Ack for abnormal S-GW geo-redundancy switchover (Feature f10188-01)

This feature releases the stuck UEs on the old S-GW pair and cleans them up before any pages can succeed those UEs.

During a normal S-GW geo-redundancy switchover, the newly active S-GW sends the dynamic domain names (DDNs) with cause value #254 to trigger the MME to provide information to help the S-GW refresh its information regarding the UEs. There are also some S-GW geo-redundancy switchover scenarios, involving network issues, that result in the relocation of the UEs to a completely different S-GW pair, using the same Tunnel End Point Identifier (TEID), before the old pair completes the switchover. When the old pair completes its switchover, the newly active S-GW of the old pair sends the DDNs to the MME for those UEs, even though it has been long since those UEs were relocated to another S-GW pair. In such scenarios, the old S-GW sends the correct TEID to the MME in the DDN from the wrong S-GW. Without this feature, the MME ignores those DDNs and does not respond with a DDN Acknowledge message. This results in stuck UEs on the old S-GW pair and requires manual intervention by the operator to clean up before any pages can succeed for those UEs.

With this feature, when the MME gets a DDN with cause value #254, and if the TEID is recognized but the DDN is from the wrong S-GW, the MME responds back, with a DDN Acknowledge message, with a TEID of value 0, with the same sequence number as it is in the DDN, and with a cause value of #64 Context not found, back to the sending (wrong) S-GW. In this case, the S-GW cleans up automatically.

18.7.8 IMSI range-based routing to the HSS (Feature m11008-01)

The *IMSI range-based routing to the HSS* feature enables operators to spread S6a load across multiple HSSs based on IMSI ranges. Increase network resilience and reliability with HSS primary/secondary configuration.

The MME performs HSS/DRA selection based on whether IMSI range-based mapping is provisioned or not. If no provisioned IMSI mapping exists, selection is based upon whether the UE has a home PLMN or roaming PLMN.

- For each defined PLMN on the MME, one IMSI to HSS rule of type `ALL` without a range defined (without IMSI MSIN minimum and maximum values) is recommended as default rule.
- If there is no ALL rule defined on a PLMN, then UEs on that PLMN are rejected by default.
- If the default IMSI to HSS rule created load balancing is not enabled (`loadBalance` is `none`), the HSS/DRA entities in an HSS group are considered 1 primary, 2 secondary, 3 tertiary, then 4-16 as n-ary HSS (or DRA) entity.

The *IMSI range-based routing to the HSS* feature requires configuration (command `imsiToHss`).

Example

For special PLMN1, only a specific set of IMSI needs access to services (i.e. by MSIN range). For this PLMN1, do not define an ALL PLMN rule, only define one or more ALL RANGE rules: then all UEs in PLMN1 are rejected by default. Only the UEs that have an IMSI matching one or more ALL RANGE rules defined on PLMN1 are accepted, and allowed to route (through their associated HSS groups).

18.7.9 Diameter connections with load balancing (Feature m11320-01, f11304-01)

The *Diameter connections with load balancing* feature enables operators to spread S6a load across group of up to 16 HSSs/DRAs based on configurable weight factors.

HSS/DRA group load balancing

The MME supports load balancing per HSS group between up to 16 home subscriber servers (HSS or DRA) in an HSS group. The load balancing algorithm is selected per IMSI to HSS rule. The HSS groups provide the infrastructure for load distribution of S6ad diameter traffic to an HSS group, using random spread.

A weight factor from 0 through 100 can be applied to each HSS in the HSS group.

The zero-weight factor is used to evenly and randomly distribute load among remaining available HSSs, only when all nonzero weighted HSS are unavailable (creating a default fallback group).

Messages within the same UE procedure go to the same HSS or DRA. Load balancing is enabled for an IMSI range or for all UEs in a PLMN, if no IMSI range is specified. Load balancing applies to both MME (S6a) and SGSN (S6d), and is supported over the S6ad

interface.

IMSI to HSS rule load balancing modes

The following load balance modes are supported:

- When the load balancing option on an IMSI rule is set to `none` (default), the n-ary HSS/DRAs are treated in the n-th order priority. For example, the secondary HSS/DRA (order number 2 HSS/DRA in the HSS group) is used for S6ad traffic only when order number 1 HSS/DRA in HSS group is not available.
- When load balance is set to `all`, HSS/DRAs with nonzero weight are treated as one primary HSS/DRA set with S6ad messages distributed in accordance with relative weights (the greater weight receives more traffic; HSS/DRA with identical weight get message traffic evenly distributed among them), a secondary HSS/DRA set is defined by the remaining HSS/DRA having a zero (0) weight value. The secondary HSS/DRA set gets S6ad traffic evenly distributed among its HSS/DRA members only when the primary group is completely unavailable (all non-zero weighted HSS are unavailable).
- When load balancing is set to '`priority_group`', a set of HSS/DRA is defined in a group with different weights.
 - The set of HSS/DRA with the same highest weight form the primary group used in load balancing.
 - The set of HSS/DRA with the next common highest weight form the secondary group used in load balancing
 - The secondary group is only used for call processing when the primary group is out of service, for example (providing one or more fallback groups).

Interworking with HSS/DRA retry different HSS/DRA

Load balancing interworks with the *HSS/DRA retry different HSS/DRA* feature as follows: When an HSS/DRA responds with a specific error or times out, the next available HSS/DRA from the load balance selection is retried.



Note:

The MME does not require that all weights add up to 100. It allows any integer between 0-100 and then computes the actual weight percentage based on the provisioned weight on each HSS/DRA in an HSS group.

When load balancing is disabled, the HSS/DRA that is currently active and has the lowest order is selected as a primary link. All the messages are routed to the primary link until it is

no longer active, and then the next active link with the next order number is used. When the HSS/DRA *retry different HSS/DRA* feature is enabled, the secondary link is retried when the HSS/DRA on the primary link responds with a specific error or times out. The HSS/DRA retry feature is only applicable to S6ad (Diameter S6a and S6d applications).

In relation to the HSS retry with load balancing, before the introduction of load balancing, the MME retries S6a message to the next HSS (HSS1->HSS2->HSS3->HSS4,->HSS5,->HSS6). However, with the inclusion of load balancing functionality, retry works the following way. If there are 2 HSSs and if the first HSS attempt fails, then the second HSS is used. Otherwise, a random number and weight factor is used to select an HSS if the selected HSS is different than the first attempted HSS.

Related descriptions

- [MME support for basic DRA \(Feature m11307-01\)](#)
- [Enhanced DRA support \(Feature m11303-01\)](#)
- [HSS retry](#)

18.7.10 HSS retry

To mitigate UE-specific failures, the MME supports a service-provider provisioned option to perform HSS retry on an alternate link.

The MME may perform HSS retry on an alternate link during the following MME-HSS sub-procedures

- Authentication (utilizing the Authentication-Information-Request (AIR) / Authentication-Information-Acknowledge (AIA) commands)
- Update location (utilizing the Update-Location-Request (ULR) / Update-Location-Acknowledge (ULA) commands)
- Notify Request (NOR) command
- Purge UE sub-procedure, that is, Purge-UE-Request (PUR) command

The global parameter `s6aRetryDifferentHss` controls HSS retry. By default, it is set to No (disabled).

When the functionality is enabled,

- Any new authentication, update location, notify request, or purge UE request procedures executed without the history of HSS always goes to the primary HSS, which is the first one provisioned in Diameter connection for home PLMN.
- Upon AIA, ULA, NOA, or PUA timeout, or one of the following diameter errors, a different

HSS is retried and selected if retry succeeded.

- DIAMETER_TOO_BUSY
- DIAMETER_OUT_OF_SPACE
- DIAMETER_UNABLE_TO_DELIVER
- If the primary HSS becomes available, the MME goes back to using the primary HSS.
- Only one retry is attempted. If the retry fails, the internal (AIR, ULR, NOR or PUR) procedure will fail (the overall procedure might be failed for AIR and ULR). The primary HSS is selected for the next procedure if it is available.

By default, HSS retry is disabled. When HSS retry is disabled,

- Even if multiple HSSs are defined, only the first HSS available (link Enabled) is selected.
- If a timeout occurs or one of above three diameter errors received in AIA, ULA, NOA and PUA, no retry is attempted.
- The feature *Diameter connections with load balancing* has the following impact to HSS retries:
If there are 2 HSSs and the first HSS attempt fails, the second HSS is used, otherwise a random number and weight factor is used to select an HSS.

Under the following scenarios, the MME does not send the ULR to HSS for service request, S1 release, and downlink data notification (the MME still sends ULR to HSS for other procedures):

- Receipt of RSR from the HSS
- Software update
- Failure to process Insert-Subscription Data Request (IDR)/Delete-Subscriber-Data Request (DSR)
- Receipt of NOA with DIAMETER_ERROR_UNKNOWN_SERVING_NODE.

The term *HSS retry* means *S6A retry different HSS*, *S6A retry different DRA* or *HSS*, or *HSS/DRA retry different HSS/DRA*, and also since MME supports mixed mode, some DRA retry and/or some HSS retry are all supported.

With EIR, both *S13 retry different EIR* and *S13 retry different DRA or EIR* are supported and in mixed mode as well.

When feature *MME support for same SCTP association to DRA and higher peer count* (f11304-01) is enabled, Diameter combines S6A and S13 (and SLG), and then the *HSS retry* feature, when enabled, provides retry to DRA over S6A and S13 (not SLG), and retry both HSS and EIR in mixed mode. With f11304-01 enabled, S13 retry different EIR (DRA) is not used.

Related descriptions

- [Diameter connections with load balancing \(Feature m11320-01, f11304-01\)](#)

18.7.11 Multiple IWSs for same MSC ID (Feature m20103-02)

The *Multiple IWSs for same MSC ID* feature addresses the MME supporting maximum of two standalone IWSs for the same MSC ID.

The messaging that is exchanged across S102 interface must stay on the same MSC/IWS path.

The two IWSs do not share information and they are completely separate systems. Therefore, once the MME selects an IWS for a given UE, all messages associated with that UE remain on that same connection.

If a link is lost to the primary IWS, the MME switches to another link.

In addition, the MME also supports load balancing and failover for multiple or a pool of IWSs for the same MSC ID.

The MME verifies the sanity of the IWS and the link using the heartbeating signaling message.

In more detail, the MME supports a maximum of 2 IWSs across the S102 interface.

Upon selecting an IWS for a given UE, the MME keeps the associated messages with the UE on the same connection. However, if a link is lost to the primary IWS, the MME switches to another link.

The MME uses round robin approach for the load balancing between multi (2) IWS per MSC ID.

The MME verifies the sanity of IWS and the link by sending heartbeating signaling message. Heartbeating between two elements is performed to verify the sanity of the peer element and the links. After 12 consecutive heartbeat messages go unacknowledged, that is, no signaling heartbeat acknowledge is received from the IWS, the link is marked as disabled. The heartbeat frequency is provisionable. There is an existing provisioning capability prior to this feature. When a link has become disabled and subsequently the MME sends the heartbeat and receives the heartbeat acknowledgement, the link is marked as enabled. The heartbeat timeout range is 1 to 300 seconds with granularity of 1 and a default value of 15.

When the MME receives a message from the IWS on the S102 interface, which can be any message, that is, signaling/heartbeat/ack, it just indicates that the IWS is up and running.

The status of the interface is changed from disabled to enabled. The MME always establishes/re-establishes the connection when S1AP CDMA 2000 message from a UE is received and contains the Reference Cell IE.

When the MME detects a link failure with the IWS, that is, when heartbeat towards the IWS fails, the MME removes all S102 UE-specific information for the affected UEs.

The MME can be provisioned with a map of 1x MSC ID to the IP address of a particular 1xCS IWS entity. The MSC ID is a 3-octet value. The MME can also be provisioned with the name assigned to the 1xCS IWS entity. There is an existing provisioning prior to this feature. For each 1xCS IWS IP address entered into the MME provisioning, a boolean value is also provisioned to indicate whether or not the MME exchanges heartbeat messages with the IWS. If the boolean value provisioned for an IWS is set to False, that is, no heartbeat is exchanged with this IWS, then, a further provisioning parameter is added to indicate the timeout value after which the MME sets the Availability status attribute state - Degraded status attribute to True for the interface MO for that IWS. The timeout value is between 15 seconds and 5 minutes, with a granularity of 15 seconds, and a default value of 30 seconds. The operator is allowed to indicate that no time limit is placed on the receipt of an Ack from the IWS. The MME can be provisioned to allow up to 96 links to 1xCS IWS entities.

The feature increases network resilience and reliability through load sharing and primary/secondary configuration.

The *Multiple IWSs for same MSC ID* feature requires configuration.

18.7.12 CLI-triggered MSS SGs offloading (Feature f11802-01)

The *CLI-triggered MSS SGs offloading* feature enables operators to offload MSC/VLR when in pool, for example, due to maintenance activity.

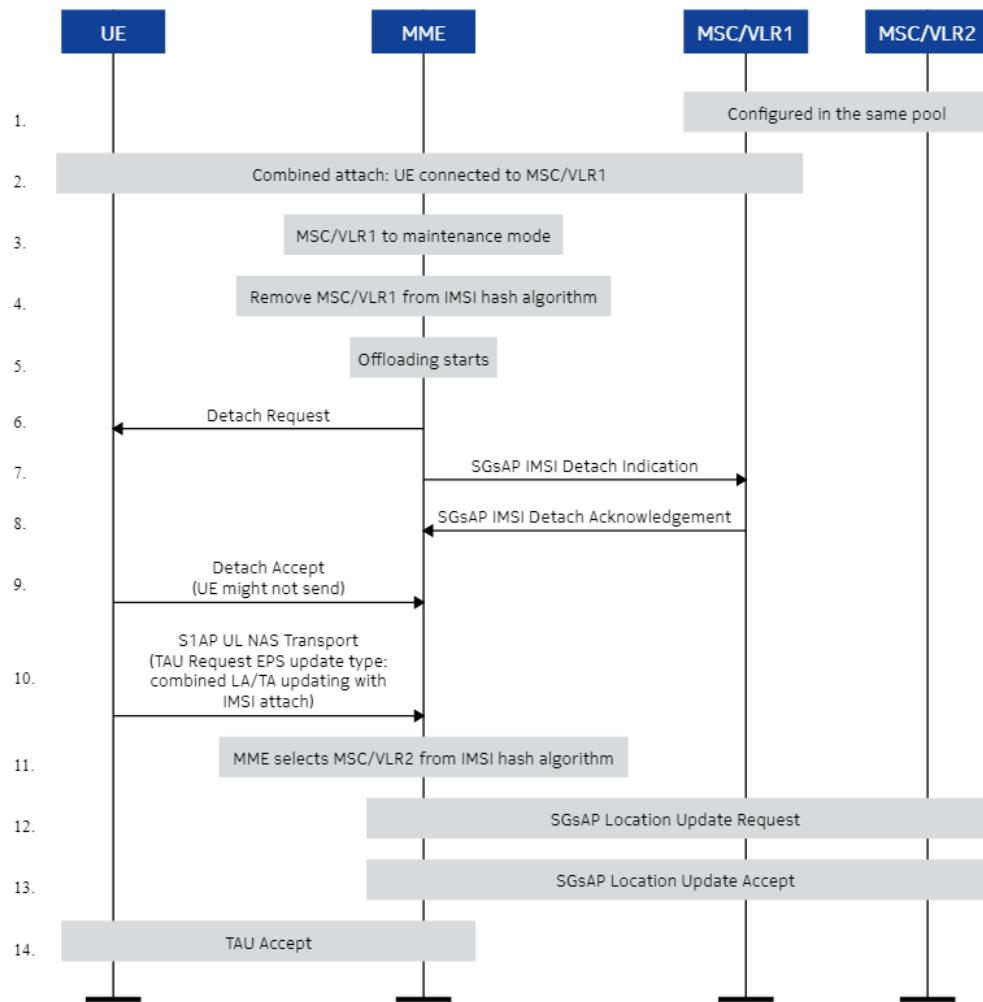
Subscribers attached to an MSC/VLR are offloaded to another MSC/VLR in the same MSC/VLR pool once the offloading command is issued. In order to avoid the system load, subscribers attached the MSC/VLR are IMSI detached in controlled way.

The MME sends detach request with type IMSI detach to the UE. This causes the UE to trigger tracking area update procedure message with EPS update type IE indicating combined TA/LA updating with IMSI attach. As the MSC/VLR is marked in maintenance mode, it is not included in the IMSI hash algorithm or round-robin selection. A new MSC/VLR is selected during the next tracking area update procedure.

IMSI detach is triggered at a rate specified by the configured UE offload rate.

The detach procedure is carried out as follows:

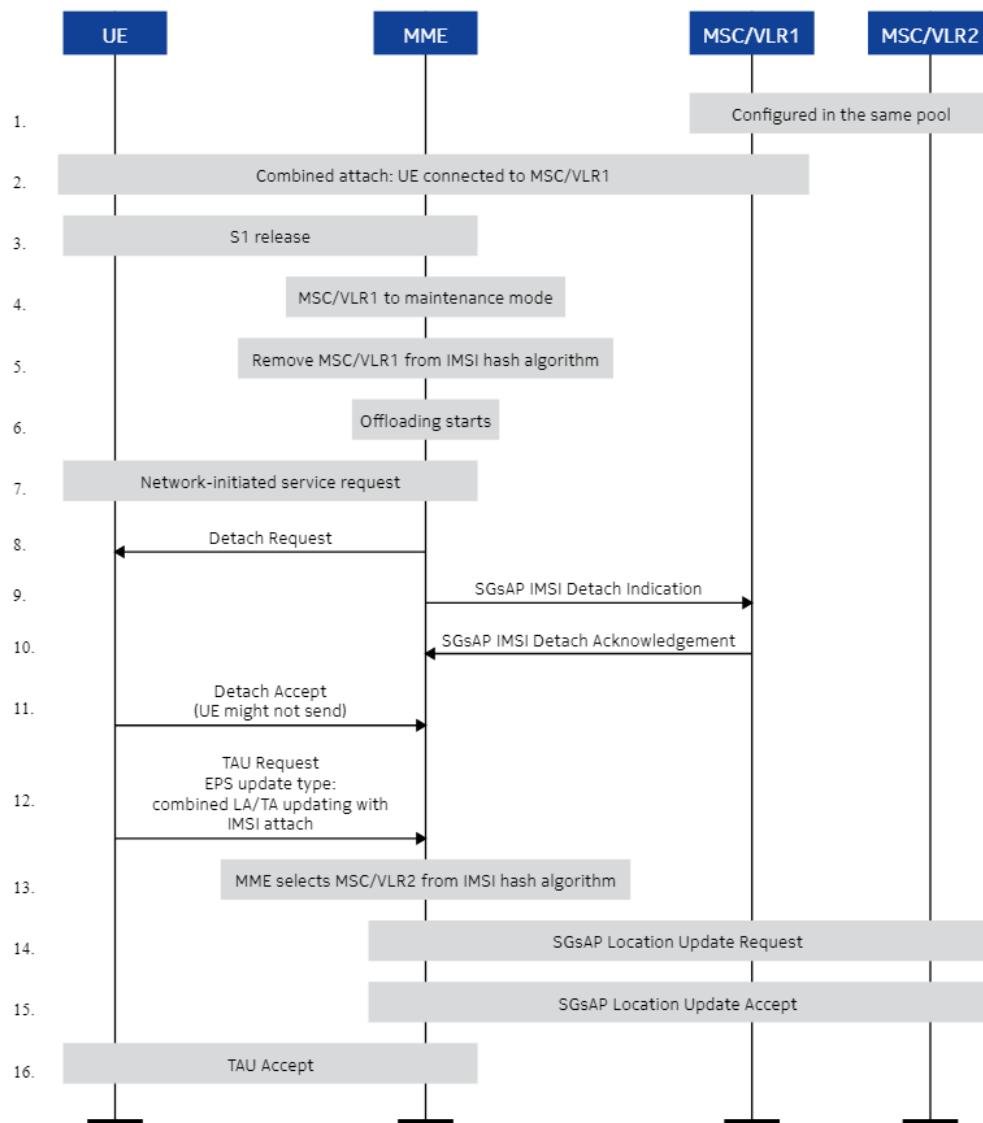
Figure 169: Signaling flow of MSC/VLR offloading when UE is in ECM-CONNECTED state



- MME sends a detach request message with the detach type IMSI detach.
- The VLR that is marked in maintenance mode is not included in the IMSI hash algorithm and as part of the combined TAU the MME selects another MSC/VLR from the same pool.

MME triggers the network-initiated service request procedure and once the UE is in the ECM-CONNECTED state, it follows the steps as above.

Figure 170: Signaling flow of MSC/VLR offloading when UE is in ECM-IDLE state



Command-initiated MSC/VLR offloading must be performed when there is no ongoing MME offloading or the subscriber moves to another MME in the pool. If there is any such activity ongoing, an error is displayed when you use the offloading command for subscriber offloading from the MSC/VLR.

The ongoing command-initiated MSC/VLR offloading procedure is cancelled if MME offloading is triggered.

18.7.12.1 MSS SGs offloading collision handling

The MME handles the network-initiated IMSI detach procedure (as part of the SGs)

offloading procedure) collision cases.

Ongoing procedure other than the network-initiated IMSI detach procedure (as part of the SGs offloading procedure) - incoming network-initiated IMSI detach procedure (as part of the SGs offloading procedure)

If a procedure other than the network-initiated IMSI detach procedure (as part of the SGs offloading procedure) is ongoing and there is an incoming network-initiated IMSI detach procedure (as part of the SGs offloading procedure):

- If a new VLR is not reselected or the SGs state is not made as NULL as part of the incoming procedure, the MME completes the ongoing procedure and then continues the network-initiated IMSI detach procedure (as part of the SGs offloading procedure).
- If a new VLR is reselected or the SGs state is NULL as part of the incoming procedure, the MME drops the incoming network-initiated IMSI detach procedure (as part of the SGs offloading procedure).

Ongoing procedures when the subscriber has a connection to the offloaded MSC/VLR

- the UE is not in a procedure.
- the UE is during periodic or combined TAU.
- the UE sends MO SMS.
- the MSC initiates MT SMS by sending paging message.
- X2HO and S1HO without MME relocation is completed.

If a UE is not offloaded during or immediately after the completion of the procedure, the MME offload manager offloads:

- service request procedure.
- extended service request procedure.
- UE initiated session management procedure.
- network initiated session management procedure.
- GMLC initiated requests.
- HSS requests.

If a UE is in EMC-IDLE state, the MME offload manager initiates a paging procedure to get the response from the UE and immediately offloads the UE without completing the service request procedure.

Pending IMSI detach procedure with other incoming procedures

MME handles collision of network requests while waiting for UE response for IMSI detach:

- If there is an incoming GW request message, the MME drops the request.
- If there is an incoming GMLC request message, the MME drops the request.
- If there is an incoming HSS request message, the MME uses the current handling of the request.
- MSC requests are not expected as the MME sends detach message to both MSC and UE simultaneously.

MME handles UE mobility management requests as specified in *3GPP TS 24.301*.

MME handles collision of X2HO and S1HO without MME relocation after the handover procedure is completed:

- If a TAU is expected, the MME offloads the UE as a part of the TAU requests that follow the handover procedure.
- If a TAU request is not expected, the MME resends the IMSI Detach Request message,

18.7.13 MME support for passive offloading (Feature f10710-01)

The **MME support for passive offloading feature enhances the UE load balancing in such a way that once the MME is drained of UEs, it remains fully connected to RAN with enabled S1-MME links but with relative capacity set to zero.**

The MME continues to move the new UEs, which attempt to access the MME for any reason, to other MMEs in the pool through load balancing TAU for as long as the MME remains removed from the pool. This avoids a condition in which the alarms are raised in the RAN and avoids having any UEs being provided service from the MME that has been removed.

 **Note:**

When the already offloaded UEs try to reconnect to the same MME, the attach TAU and the service request procedures are rejected. For this reason, it is recommended that the eNBs are connected to more than one MME in a pool when the passive offload feature is enabled.

The passive offloading functionality is enabled or disabled via `passiveOffload` parameter. By default, the parameter is disabled.

Certain interactions of passive offloading functionality with UE load balancing out of local MME (LTE only) are given below:

- Passive offloading can be enabled in the middle of the the UE load balancing. Actions of the UE load balancing take precedence over those of passive offloading. Since the MME sends the MME configuration update message with relative capacity set to 0 to all connected RANs at the start of the UE load balancing, this action is omitted for passive offload. Once the UE load balancing is completed, the action to send the MME configuration update message with the MME relative capacity of zero to RANs is omitted as passive offload is enabled in the MME.
- The UE load balancing can be enabled out of the local MME (LTE only) in the middle of passive offloading. At the onset of passive offload, the MME sends the configuration update message with relative capacity of zero to all connected RANs, this action is omitted when the UE load balancing is started in the middle of the passive offload. Also, once the UE load balancing is started, actions related to UE load balancing takes precedence over those of passive offloading.
- When the UE load balancing ends, the actions of passive offload resume.

18.7.14 Directed UE moved by TA (Feature f10711-01)

The directed UE moved by TA feature supports offloading of 4G UEs selected by last seen tracking area from one MME to another specified MME within the same pool.

Tracking areas and tracking area lists can be configured by using the `cmm tailist create` or `cmm tailist modify` commands. Once the UE load balancing is started, the list cannot be modified any more. The UE load balancing may contain up to 3 TAI lists. Up to 300 TAIs can be added among all the configured TAI lists.

When using directed UE moved by TA feature, operator can not choose to lock or quarantine the MME upon completion of UE load balancing.

All UEs whose last seen TAI matches the configured TAIs are offloaded.

The operator can not choose to offload a certain fraction of UEs with this feature.

18.7.15 Relative capacity calculation enhancements (Feature f71001-12)

This feature enhances the relative capacity calculation to consider that the limiting factor on relative capacity needs to take into account both the CPPS and IPDS capacity.

With this feature, a service provider can specify the number of spare CPPS VMs (protected CMM VMs) that are not considered when calculating automatic relative capacity. The `numProtCPPS` parameter of the `cmm mmeGrpNode` command specifies the number of spare CPPS VMs `K` that are not considered when calculating auto relative capacity.

The setting for the `numProtCPPS` parameter must be equal to or less than the `total number of CPPS instances` - 1. This parameter is considered the `K` value in the N+K sparing arrangement; it is used only when the `autoAdjustCap` parameter is set to `true`. In addition, the `numProtCPPS` parameter is set only when the command is executed for the home network.

For non-appliance CMMs, provision the `numProtCPPS` parameter based on the N+K used in your CMM design. For small configuration, supported N+K sparing configurations are 2+2, 1+1, or 2+1.

Appliance CMM supports the following N+K sparing configurations:

Table 79: CPPS N+K sparing

Appliance	Configuration	Airframe	CPPS N+K
CMM-a8	MME	RM17	10+10
CMM-a8	MME	RM18	10+4
CMM-a8	MME/SGSN	RM17	8+2
CMM-a8	MME/SGSN	RM18	10+4
CMM-a2	MME/SGSN	RM17	not supported
CMM-a2	MME/SGSN	RM18	1+1
CMM-a2	MME	RM17	2+2
CMM-a2	MME	RM18	2+2
CMM-a2	AMF	RM18	2+2

Following are the impacts to relative capacity calculation when the `numProtCPPS` parameter is set.

- The CMM weight factor is six for each of the N CPPS instances. The nominal relative capacity is the weight factor (6) multiplied by the number of non-K CPPS instances ($6 \times N$). For example, if the total number of CPPS instances is 9 and the system indicates that there is one K CPPS instance, the nominal relative capacity is 48 (6×8). For CMMA2, the weight factor is 6 for each of the N (2) CPPS instances, so the total nominal relative capacity is 12.
- When the number of failed CPPS instances is greater than the value of K, relative capacity is the weight factor multiplied by the number of remaining CPPS instances. For example, when $N+K$ is 9 and $K=1$, if two CPPS instances fail, relative capacity is 42. The value resets to 48 when one CPPS instance recovers.
- When one CPPS instance is scaled-out, relative capacity is recalculated. If the number of K CPPS instances remains the same, the relative capacity is increased by 6.
- When one CPPS is scaled-in, the relative capacity is recalculated. If the number of K CPPS instances remains the same, relative capacity is decreased by 6.
- If the scale-in or scale-out corresponds to a change in the K value for CPPS instances, relative capacity is not changed.
- When the CMM relative capacity is calculated, the number of IPDS pairs is also considered. If there are one or two IPDS pairs, relative capacity is limited to 60 (10×6), regardless of the number of N CPPS instances. For example, if a CMMA8 is configured with the CPPS sparing method of 16+4, the nominal relative capacity is 96 (16×6), but since there is only one IPDS pair, relative capacity is limited to 60. In this scenario, there would have to be 11 failed CPPS instances before the relative capacity changes to a value less than 60. For three IPDS pairs, relative capacity is limited to 120; with four IPDS pairs, relative capacity is limited to 180.

The eNBs obtain the corresponding MME relative capacity either through an S1 Setup Response or MME Configuration Update message.

18.7.16 UE load balancing compatibility (Feature f10712-01)

This feature makes it possible for the CMM to perform Flexi Network Server (FNS) style UE load balancing (UELB) in a network which has both FNS and CMM in it. It also allows the CMM to support FNS directed move which results in reattach. The scope of the application is per FNS.

Flexi Network Server style of directed UELB involves setting bit 7 in a FNS assigned GUTI

MTMSI to 1 to indicate the UELB. The target FNS assigns other items, including part of the MMEC and part of the GUTI. Then the UE is detached. The FNS checks bit 7 to know that the attach request is received as the result of UELB, and immediately sends NAS identity request to the UE to retrieve IMSI information.

In the CMM, bit 7 of the GUTI MTMSI is used as a way of handling restart counter. This function is recommended in the standards. To maintain current CMM GUTI handling and provide FNS UELB compatibility, additional provisioning is required.

If the CMM is the source MME where the UELB command is executed from, the CMM generates a fake MTMSI to use in the GUTI of which the bit 7 MTMSI value has been set. This value is sent to the UE to be detached in the procedure. This allows a receiving FNS to recognize the request resulting by the UELB.

If the CMM is the target MME and a global parameter is set to indicate that the network has both the CMM and the FNS in pool, the CMM sends the NAS Identity Request message to the UE whenever the CMM receives a GUTI that bit 7 is set in the Attach Request message.

18.7.17 UELB enhancements for soft offload of UE (Feature f10710-02)

This feature enhances the handling of emergency and non-emergency calls during UE load balancing (UELB).

For this feature, in contrast to the current UELB method, the MME waits for the eNB-initiated UE context release with "user inactivity" to offload an ECM-CONNECTED UE by sending the UE context release command with "Load balancing TAU required".

For ECM-IDLE UE, the MME pages the UE to trigger UE to transition to ECM-CONNECTED state and wait for eNB-initiated UE context release to offload the UE.

The scheme is applied to emergency, high priority and non-emergency UE. The MME controls soft offload rate to not cause overload of other network elements such as the HSS.

The feature enhances the current UELB and passive offload functionalities as follows:

- New options are added to allow the UE to be offloaded by initiating the offload procedure upon reception of a context release request with cause code = user inactivity. For the idle UE, the CMM pages the UE to bring it in connected state and then waits for the user_inactivity request to be received.
- For the VoLTE UE, the node initiates the relocation upon deactivation of the bearer with QCI=1.
- For the former and new UELB, the handling of the emergency calls is modified: in pre-

release 20, emergency calls were not relocated and the only option available to the customer is to pause or to lock the MME (in which case the emergency calls are lost); if pause option is selected, manual monitoring of the emergency call is needed.

- The new UELB relocates UE involved in either emergency or high priority (HP) session upon autonomous termination of the emergency/HP session or they will be relocated before the lock operation (if requested) is performed.
- The new UELB allows to create a dedicate “paging” policy exclusively for use during UELB procedure. The former UELB only allows to specify the maximum number of attempts for paging procedure initiated by the CMM to relocate the UE; basic paging policy is used in regard of paging strategy and timers.
- The new functionality allows to define besides max number of attempts, the paging strategy and the values of timers to be used only during offload procedures per serving PLMN.
- This feature also allows to define the max rate that can be reached during the offload procedure (number of UEs relocated per second per CCPPS). This control is made available for both UELB and passive offloading.
- VLR scan frequency has been doubled: from one fetch every 2 seconds to 1 fetch every second.
- Finally, it is possible to specify which UE type can be fetched from the DBS during the fetch from DBS phase in UELB (that is only active if lock option is selected, as in former UELB). Four options are available: none, all, nbio, mbb.

18.8 System/process reliability

Features providing system-internal problem detection and recovery.

18.8.1 CMM support for using REMc (Feature f70012-03)

With this feature, services (such as the CPPS, the IPPS, and the PAPS) are connected to the redundancy manager control (REMc) process on the NECC to control the state of the service. In addition, for duplex REM-controlled services, the redundancy manager (REM) controls which one of each pair is active and which one is standby.

REM-controlled services provide their states to the REM and receive state updates.

REM-controlled services send messages (heartbeats) to the REM at a regular interval. If the REM sees the heartbeats stop arriving from a service, it assumes that the service is down and tries to recover it. Each REM-controlled service has a provisionable REM timer which is

the time between TCP heartbeats. Services other than PAPS have the following default timers:

- 200 ms between heartbeats on the VNF
- 600 ms on the CNF

The default PAPS REM timer is 200 ms on both the VNF and the CNF. The REM timers have "RemHeartbeat" in the name along with the name of the service (such as, ipdsRemHeartbeat).

Normally, there is no need to change the REM timer values unless the CMM Support recommends it.

18.8.2 Full/partial IP isolation detection (Feature f70012-05)

This feature increases system reliability by improving the detection of IP isolation of VMs. It also allows SGSN processes to know the statuses of other processes more quickly, reducing call processing impact of process failures.

This feature supports detection and recovery from full or partial IP isolation.

Each VM monitors the IP communication paths to determine if the VM is isolated from the system. The isolation is based on a five-second timing interval by default.

When a VM is declared IP isolated, it reboots and waits for recovery from isolation. At recovery of IP communications with the NECC (REM_c), the VM process completes the recovery by heartbeating with REM_c and following recovery actions.

With this feature, PAPS and NECC processes use notifications from REM to know the states of other processes, and PAPS processes report their states to REM. IPDS, DBS, CPPS, IPPS already used notifications from REM and reported their states to REM.

Timer `internalIpIsolationThreshold` controls internal IP isolation detection. The default value of 5 seconds is usually sufficient. A timer value of 0 means that the IP isolation is turned off: no IP isolation analysis or actions will be taken.

19. Interface/Link management

These features provide flexible configuration of external interfaces.

19.1 IP address management

Features supporting IP address sharing.

19.1.1 Same IP address for S6a and SLg (Feature m11310-01)

The *Same IP address for S6a and SLg* feature supports use of the same far end IP address for S6a and SLg interfaces (with different remote port used for S6a and SLg) when both interfaces share the same GigE interface.

The MME provides configuration of separate SCTP ports for S6a and SLg interfaces when the same remote IP address is used.

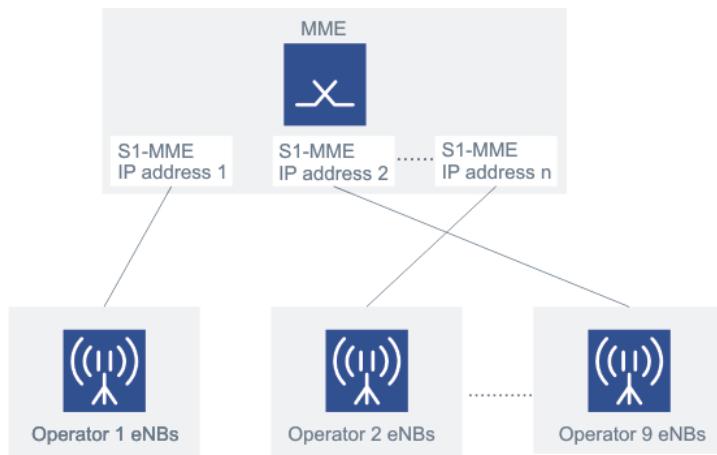
19.1.2 Multiple S1-MME local IP addresses (Feature m10910-01)

The *Multiple S1-MME local IP addresses* feature supports multiple local IP addresses for the S1-MME interface to facilitate segregation of eNB S1-MME traffic.

For example, in the case of network sharing, all of an operator's eNBs can use one of the IP addresses and all of a different operator's eNBs can use a different IP address to keep their S1-MME traffic logically separate.

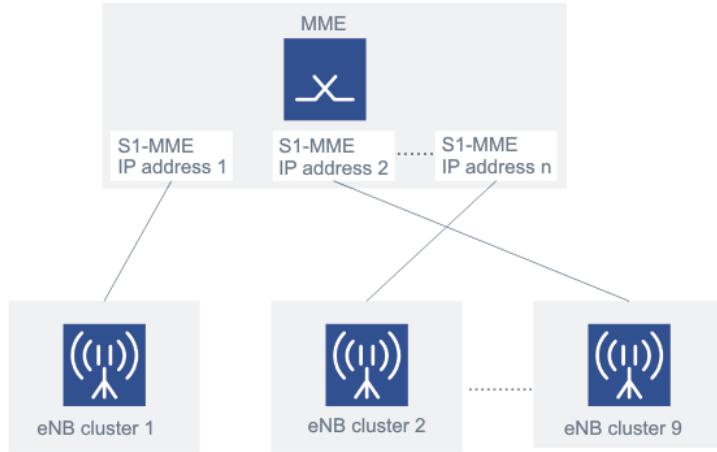
The figure illustrates use of multiple IP addresses to segregate traffic of eNBs of different PLMNs when MME is shared (for more information, see [Network sharing](#)).

Figure 171: Use of multiple S1-MME IP addresses to segregate traffic to eNBs of different PLMNs



Another example of the use of this feature is clusters of the same operator's eNBs using different IP addresses. The term cluster is used here to describe a collection of eNBs in a geographical area for convenience (provisioning of a cluster does not exist on eNBs or on the MME).

Figure 172: Clusters of operator's using eNBs using different S1-MME IP addresses



For this feature the MME supports up to 9 local IP addresses. Additionally, this feature supports:

- provisioning of separate SCTP profiles for each S1-MME local IP address
- PM counts to monitor bandwidth usage for each local S1-MME IP address

The total number of eNB associations across all the local S1-MME IP addresses is limited by the maximum number of eNBs supported by the MME.

19.1.3 Multiple eNBs with the same IP address (Feature m10919-01)

The **Multiple eNBs with the same IP address feature allows multiple S1-MME connections to use the same IP address.**

In particular, where there is a HeNB GW implemented, multiple S1-MME connections each defining a virtual GW can be established with the MME using a single IP address.

19.1.4 Sv and SGs interface using the same remote endpoint IP and different port number (Feature m30102-06)

The **Sv and SGs interface using the same remote endpoint IP and different port number feature supports using the same endpoint IP address for both Sv and SGs interface.**

Some WCDMA MSCs use the same report endpoint IP address for both Sv and SGs interface. Prior to this feature, the MME expected different report endpoint IP addresses for each of these links. With this feature, the MME is able to set up separate links to the MSC for Sv and SGs logical interfaces using the same IP address.

19.1.5 S1-MME and M3 sharing the same IP with different ports (Feature m10432-01)

The **S1-MME and M3 sharing the same IP with different ports feature supports sharing the same local IP address for S1-MME and M3 interfaces.**

The MME supports sharing the same local IP address for S1-MME and M3 interfaces. It also supports the increase of M3 interfaces using the same IP address as the S1-MME links, without interrupting UEs in ECM-CONNECTED and ECM-IDLE state and also without interrupting call processing.

SCTP multi-homing is supported on both S1-MME and M3 interfaces. However, operators must use different SCTP ports for S1-MME interface (standards port # 36412) and M3 interface (standards port# 36444).

Operators must provision the same SCTP configuration (that is, MH or SH) for S1-MME and M3 when the IP address is shared.

19.1.6 IP address flipping for SGs and S6a interfaces (Feature m10432-02)

The **IP address flipping for SGs and S6a interfaces feature provides flexibility to flip the IP address for SGs and S6a interfaces.**

This feature incorporates the IP address flipping whereby if the MME has two remote SGs/S6a endpoints (EP1 and EP2) with same IP address pointing to one MSC/DRA, the MME supports the IP address flipping so that the primary IP address of EP1 is the same as the secondary IP address of EP2 and vice versa.

19.1.7 MME support for detection of S11 load balancer by IP address (Feature f10195-01)

An IP is determined to be a load balancer if the MME has received a Create Session Response message with a sender F-TEID for the control plane specifying a different IP address than the IP header.

If the MME subsequently receives a Create Session Response message from a load balancer IP and the fully qualified tunnel end point identifier (FTEID) matches the IP header, an S11 link/managed object is not created.

19.2 IP version support

Features enabling IPv4, IPv6, and dual stack support.

19.2.1 Bidirectional Forward Detection for dual stack (IPv4 and IPv6) (Feature m80140-06)

The **Bidirectional Forward Detection for dual stack (IPv4 and IPv6) feature supports reliable communication between the MME and other nodes.**

Bidirectional forwarding detection (BFD) is used to detect failures in communication with a forwarding plane next hop. It provides low-overhead, short duration detection of failures in the path. BFD supports both IPv4 and IPv6.

The MME also supports external IP manager – active connection management (EIPM-ACM)

and reliable static routing (RSR). EIPM-ACM provides fast fault detection for deployments with L2 connectivity between 1st hop routers. SCTP with multi-homing provides fast fault detection. This is only used with those interfaces that have SCTP on the protocol stack. Reliable static routing (RSR) uses address resolution protocol (ARP) and neighbor discovery protocol (NDP) to detect failures in communication with a forwarding plane next hop. RSR is typically used for the OA&M transport subnets. The goal of RSR is to provide low-overhead detection of failures in the path.

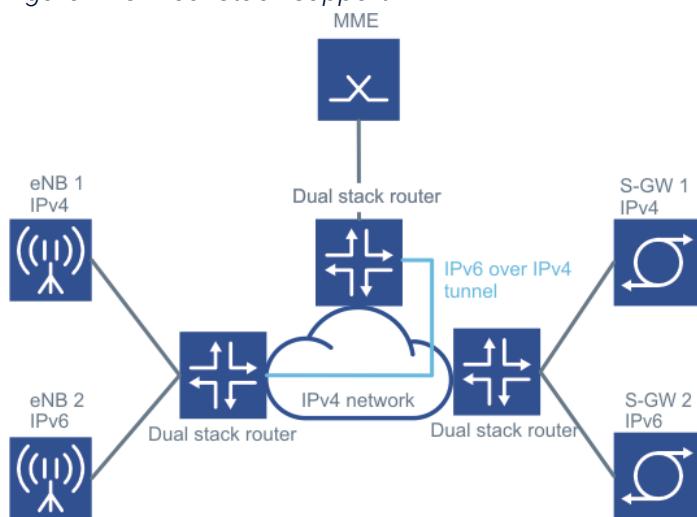
19.2.2 IPv4/IPv6 dual stack (Feature m10403-01)

The IPv4/IPv6 dual stack feature supports IPv4 and IPv6 stacks on the MME to enable the MME to communicate with IPv4-only nodes and IPv6-only nodes.

The support of dual stack on the MME provides a graceful migration to an all-IPv6 network. This feature supports IPv4 and IPv6 addresses for all the MME interfaces: DNS, NTP, SNMP, SSH, M3, S1-MME, S3, S6a, S10, S11, S13, S102, SBc, SGs, SGslite, SLg, SLs, Sm, Sv, X1_1 and X2. RS10 MME interface is IPv6 only. This feature also supports ICMPv6. The IPv6 is supported for OA&M interfaces and can be used for services such as SFTP.

The figure shows an example of supporting IPv4 and IPv6 nodes using an IPv4 network.

Figure 173: Dual stack support



In the figure, the MME is connected to routers that support both IPv4 and IPv6. The network shown is an IPv4 network and the IPv6 is carried over IPv4 tunnels between IPv6 nodes.

- The MME has an IPv4 address and IPv6 address for the S1 interface so that an IPv4 eNB can set up an SCTP association using the S1 IPv4 address and an IPv6 eNB can set up an SCTP association using the S1 IPv6 address.

- The MME is provisioned with S11 interface IPv4 and IPv6 addresses. In addition, the S-GW 1 IPv4 and S-GW 2 IPv6 addresses are provisioned on the MME.

19.2.3 IPv4, IPv6 implementation for ping/traceroute source based routing enhancement (Feature m10425-02)

The *IPv4, IPv6 implementation for ping/traceroute source based routing enhancement* feature supports source based routing to eliminate static routes for each and every MME interface.

This feature supports Linux policy based routing employed in the control plane to create a source-based rule for each resident subnet. Each rule points to a route table containing the next hop address for the subnet. Linux control plane script reads data plane information through `/proc/ippathmgt/ (v4localip, v6localip)` files.

This feature introduces a 30-second periodic audit that reads the data plane routing table and creates and/or deletes source-based routing in the control plane. This allows ping/traceroute work beyond the first hop router. There is no need to run `installRoutes`. This feature updates control plane routing as failure conditions arise dynamically within 30 s (that is, updated to match data plane routing with 30 s). Also, traceroute is updated to require system admin privilege. In this feature both IPv4 and IPv6 are supported.

19.2.4 MME support for IPv4/IPv6 dual stack transport for Gn (Feature f12101-09)

The support of IPv4v6 on MME provides the means for a graceful migration to an IPv4v6 network.

This feature removes the restriction that MME Gn interface could support only IPv4 version. The feature supports IPv4v6 dual stack and IPv6 only for the Gn interface.

The new Alternative GGSN Address for control Plane and Alternative GGSN Address for user traffic IEs are grouped in pairs. In the abnormal case where either one IE is not available, none will be included in the message.

19.2.5 CMM support for Gn dual stack (Feature f11810-01)

This feature provides IPv6-only GN capability to CMM and enhances functionality according to latest 3GPP TS 29.060 changes regarding to Alternative GGSN Address IE

handling.

The MME is optimized to support IPv6 only capability for the MME Gn control plane interface. Furthermore, through this feature, MME's functionality is enhanced to support proper handling of Alternative GGSN Address IEs in case of mobility over Gn towards SGSN through routing area update or handover procedure. MME's behavior is according to 3GPP TS 29.060 (GTPv1) CR#1062.

MME's rules for handling partial pairs of Alternative GGSN IEs:

- MME performs 1:1 EPS bearer to PDP context in case of mobility. MME populates Alternative GGSN IEs when sending SGSN Context Response (RAU) or Forward Relocation Request (handover) messages as stated in 3GPP TS 29.060 Rel.15.
- If an alternative IP address is available either for the control plane or for the user plane (but not both), a pair of Alternative GGSN Address for control plane IE and Alternative GGSN Address for user traffic IE is encoded; one of these IEs includes the alternative address and the other IE is set to a null IPv4 or IPv6 address (that is, 4 or 16 octets set all to zero).

Notes:

- The current version of 3GPP 29.060 (Rel-15) does not require to take into account the IPv6 capabilities of the target node for encoding the GGSN user plane addresses in the Forward Relocation Request and SGSN Context Response messages.
- The current version of 3GPP 29.060 (Rel-15) requires to take into account the IPv6 capabilities of the target node for encoding the GGSN control plane addresses in the Forward Relocation Request and SGSN Context Response messages.
- The relevant CR number for 3GPP 29.060 is CR#1062.

Example: 1 PDP context having an IPv4 GGSN address for control plane and IPv4 and IPv6 GGSN addresses for user traffic

The message encodes the IEs as follows:

- Alternative GGSN Address for control plane IE (null IP address);
- Alternative GGSN Address for user traffic IE (alternative IPv4 or IPv6 address to the one encoded in PDP Context IE).

Example: 1 PDP context having IPv4 and IPv6 GGSN addresses for control plane and an IPv4 GGSN address for user traffic

The message encodes the IEs as follows:

- Alternative GGSN Address for control plane IE (alternative IPv4 or IPv6 address to the one

- encoded in PDP Context IE);
- Alternative GGSN Address for user traffic IE (null IP address).

19.2.6 CMM support for IPv6 internal communication (Feature f12119-01)

This feature support the internal CMM communication over IPv6.

Operators have an option to use either IPv4 or IPv6 for internal CMM communication, but not dual stack. The choice is made as part of the cloud definition. At instantiation, Cloud_init creates an IPv6 or IPv4 network.

The CMM supports IPv6 internal network for service discovery, all applications and third party software.

 **Note:**

Virtual guest tagging and an internal IPv6 subnet (the CMM internal subnet used for IP communication between virtual machines) are not compatible. Configuring the CMM with virtual guest tagging and an internal IPv6 subnet may cause communication issues between VMs.

19.3 SCTP

Features supporting stream control transmission protocol (SCTP) association and multi-homing.

19.3.1 SCTP multi-homing (Feature m10402-07)

The *SCTP multi-homing* feature provides higher availability of the related logical interface and lower procedure failure due to poor backhaul performance.

This feature provides the support of SCTP local multi-homing and remote multi-homing on the following MME interfaces that use SCTP as the transport protocol: S1-MME, S6a, S13, SBC, and SGs. The SCTP multi-homing capability supports multiple SCTP paths between two SCTP endpoints. The goal is to increase the transport reliability between these two SCTP endpoints. To support local SCTP multi-homing, the MME must be provisioned with two

floating local IP addresses on these interfaces. For each interface, either IPv4 or IPv6 address can be provisioned, but mixing of IPv4 and IPv6 addresses on a given interface is not supported. This feature also supports the provisioning of up to two remote IP addresses for an SCTP peer. This is needed when the MME interfaces with a remote SCTP peer that supports remote SCTP multi-homing.

The stream control transmission protocol (SCTP) standard is specified in RFC.

The *SCTP multi-homing* feature requires support from peer nodes (S-MME/eNB, S6a/HSS, S13/EIR, SBc/CBC, and SGs/MSC).

19.3.2 SCTP multi-homing: S1-MME, S6a, SGs, SBc interface enhancements (Feature m10402-06)

The *SCTP multi-homing: S1-MME, S6a, SGs, SBc interface enhancements* feature provides higher availability of the related logical interface and lower procedure failure due to poor backhaul performance. This feature provides added benefit in flexibility of configuration.

With this feature the MME is able to support SCTP associations with local multi-homing or remote multi-homing or both on the S1-MME, S6a, and SGs interfaces. A maximum of two local multi-homing addresses per SCTP association is supported. When the MME is the SCTP client, the MME supports the provisioning of up to two addresses per SCTP association for a remote multi-homed SCTP peer.

When the MME as the SCTP client is setting up an SCTP association with a remote SCTP peer, the MME chooses its local IP addresses (IPv4 or IPv6) that match the IP address type (IPv4 or IPv6) of the remote SCTP peer.

With respect to single-homed (SH) or multi-homed (MH) SCTP endpoint, three configurations are supported:

- MME SH, remote SCTP peer SH
- MME MH, remote SCTP peer SH
- MME MH, remote SCTP peer MH

When SCTP local multi-homing is supported on an SCTP endpoint, an SCTP association consists of multiple paths at the local end; each path is terminated on a different physical port. If the remote SCTP endpoint also supports local multi-homing, then at the remote endpoint each path is also terminated on a different physical port. With SCTP multi-homing, if there is a network failure that brings down one path (for example, cable cut, router, or switch failure), the SCTP stack detects the path failure and switches to the other path; thus the SCTP association stays established unless both paths fail and the association

retransmission count is reached. In other words, a single SCTP path failure does not affect the communication between the two SCTP endpoints. For SCTP local SH and remote MH, the MME allows the association to be established as long as one of the derived remote IP addresses received in the INIT ACK chunk matches provisioned values.

When the MME successfully establishes an SCTP association to a remote SCTP multihoming peer over the S6a/SGs interfaces, if the addresses returned in the INIT ACK from the remote SCTP peer is different than the remote addresses locally provisioned on the MME, the MME generates an event notification to indicate mismatch between provisioned and derived (received from far end) IP addresses. The event notification includes the first (one or) two remote addresses in the INIT ACK chunk that are not locally provisioned on the MME and the number (up to 2) of remote addresses received.

Once the MME has successfully established an SCTP association with a remote SCTP peer, later the remote SCTP peer can perform an SCTP association restart by sending an INIT chunk to the MME on the existing association. If the INIT chunk does not add any new addresses, the MME processes the INIT chunk according to the SCTP association restart procedure per *RFC4960 section 5.2.4.1*. If the INIT chunk adds new addresses to the association, the MME responds with an ABORT as per *RFC4960 section 5.2.2*.

When the provisioned remote addresses of a remote S6a/SGs SCTP peer is added, deleted, or changed, the MME tears down the respective S6a/SGs SCTP association and recreates the SCTP socket and re-establishes the respective S6a/SGs/S13 SCTP association.

On the S6a/SGs interfaces, when the respective SCTP association does not exist, the MME establishes the SCTP association as follows:

- If the respective local end SCTP configuration parameter is set to SH and if the local SH address is not configured, the MME sends an event and checks periodically, until the local SH address is configured.
- If the respective local end SCTP configuration parameter is set to MH and if one or both local MH addresses are not configured, the MME sends an event and checks periodically, until both local MH addresses are configured.

On the S1-MME interfaces, when the listening SCTP socket does not exist, the MME creates the SCTP socket as follows:

- If the S1-MME local end SCTP configuration parameter is set to SH and if the local SH address is not configured, the MME sends an event and checks periodically, until the local SH address is configured.
- If the S1-MME local end SCTP configuration parameter is set to MH and if one or both local MH addresses are not configured, the MME sends an event and checks periodically, until both the local MH addresses are configured.

The *SCTP multi-homing: S1-MME, S6a, SGs, SBc interface enhancements* feature requires support from peer nodes (S-MME/eNB, S6a/HSS, S13/EIR, SBc/CBC, and SGs/MSC).

19.3.3 Provisioning of separate SCTP interfaces for SGs interface (Feature m10404-01)

The *Provisioning of separate SCTP interfaces for SGs interface* feature provides flexibility in setting different SCTP profiles for different SGs VLR entity that may each have different design limitations.

This feature supports provisioning profiles per SGs interface, expands range values for various SCTP parameters, and supports provisioning of a wait timer for initiating SCTP association establishment:

- Up to 6 SCTP profiles can be provisioned for the SGs NI types. The operator can assign any of the provisioned profiles to any SGs VLR entity.
- The SACK period parameter value range is 0 - 500 milliseconds
- There is a provisionable timer on the S6a interface for SCTP association reestablishment on receipt of a Shutdown command from the far end peer. The timer has a value range of 0 – 10 seconds in units of 1 second, and has a default value of 0 seconds.

SCTP multi-homing requires support from the SGs/MSC. This feature does not require any incremental peer node capability beyond that.

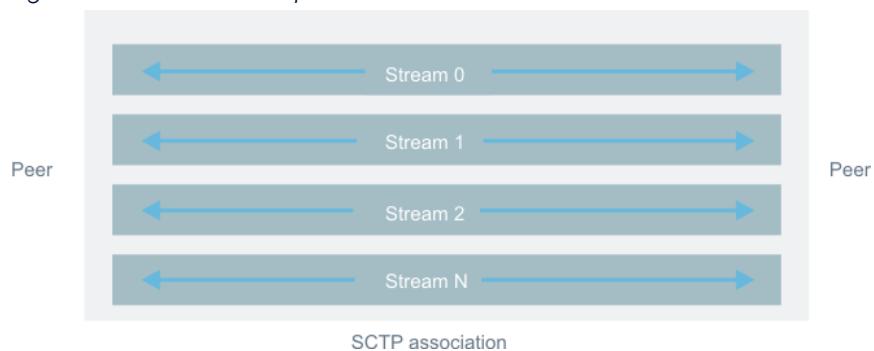
19.3.4 Multiple S6a streams (Feature m80300-02)

The *Multiple S6a streams* feature supports reliable communication between MME and other nodes.

This feature provides SCTP multi-stream support on the S6a (HSS) interface.

SCTP multi-streaming allows data to be partitioned into multiple streams that have the property of independently sequenced delivery, so that message loss in any one stream only initially affects delivery within that stream, and not delivery in other streams. At the same time, transport is done within a single SCTP association, so that all streams are subjected to a common flow and congestion control mechanism, reducing the overhead required at the transport level.

Figure 174: Relationship of an SCTP association to streams



In-order delivery of user messages is retained within each stream but not across multiple streams. However, reliable data transfer and congestion control is applied to the entire association. SCTP separates data transmission and data delivery. Specifically, each DATA chunk has two independent sequence numbers: a per-association transmission sequence number (TSN) and a per-stream stream sequence number (SSN). The TSN is used for data transmission including loss recovery, flow control, and congestion control while the SSN (along with stream ID) is used for the data delivery.

This independence of mechanisms allows the receiver to determine immediately when a gap in the transmission sequence occurs (for example, due to message loss), and also whether or not messages received following the gap are within an affected stream. If a message is received within the affected stream, there is a corresponding gap in the stream sequence number, while messages from other streams do not show a gap. The receiver can therefore continue to deliver messages to the unaffected streams while buffering messages in the affected stream until retransmission occurs.

The term stream is used in SCTP to refer to a sequence of user messages that are to be delivered to the upper-layer protocol in order with respect to other messages within the same stream. The MME can specify at association startup time the number of streams to be supported by the association. This number is negotiated with the remote end.

Per RFC 4960:

In the INIT and INIT ACK chunks, the sender of the chunk must indicate the number of outbound streams (OS) it wishes to have in the association, as well as the maximum inbound streams (MIS) it accepts from the other endpoint.

After receiving the stream configuration information from the other side, each endpoint must perform the following check: If the peer's MIS is less than the endpoint's OS, meaning that the peer is incapable of supporting all the outbound streams the endpoint wants to configure, the endpoint must use MIS outbound streams and may report any shortage to the upper layer. The upper layer can then choose to abort the association if the resource

shortage is unacceptable.

After the association is initialized, the valid outbound stream identifier range for either endpoint is 0 to min(local OS, remote MIS)-1. (That is, when the MME is provisioned with number of outbound stream =1, all outbound messages are tagged with stream ID=0.)

The following two fields must be supported for the S6a profile:

- number of SCTP outbound streams, with value range 1 - 10 and default value 1
- number of SCTP inbound streams, with value range 1 - 10 and default value 1

With multiple outbound streams, the MME selects a stream to send using the round-robin selection method.

With multiple inbound streams, the MME lumps messages from all streams together and processes them as if they are from a single stream.

Upon a successful establishment of SCTP association, the number of inbound and outbound streams are negotiated to the lower number between the MME and SCTP peer during INIT and INIT ACK handling. When the other endpoint and the MME have different inbound and outbound values, the lower numbers is chosen.

If the SCTP association is not successfully established, the association is gracefully terminated.

19.3.5 SCTP path availability alarm for multi-homed connections (Feature m10402-12)

The *SCTP path availability alarm for multi-homed connections* feature provides the capability to send a major alarm when a path of a multi-homed SCTP connection becomes unavailable.

For the alarm to be raised, the SCTP association has to be established first. Once established, the MME heartbeats with the SCTP end points until an acknowledged heartbeat is received or the provisioned number of heartbeat retransmissions is reached. If none of the heartbeats are acknowledged, the MME generates a path unreachable alarm (`LSS_pathAvailability`) with a major severity.

The SCTP path alarm is cleared in the following circumstances:

- When an unreachable path becomes reachable.
- When the path's SCTP association changes operational state, either from enabled to disabled or from disabled to enabled. This change can result from an administrative lock or unlock action or a change in the collective availability of the association's paths. Any

path unreachable alarms are cleared. If the new association state is disabled, a single link/association alarm (`LSS_mmeExternalLinkDown`) is raised.

The feature also provides the capability to send a major alarm when a data mismatch has been found in the SCTP provisioning. The alarm is generated when either the SCTP interface profile and network interface types for an SCTP multi-homed link do not match or when an SCTP multi-homed link has been provisioned with remote addresses that do not match the addresses learned from the remote end in the INIT ACK message.

The feature supports reliable communication between the MME and other nodes.

19.3.6 MME support for same SCTP association to DRA and higher peer count (Feature f11304-01)

The *MME support for same SCTP association to DRA and higher peer count* feature supports a combination of three Diameter application IDs (S6A, S13 and SLG) on same (combined) SCTP associations.

The feature is disabled by default. When the feature is enabled, all previous diameter traffic will be combined over available S6A associations provisioned.

If the S13 interface, the SLg interface or both are in use, apply configurations de-growth for them before using the combined SCTP association.

Note:

It is possible to shut down the SLg interface before the *MME support for same SCTP association to DRA and higher peer count* feature is enabled, but this causes loss of SLg service access until the feature is enabled. Therefore, it is recommended to shut down the SLg interface when the feature is enabled.

When the associations need to be restarted and updated, if possible shutdown of existing S13 and SLg links is initiated, the existing S6A connections are restarted, and Capability Exchange Request/Capability Exchange Answer is exchanged with the DRA peers to request the new S6A/S13/SLg combination. When the feature is enabled, and the provisioned S13 and SLg interfaces, the remote endpoints and links are shut down or unused,

- alarms are raised for each disabled S13 links.
- alarms may be raised for previous SLg emergency links.

In the de-growth process, each interface for Diameter application ID combined with S6A

(S13 or SLg) is not usable. The interfaces local end-points are shut down, remote end-points and link associated are de-provisioned, and the local endpoints are deleted.

Alarms for the S13 interface, the SLg interface, or both that are raised for the switch to the combination mode need to be cleared are part of the de-growth procedure.

Related descriptions

- [Using the S6a/S13/SLg SCTP association for T6a \(Feature f11701-15\)](#)

19.3.6.1 DRA requiring different realms per application ID

DRA FQDN are extended to use a new variable format and definition to support provision of DRA when HSS, EIR and NLS (GMLC) are on independent separate realms.

When the *MME support for same SCTP association to DRA and higher peer count* feature is enabled, the MME supports a combination of three Diameter application IDs (S6A, S13 and SLG) on same (combined) SCTP associations. The *DRA requiring different realms per application ID* feature makes the provisioning of the DRA easily to be changed for routing, while HSS, EIR and NLS (GMLC) are on independent separate realms.

Typical standard FQDN used as Destination-Realm AVP in diameter requests from MME (default):

- epc.mnc{ueMnc}.mcc{ueMcc}.3gppnetwork.org

DRA Destination Realm FQDN string can be extended as follows when needed:

- {s6aHss:eir:gmlc}-core.epc.mnc{ueMnc}.mcc{ueMcc}.3gppnetwork.org

Example: DRA Destination Realm FQDN string example

{s6aHss09:eir2470:gmlc997}-core.epc.mnc{ueMnc}.mcc{ueMcc}.3gppnetwork.org

Example of FQDN expansion for a UE in home PLMN 310_012

- S6A -> MME: s6aHss09-core.epc.mnc012.mcc310.3gppnetwork.org
- S13 -> MME: eir2470-core.epc.mnc012.mcc310.3gppnetwork.org
- SLG -> MME : gmlc997-core.epc.mnc012.mcc310.3gppnetwork.org

19.3.6.2 Emergency service DRA selection for SLg

For emergency services, UE attach with IMEI requires default fallback rule for routing to DRA for positioning requests.

Two approaches are available to manage positioning requests for emergency calls when S6A/S13/SLG is combined. Use either or both of two approaches to support the emergency service DRA selection for SLg.

- Define an `imsiToHss` rule without minmsin and maxmsin, so it is defined for the full realm (home PLMN).
- Define an `imsiToHss` range rule on the MME home PLMN that specifically targets the NULL imsi range.

In case a UE IMSI is not known (as in emergency call), the NULL imsi, visited PLMN, and MME home PLMN, are considered (in this order) to select a DRA that will find a route to a GMLC.

Note:

By default, the last selected GMLC per UE when available is remembered and will be used as (fixed) destination Host and Realm given to the LRR to the selected DRA.

Related descriptions

- [IMSI to HSS rules](#)

19.3.7 Enhancement of SCTP state when locking SGs links (Feature f11806-01)

The MME supports the changing of the SCTP state when SGs links are locked.

When the SGs links are locked:

- if the link admin state is set to locked, the operational state of SCTP is disabled and the MME stops sending heart beat messages over locked SGs links.
- if the link admin state is set to unlocked, the operational state of SCTP is enabled and the MME continues sending heart beat message over locked SGs links.

19.3.8 UE Retention Information IE in S1 Setup Request/Response message to handle SCTP association restart (Feature f10909-01)

The new UE Retention Information IE is used in S1 Setup Request and S1 Setup Response messages to indicate whether eNB/MME supports the retention of the UE S1 connection.

This feature complies with 3GPP TS 36.413 CR1401 Revision 2: UE Context Retention at SCTP Recovery, which is updated in 3GPP TS 36.413 Release 13.2.0.

When the MME receives the S1 Setup Request message without the UE Retention Information IE from the eNB:

- If the SCTP association between the eNB and the MME is down and comes up, and the S1 Setup Request is received, no UE action is needed because the MME has initiated idling of all ECM-connected UEs on that eNB when the SCTP association is lost.
- If the SCTP association between the eNB and the MME is up and the S1 setup procedure takes place, this is treated as a repeated S1 setup procedure.

With this feature, when the MME receives the S1 Setup Request message with the UE Retention Information IE from the eNB:

- If the SCTP association between the eNB and the MME is down and comes up, and the S1 Setup Request message is received, no UE action is needed because the MME has already initiated idling of all ECM-connected UEs on that eNB when the SCTP association is lost. In addition, there is nothing to retain. The UE Retention Information IE does not need to be echoed back to the eNB since the UEs are not retained.
- If the SCTP association between the eNB and the MME is up and the S1 setup procedure takes place (note that this is the case that can occur after an IPDS switchover), the MME does not treat this as a repeated S1 Setup Request message. Instead, the MME retains the UE context and does not initiate idling of all ECM-connected UEs on that eNB.

19.3.9 Reassembly of fragmented IP datagrams (Feature f12113-01)

The Reassembly of fragmented IP datagrams feature adds support for SCTP IP reassembly. Previously, the MME supported IP reassembly and fragmentation only for UDP.

This feature allows the MME to receive SCTP packets from an endpoint with an MTU that is greater than 1500 bytes. Previously, the MME only supported reception of SCTP packets

from an end point with an MTU that is less than or equal to 1500 bytes.

The SCTP packet sizes that exceed the MTU can be either SCTP fragmented or SCTP IP fragmented or both. SCTP IP fragmentation remains unsupported. The CMM MTU continues to be statically configured and must be less than or equal to 1500 bytes. PMTU continues to be unsupported.

For a CMM end point to be configured with an MTU greater than 1500 bytes, the next hop router is required to generate an `ICMP Destination Unreachable message` or `ICMPV6 Packet Too Big message` for an MME ingress packet with a 802.3 Ethernet payload length exceeding the CMM MTU.

The ICMP Next-Hop MTU or ICMPv6 MTU field is set to the CMM MTU (less than or equal to 1500 bytes). This setting results in the end point updating its PMTU and retransmission of the SCTP packet using IP fragmentation. Subsequent SCTP packets that exceed the updated PMTU are expected to be SCTP fragmented and not SCTP IP fragmented.

19.3.10 MME support for MTU discovery for S1/M3 links over IPv6 (Feature f12107-02)

This feature supports the maximum transmission unit (MTU) discovery for IPv6 based on S1/M3 links (single-homed and multi-homed SCTP).

On receipt of a SCTP INIT chunk, the CMM sends an SCTP INIT ACK chunk that is the size of the minimum (<= 1500 bytes) of the SCTP profile MTU size and the network interface controller (NIC) MTU size. If no `ICMP6 Packet Too Big message` (type=2, code=0) is received, the association MTU is set to the probe value. If an `ICMPV6 Packet Too Big message` is received, the association MTU is set to the MTU contained in the Packet Too Big message. For a MH link, the MTU for each path is set to the smallest MTU across all paths.

In case the MTU for a network segment is subsequently reduced after link establishment, the CMM will receive an `ICMPV6 Packet Too Big message` when the new MTU size is exceeded. The received `ICMPV6 Packet Too Big message` will then result in a reduction of the association MTU and the MTU for each path. Retransmitted packets will be IPv6 fragmented to conform to the new MTU, subsequent packets will be SCTP bundled or SCTP fragmented using the new MTU size.

19.3.11 MME support for 32 SCTP associations per MSC for SGs and 32 endpoints for Sv (Feature f12123-01)

Previously, the MME supported 4 remote SCTP endpoints per MSC peer for the SGs connection. With this feature, the MME supports up to 32 associations per MSC peer for the SGs connection.

In addition, the MME supported 1 endpoint per MSC for the Sv interface previously. With this feature, the MME supports up to 32 endpoints per MSC for the Sv interface.

19.3.12 MME support for SGd on combined SCTP association (Feature f11004-05)

With this feature, the MME supports the SGd application on an SCTP association combined with the S6a/ S13/ SLg and S6a/S13/ SLg/T6a Diameter applications.

This feature moves the messages that are sent on SGd links to common links shared with HSS and EIR. Specifically, the feature combines the SGd interface to the already supported combination of the S6A/S13/SLg and S6A/S13/SLg/T6a Diameter applications on a single association to the Diameter routing agent (DRA). The DRA forwards the requests to the appropriate server type, such as the SGd messages to the SMSC target.

When the feature is enabled, it is not possible to use the direct link to SMSC target, even if it is provisioned. If changes are done to add, delete or modify the SGd interface remote end points or links, it will have no impact on CMM since the SGd-specific links are no longer used and combined with the S6a application.

19.3.13 MME support for override diamConnection profile default value parameters per UE PLMN service (Feature f11347-01)

This feature introduces a diameter application profile to override the default diameter application timeout set in the `diamConnection` command.

This allows the operator to define a longer default timeout for the inbound roammers whose home network is subject to longer round-trip delays while keeping a default timeout window for home subscriber diameter applications.

The profile contains a list of diameter applications and their respective timeouts. Each defined diameter application type can appear at most one time in each profile. The diameter

application profile structure is presented in the table *Diameter application profile logical view*.

Table 80: Diameter application profile logical view

Diameter Application Type	Timeout
S6A	6
S13	7
SLG	8
....

The `uePlmnServices` translation supports a pointer to the above table. The default pointer is blank.

When the MME sends a diameter request, the MME determines its timeout as follows:

- If the `uePlmnServices` record for the UE is not provisioned with a pointer to the `diamApplProfile` command, set the diameter timeout per the current logic prior to this feature. Use the `diamApplTimeOut` parameter in the `diamConnection` command, which applies also for the associated combined application types and can be overridden for certain applications such as T6a and SGd depending on the scenario.
- If the `uePlmnServices` points to a valid `diamApplProfile` but that profile does not contain an entry for the application type corresponding to the message to be sent, proceed as per the above case using the current logic prior to this feature.
- Otherwise, the MME sets the diameter timeout to the corresponding value in the `diamApplProfile` command.

This logic applies regardless of whether the message diameter application corresponds to a standalone diameter interface (for example, when the `diamApplType` is set to `S6A`) or to a combined diameter application type over S6a (for example, when the `combinedApplType` equals to `S6A/S13/SLG`).

After the diameter timeout is set according to the above logic, the MME sends the message and waits for a response or a timeout.

19.4 GTP

Features related to GTP-based interfaces, for example, GTP echo and GTP profile provisioning.

19.4.1 Extended GTP Echo Timer (Feature m11501-02)

The **Extended GTP Echo Timer** feature extends the expanded range for the send echo timer value within GTP profile. It also allows expanded range for the wait echo timer value within GTP profile.

With this feature the MME can allow for an expanded range for the send echo timer value within the GTP profile. The range of values is extended to 60 – 10 800 seconds from prior range of 60 - 300 seconds. The MME can also allow for an expanded range for the wait echo timer value within the GTP profile. The range of values is extended to 1 - 600 seconds from prior range of 1 - 60. This extension allows for very infrequent GTP echo exchange when the peer node is down, in overload, or during troubleshooting.

19.4.2 Configuration options for GTP echo (Feature m11501-01)

The **Configuration options for GTP echo** feature supports configuration capabilities for enabling and disabling Echo Request message for GTP control (GTPv1C and GTPv2C) interface path monitoring.

This feature provides configuration capabilities for the Echo Request message for GTP control (GTPv1C and GTPv2C) interface path monitoring. Operators can

- enable or disable periodic Echo Request per interface basis.
- enable sending Echo Request on a failure.

The MME always responds to Echo Request from a peer irrespective of whether MME is enabled or disabled to send the Echo Request. The MME does not monitor GTP paths if the echo request procedure is disabled. As a result, the MME does not report loss GTP paths using alarms.

Additionally, the feature supports provisioning of deletion timer for deleting Gn-GGSN, S3, and S16 link maintenance objects (MO) if there is no activity on a link continuously for a period indicated by the deletion timer.

For this, two timers are supported: GTP path MO deletion timer 1 and GTP path MO deletion timer 2. The timer 1 applies to Gn-SGSN MO and the timer 2 applies to Gn-SGSN, S3, and S16 MOs.

With this feature, the MME does not send the GTP control (GTPv1C and GTPv2C) Echo Request message and does not monitor and report alarms if periodic echo and echo on a

failure capabilities are disabled for a GTP interface.

This capability is supported for all MME supported GTPv1C and GTPv2C interfaces: Gn, S10, S11, S3, Sv, and Sm.

The MME always responds to a received Echo Request message irrespective of whether sending the Echo Request is enabled or disabled.

The MME sends periodic Echo Requests if the periodic Echo Request capability is enabled.

If the capability for sending Echo Requests upon detecting a failure is enabled and sending of Echo Request was triggered by lack of GTP-C control message response, if no message is received from the peer network element during the echo request $T3 * N3$ time interval, the MME marks the link MO disabled and issues the corresponding link alarm. The MME also sends periodic Echo Requests while the link is disabled in order to monitor the availability of the peer network element. Reception of a message from the peer results in marking the link enabled and MME clears the corresponding alarm. This behavior is independent of the provisioning of sending periodic Echo Request.

The MME/SGSN performs the echo request procedure upon the link MO creation, IPDS initialization or switchover for the purpose of exchanging recovery counters and node features.

19.4.3 N3 and T3 timers per GTP message type (Feature m11502-01)

The *N3 and T3 timers per GTP message type* feature supports different GTP profiles with different T3/N3 values for GTPv2. Operators can configure preferred values specially for roaming partner, where there is a need to have, for example, a longer T3 timer (or higher N3 counter or both).

This feature supports configuring T3/N3 per GTP message type on each of the supported MME GTPv2-based interfaces, S11, S10, S3, and Sv.

This allows operators to specify a default GTP profile with default T3/N3 values for each of the GTPv2 message types.

- Should there be a need to override the default T3/N3 values, different GTP profiles from the default can be created and assigned per GTPv2 interface.
- The different GTP profiles include all the GTPv2 messages of the default GTP profile but with different T3/N3 values for messages that require a different value from the default.
- The GTP profile contains all supported GTPv2 and GTPv1 messages.

This feature also supports allowing the creation of a separate T3/N3 per GTP message type profile for MME GTPv2 interface (S11/S8) toward the P-GW where such nodes belong to roaming network partners. This addresses the scenario where the roaming partner P-GW is located far from the S-GW and might require longer time for GTP requests/responses to arrive at intended destination because of possibly longer transport latency.

GTP-based interfaces use the default GTP profile if they are not explicitly assigned a different GTP profile.

The MME supports assigning a per GTPv2 message type T3/N3 GTP profile for roaming partner networks where the P-GWs, or collocated P-GW/GGSNs, reside in the roaming partner networks and there is a need to have a longer T3 timer (and higher N3 counter or both) to account for the extra latency between the serving S-GW in the visited network (VPLMN) and the P-GW in the home network (HPLMN).

The MME uses the T3/N3 values from the assigned GTP profile for the roaming networks when UE session is established over S8 interface to the roamer's HPLMN P-GW/GGSN. If the GTP profile under roaming networks is blank (no string), the MME uses the S11 interface GTP profile for homers and roamers.

The following are GTP request messages that are exchanged over the S8 interface:

- Create Session Request
- Delete Session Request
- Modify Bearer Request
- Change Notification Request
- Resume Notification
- Modify Bearer Command
- Delete Bearer Command
- Delete PDN Connection Set Request
- Suspend Notification

The MME supports up to 256 GTP profiles.

 **Note:**

256 GTP profiles are not enough to assign a separate GTP profile for each of the roaming partner networks when there are more than 255 roaming partners. However, it is assumed that operators share GTP profiles among roaming partners.

The MME supports the following defaults and ranges for the GTP profile T3/N3:

Table 81: GTP profile T3/N3

Parameter	Range	Default	Exceptions
T3	100-60000 ms in 100 ms increments	3000 ms	echo-request-timeout T3 range is 60000-10800000 ms, default is 60000 ms echo-response-timeout T3 range is 1000-600000 ms, default 6000 ms
N3	1-5	3 attempts	echo-request-attempts N3 range is 5- 20, default is 9

19.4.4 Improved S11 path management (Feature m10144-01)

The **Improved S11 path management feature supports enabling S11 link based on successful S11 Create Session Request/Response exchange.**

For mode 2 selection of a S-GW/P-GW, when S11 interface is disabled due to no GTPv2 Echo Request from the S-GW, a new attach to the S-GW succeeds but the MME does not change the status of the S11 path and the MME forces a detach. This feature changes the current behavior to enable the S11 link based on a successful S11 Create Session Request/Response message exchange.

19.4.5 Configurable CRSI flag for GTPv2 messages (Feature f11502-01)

This feature supports a configurable parameter so that the MME always sets the CRSI flag to 0 in GTPv2 messages.

CMM can be provisioned to control the support for Change Reporting Support Indication Flag that is sent in GTPv2 messages (Create Session Request, Modify Bearer Request, Forward Relocation Request, Context Response). Change Reporting Support Indication flag is set to 1 (indicating MME support) in the GTPv2 messages when the parameter is enabled. When the parameter is disabled, CRSI flag is set to 0 in GTPv2 messages. By default this capability is enabled.

19.4.6 MME support for provisioning control for GTPv2 cause code 110 (Feature f11505-01)

This feature controls the support of GTPv2 cause code 110 (temporarily rejected due to handover/TAU/RAU procedure in progress) that is sent in GTPv2 message to S-GW across S11 interface.

This feature introduces a global parameter, `sendSgw3gppS11cc`, to enable or disable the usage of GTPv2 cause code 110 that is sent in GTPv2 message to S-GW. The allowed values of this parameter are `Yes` and `No` (default). If the parameter is set to `Yes` indicates MME supports and sends the cause code 110 to S-GW. If it is set to `No` indicates that MME does not send the cause code 110 to S-GW across S11 interface.

19.4.7 Create session request enhancements (Feature f10186-01)

With this feature, an older S-GW, which is in compliance with 3GPP TS 29.274 Release 10, should be able to decode the GTPv2 Indication IE from TS 29.274 Release 11 and later.

For an older S-GW, which is in compliance with 3GPP TS 29.274 Release 10 and only supports an Indication IE of octet field no more than 7 bytes, when the Create Session Request message with an indication IE including octets 8-11 field is received, the S-GW will reject with cause value Invalid length.

When this feature is disabled, the CMM supports standards-based encoding for the Indication IE.

When this feature is enabled, the CMM only encodes the first three bytes of indication flags with the Indication IE.

This feature does not only apply to the Indication IE contained within the GTPv2 Create Session Request message sent over the S11 link to the S-GW, but also applies to all GTPv2 encoded messages which are sent over the S11 link and contain the Indication IE.

This feature is controlled by global parameter `octetEncodingSupport`. Default value is `No`.

19.4.8 GTP sequence number management enhancements (Feature f11506-01)

This feature enhances the management of the GTP sequence number to improve the behavior of the CMM and to avoid exhausting available GTP sequence numbers.

The following enhancements have been implemented for the management of GTP sequence numbers:

- The GTP sequence number search algorithm for all GTP interfaces has been enhanced to more efficiently find available sequence numbers, especially in the cases where the number of available sequence numbers decreases.
- Lost sequence numbers can now be found and recovered.

This feature impacts the signaling messages between the CMM and S11 S-GW and between the CMM and the S4-SGW.

19.4.9 MME support for GTP restart counters dump (Feature f11507-01)

This feature provides a utility mechanism to report the local MME and the remote S-GW recovery restart counters for all the GTPv2 S11 interfaces known to the system.

This mechanism is achieved through CLI commands that enable the operator to display the MME restart counter and set it to a specific value.

19.5 Link management

Interface/link management features.

19.5.1 Restricting S10 to neighboring MME (Feature m10533-01)

With the *Restricting S10 to neighboring MME* feature the S10 dialog to non-neighboring MMEs can be restricted and the usage of poor S10 links can be disabled.

This feature restricts S10 links to neighboring MMEs when a GUTI Attach Request is received if the globally unique temporary identity's (GUTI's) public land mobile network (PLMN) ID matches the serving network PLMN ID but has a different Group ID and the MME discovery is

enabled:

- If the S10 link does not exist:
 - the MME does not create a S10 link to the old MME.
 - the MME retrieves international mobile subscriber identity (IMSI) directly from the UE to proceed with the attach procedure.
- If S10 link exists to the old MME, the MME uses the current handling of the attach procedure.

The current behavior of S10 link creation is not changed for the following procedures because these events occur between the MME of an adjacent pool (S1 handover and tracking area update (TAU) request) or between MMEs of the same pool (TAU request):

- S1 handover with the MME relocation because that S1 handover with the MME relocation only occurs between two adjacent MME pools
- TAU with MME relocation
- Reception of S10 Identity Request, Context Request, Forward Relocation Request, and Echo Request messages

This feature effectively lets operators use domain name system (DNS) selection for the MME discovery where the operator wants to limit the pool of available MMEs to local MMEs because of poor long haul core backhaul.

19.5.2 Eliminating alarms for links that were never active (Feature m30111-02)

The ***Eliminating alarms for links that were never active*** feature provides elimination of alarms for any link that was never active.

With this feature, the MME may eliminate alarms for any link that was never active. The specific request in this case is for Gn links to SGSNs that are never active. This can happen if the SGSN is in another provider's network that is unknown to the serving network.

 **Note:**

This happens when a request is sent to an SGSN that does not respond. The MME keeps this link disabled for 24 hours, with an alarm, before deleting the managed object (MO). The MO in this case is not sent.

19.5.3 Multiple DSCP values on all network interfaces (Feature m11014-01)

The **Multiple DSCP values on all network interfaces** feature provides differentiated services code point (DSCP) support on all network interfaces on the MME. Differentiated services is a mechanism for classifying and managing network traffic and providing quality of service (QoS) guarantees.

DSCP values can be provisioned for OAM, CALEA/LI (X1, X2), and all network interfaces:

- GTP/UDP: S11, S10, Gn, Sv, S3, Sm
- SCTP: S1-MME, S6a, SGs, S13, SBc, SLs, SLg, M3

Provisionable values include the following five assured forwarding (AF) classes:

- AF11 (DCSP 10 decimal)
- AF21 (DCSP 18 decimal)
- AF31 (DCSP 26 decimal)
- AF33 (DCSP decimal 30)
- AF41 (DCSP 34 decimal)

In addition, a choice of CS5 (DCSP decimal 40) and EF (DCSP 46) are available. The default value is AF 41 (DCSP 34 decimal).

The feature provides efficient transport of messages from MME.

19.5.4 Link and interface specific alarms with severity control (Feature f14208-01)

The feature provides specific alarms for each interface type, link and path. The configurable interface name and link/path severity are included in the alarm names. The `cmm alarm active list` command can be used to view detailed alarm information.

With this feature, operators can easily recognize and act on link failures for interfaces that have higher impact on the operation of the network.

19.5.5 S1 CLI enhancements (Feature f14603-05)

This feature introduces CLI commands for bearer administration and S1 reset.

This feature enables the operator to

- initiate default bearer deactivation for a subscriber. (If the bearer is the last bearer for the subscriber, then the implicit detach method for the last bearer deletion will be used.)
- initiate dedicated bearer deactivation for a subscriber.
- initiate S1 connection release for a subscriber (implicit detach).
- display the bearers of a subscriber.
- reset all S1 connections for a specific eNB. The S1 reset will use cause 'Transport resource unavailable'.

19.5.6 Enhancements to eNB configuration update and S1 setup procedures (Feature f10933-01)

This feature incorporates 3GPP 36.413 CR#1662-related enhancements to eNB configuration update and S1 setup procedures to provide connected en-gNB list to the MME.

This CR also enhances eNB/MME configuration transfer procedures to carry EN-DC SON configuration transfer information.

19.5.7 Extending TAI/eNB query to include TAC range and state of S1-MME links (Feature f14611-01)

This feature enhances the `enbTaiQuery` and `taiEnbQuery` commands to allow multiple TACs and a range of TAC, to add the state of S1-MME link for an eNB, and to add broadcast PLMNs.

You can now use fields `linkAdminState` (values `locked/unlocked`) and `linkOperationState` (values `disabled/enabled`) as filters on the `cmm enbTaiQuery list` and `cmm taiEnbQuery list` commands.

Additionally, you can use fields `minTac` and `maxTac` on the `taiEnbQuery` command to display a range of records.

Example: eNB TAI/TAI eNB queries

```
cmm enbTaiQuery list --mcc 310 --mnc 012 --enbId 17476

cmm taiEnbQuery list --taiMnc 012 --taiMcc 310 --minTac 25600 --
maxTac 25606

cmm enbTaiQuery list --mcc 310 --mnc 012 --enbId 17476 --
```

```
linkAdminState unlocked --linkOperationState enabled  
cmm taiEnbQuery list --taiMnc 012 --taiMcc 310 --minTac 25600 --  
maxTac 25606 --linkAdminState unlocked --linkOperationState enabled
```

19.5.8 MME support for increasing the S11 links (Feature f12118-03)

This feature increases the maximum number of S11 link managed objects (MO) from 256 to 1024.

This feature interworks with S-GW/P-GW selection based on IMSI/MSISDN range (Feature f10110-01). Feature f10110-01 limits S11 link managed objects indices to [241, 256] for provisioned S-GW, which is now increased to [1001, 1024] with feature f12118-03.

When the f10110-01 feature is enabled, the maximum number of S11 link managed objects is 1000.

When the f10110-01 feature is disabled, the maximum number of S11 link managed objects is 1024.

19.5.9 MME support for increasing the number of S10 and N26 links from current limit to combined 512 (Feature f12118-01)

This feature increases the maximum combined number of S10 links and MME N26 links to 512. MME generates alarms when the number of S10 or N26 links approaches their combined limit. This feature also supports aging out N26 links.

As S10 and MME N26 interface types share the same link indexing space (that is, if S10 uses link 1, N26 uses the next available link index, which is link 2), this feature increases the combined S10 and N26 link limit to 512. This feature supports any combination of S10 or N26 links that add up to 512. The link exhaustion alarm uses the combined link limit. A major level alarm is raised at 85% capacity of the combined maximum limit, while a critical level alarm is raised at 100% of the combined maximum limit. The alarm level drops from critical to major when lowered to 95% and from major to clear at 80%.

19.5.10 Dynamic link exhaustion alarm at reaching static thresholds (Feature f13306-01)

This feature enhances link exhaustion alarm.

In this feature, when the number of used links for each of the listed link type is approaching its maximum allowed engineered capacity, alarms are raised. A major level alarm is raised at 85% capacity, while critical level alarm is raised at 100%. Alarm level automatically reduces from critical to major when capacity drops back down to 95% and from major to clear at 80%. The link types supported are: S1-MME, M3, S11, S11-U, S3, S16, and Gn.

20. Layer 3 network steering (L3NS)

L3NS acts as a layer 3 networking device and is the single entry point through which signaling is steered to the multiple IPDS (M-IPDS) instances.

When the CMM is configured as a large system, it uses multiple pools of IPDS instances to handle the message load. L3NS is used to route S1, S11, S11U and M3 traffic to the correct spread IPDS pool. All other traffic is sent to the lead IPDS pool. OA&M connectivity never traverses L3NS.

L3NS adds some layer 3 router functions to the CMM. The LAN and IP configuration supported for MME to external MLS is supported by the L3NS service and the configuration requires minimal or no changes. L3NS service can be used to support routing protocols, such as OSPF and BGP. Between the IPDS instances and L3NS service, a private transport network is used. L3NS leverages OpenFlow and sticky ECMP to define routes toward IPDS pairs for CMM signaling services. An OpenFlow connection is set up between the lead IPDS and the L3NS service. OpenFlow is used to program which IPDS the external connections terminate.

For information about achieved capacity at various spread configurations, refer to the *Capacity* guide.

20.1 Achieved capacity at various spread configurations

Progression of capacity as the configuration is grown from 1 IPDS pool (not spread) to 2 - 4 IPDS pools (spread).

Table 82: Progression of capacity as configuration is grown for MME-only deployments

Number of IPDS pools	Description	Capacity (msgs/second)
1	Not spread and L3NS is not used	500K
2	Minimum spread configuration	600K
3	Provides additional capacity increase	1.1M
4	Supports 1.6M messages/second	1.6M

Table 83: Progression of capacity as configuration is grown for MME/SGSN deployments

Number of IPDS pools	Description	Capacity (msgs/second)
1	Not spread and L3NS is not used	500K
2	Minimum spread configuration	800K (of which 500K is S1/S11 and served by the spread IPDS)
3	Provides additional capacity increase	1.3M (of which 1M is S1/S11 and served by the spread IPDS)

20.2 Multiple IPDS (Feature f80005-01)

This feature provides additional processing resources to meet the 1.6 million messages/second MME configuration.

This feature increases the number of IPDS pairs (1+1 redundant) that are allowed in the CMM. The number of possible pairs is from 1 to 4. The additional pairs of IPDSs terminate the S1_MME, M3, S11 and S11U interfaces. These interfaces carry most of the traffic in an MME and thus to meet the 1.6M messages/second capacity, more than one interface pair is required. The remaining interfaces are still terminated on the first, or lead, IPDS pair. The lead IPDS is responsible for the mapping of interface or links to the additional IPDS instances, maintaining the user mapping tables, and system overload control.

The lead IPDS programs the L3NS VMs with the correct interface mapping between the additional IPDSs and L3NSs using the OpenFlow mechanism.

20.3 L3NS/VSR for multiple IPDS (Feature f12112-03)

The L3NS/VSR for multiple IPDS feature provides Layer 3 network steering (L3NS) service as VMs on the CMM. L3NS, based on Nokia virtual service router (VSR), is used to support multiple IPDS instances.

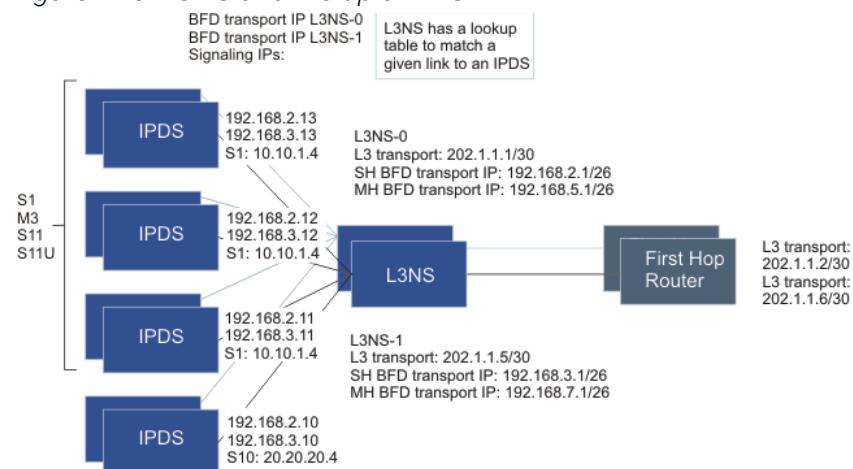
When the CMM is configured as a large MME system, it uses multiple pools of IPDS instances to handle the message load. The L3NS VM (VSR) is used to route S1, S11, S11U, and M3 traffic to the correct spread IPDS pool. All other traffic is sent to the lead IPDS pool. OA&M connectivity never traverses L3NS.

The L3NS adds some layer 3 router functions to the CMM. The LAN and IP configuration supported for MME to external MLS is supported by the L3NS and the configuration requires minimal or no changes. The L3NS can be used to support routing protocols such as OSPF and BGP.

Between the IPDS and L3NS instances, a private transport network is used. L3NS leverages OpenFlow and sticky ECMP to define routes toward IPDS pairs for CMM signaling services. An OpenFlow connection is set up between the lead IPDS and the L3NS instances. OpenFlow is used to program which IPDS the external connections terminate. The following diagram shows an example of how this network could be set up.

The routers are set up to use ACL chain groups across the L3NS. The L3NS instances ensure that all traffic for a given link goes to the same IPDS.

Figure 175: L3NS and multiple IPDS



20.4 MME support for 1.6M messages per second on OpenStack (Feature f80012-01)

The *MME support for 1.6M messages per second on OpenStack* feature scales the capacity of a CMM to 1.6M messages per second in the MME configuration on OpenStack.

This feature supports 1.6M messages per second on OpenStack for the MME. The feature is dependent on both the *Multiple IPDS* (f80005-01) and *L3NS/VSR for multiple IPDS* (f12112-03) features. When used together, the capacity increase allows the MME to serve additional eNBs, subscribers and procedures.

20.5 SGSN support for TA configuration with MME scaled to 1.2M on OpenStack (Feature f80005-09)

This feature provides support for the **MME support for Multiple IPDS (f80005-01)** feature when it is deployed in a CMM with MME/SGSN configuration. Previously, multiple IPDS with L3NS was supported on MME-only deployments.

All SGSN interfaces terminated on a IPDS (single IPDS) remain on the leader IPDS (pair 0) and traffic goes through VSR. On an MME/SGSN CMM, IPDS pair 0 is always selected for establishing the PAPS – IPDS TCP channel.

20.6 CMM support for fourth IPDS pair in a TA configuration (Feature f80005-18)

With this feature, SGSN supports a fourth IPDS pair, allowing the CMM to support 1.6M messages per second in an OpenStack MME/SGSN configuration. When configured with the **Multiple IPDS (f80005-01)** and **L3NS/VSR for multiple IPDS (f12112-03)** features, the capacity of a CMM in an OpenStack MME/SGSN configuration increases to 1.6M msg/sec.

20.7 Support for L3NS Release 20.5 (Feature f12112-11)

This feature validates L3NS/VSR release 20.5 with the CMM. This feature also validates L3NS/VSR using the Intel XXV710 NIC.

20.8 CMM support for 100K asymmetric MH SCTP eNodeB in deployments with L3NS (Feature f12112-08)

With this feature, a CMM deployed with L3NS can support up to 100K eNBs using asymmetric MH SCTP with the remaining eNBs of the total eNB limit possible being SH SCTP. The limit for symmetric MH SCTP eNBs remains 50K.

With asymmetric MH, an SCTP association has two IP addresses on the MME side and one IP address on the eNB side. Previously, the CMM supported only symmetric MH, where there are two IP addresses on the MME side and two IP addresses on the eNB side.

20.9 L3NS-based multiple IPDS deployment with dedicated spread S11 IPDS (Feature f12112-10)

With this feature, you can deploy multiple IPDS with L3NS and configure the S11 traffic to be served exclusively by a dedicated spread IPDS pair.

One or two additional IPDS pairs exclusively serve the S1/M3 traffic. This configuration can be useful for a provider who connects the CMM (MME-only or MME/SGSN) to a single S-GW that is engineered to terminate a large amount of S11 traffic.

21. Operability

PCMD is a tool for data analysis and troubleshooting. In addition, features such as performance management, component performance indicators and call trace provide data about system and network performance.

21.1 Real time monitoring

The CMM supports PCMD real time reports to monitor the system's performance and resolve user or network related issues.

The feature is:

- Per call measurement data (PCMD) (Feature f60110-14)

21.1.1 Per call measurement data (PCMD)

Per call measurement data (PCMD) on the CMM provides selected call measurement data on a per-procedure basis for most of the procedure interactions that the user has in 4G and 5G network.

A PCMD record is generated for every procedure (attach, service request, handover, and so on) – all the detail of call trace, at a fraction of the network cost. PCMD reports are supported only for the MME.

A rich set of signaling and bearer data is streamed northbound for either historical or near real-time data analysis and troubleshooting. Each record captures quality of signaling events, data throughput (per QCI), procedure setup latency, channel quality, dropped packets, and UE experience (RSRP, RSRQ, RTD, and so on) – a complete view of user experience, eNB conditions and mobility management in a single record.

PCMD can help in the following scenarios:

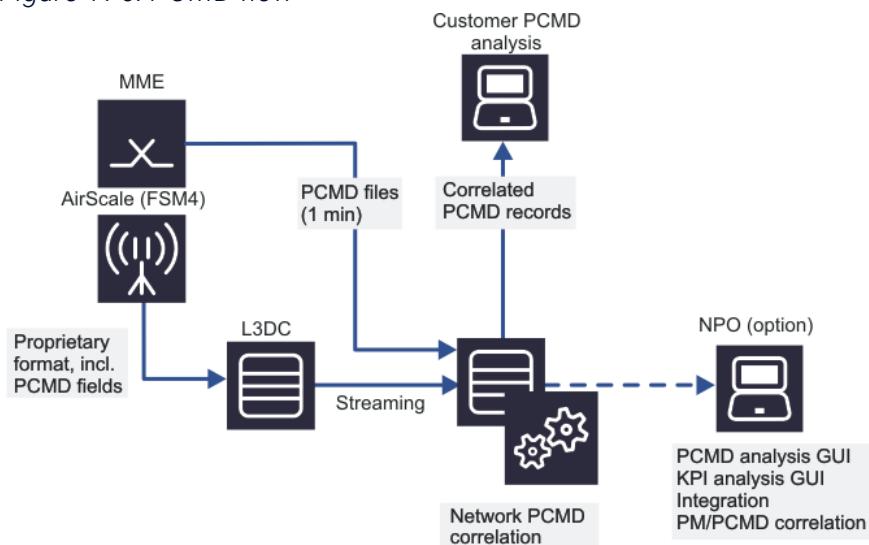
- Evaluate UE performance. PCMD can determine if a particular brand or model or even a specific mobile is causing set-up failures and dropped calls. This enables the service provider to narrow down the root cause of the problem - network related, UE related, or air interface related.
- Quickly determine failure scenarios. PCMD collects data associated with the call/connection. This capability allows quick response to customer trouble tickets. There is no need to recreate the failure scenario in the lab to understand why a call failed or was

dropped. This greatly reduces the need for the drive test, which is very expensive and time consuming.

- If data is also collected from the Nokia AirScale eNB, PCMD can be used to analyze RF coverage. PCMD gives very useful information about RF coverage. Once the network is established, RF coverage can be analyzed by looking at signal strength at the end of calls. Inadequate RF coverage can result in lost calls, and signal strength at the time of a lost call can be examined in the PCMD record. PCMD significantly reduces RF optimization and engineering costs.

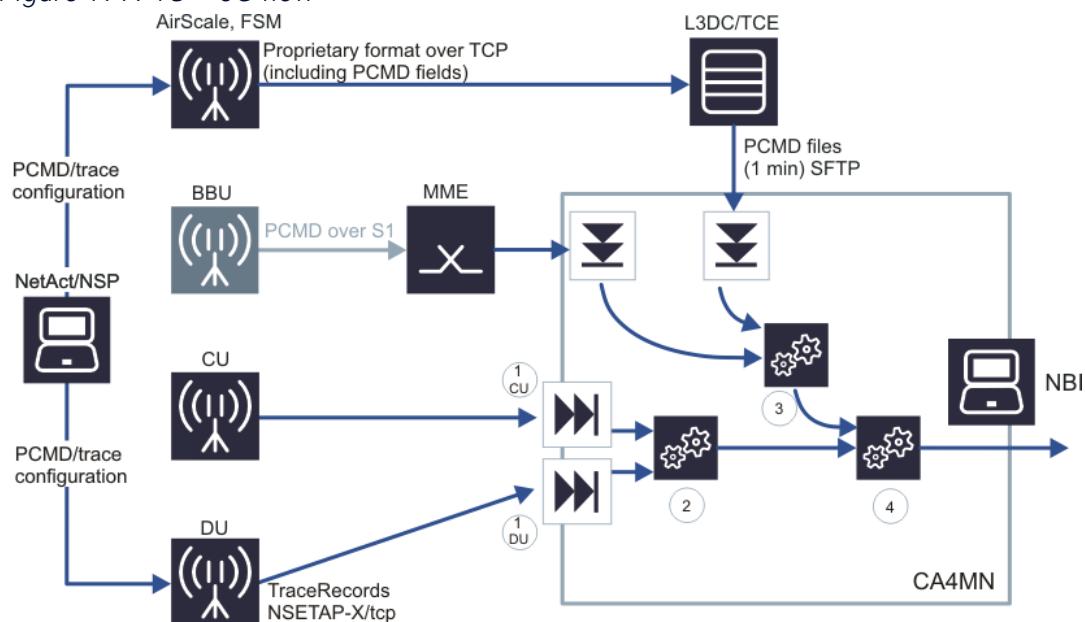
The following figure shows the flow of PCMD records collection for a pure 4G call.

Figure 176: PCMD flow



The following figure shows the flow of PCMD record collection for 4G+5G call.

Figure 177: 4G + 5G flow



21.2 MME/SGSN PM data transfer towards ONAP-DCAE and MME/AMF PCMD data transfer towards CA4MN (Feature f14615-05)

This feature adds initial PM data support for the Open Networking Automation Platform (ONAP), Dublin version. Other functionalities for ONAP are not yet supported. This feature also provides the capability for Cognitive Analytics for Mobile Networks (CA4MN) tool to fetch PCMD files from the NECC.

ONAP is an open source project hosted by the Linux Foundation. ONAP provides a comprehensive platform for real-time, policy-driven service orchestration, and automation. For more information, see <https://docs.onap.org/>.

You can configure the CMM to send notification about non-real-time PM files (3GPP) and to send close-to-real-time PM counters directly to ONAP. The non-real-time PM file is common for all access types and is configured only once regardless of the supported access type. These files are zipped and stored in the `/data-pm/gzip` directory. The retention policy is common for all PM files in the `/data-pm/` directory. Notification is sent to ONAP once every 5 minutes. After receiving notification, ONAP can fetch the zipped PM files with SFTP. The default user `dcae-dfc` is used for this operation. The `cmm dcaeServer` command is used to configure the CMM for data transfer to ONAP.

Close-to-real-time counters are configured separately for each access type. Close-to-real-

time counters are limited to predefined counters. These counters are sent to ONAP once every minute. For a list of supported counters, see the counters documents.

With this feature, the CA4MN can fetch the AMF PCMD files from the NECC. The CA4MN polls the `/data-pcmd` directory and fetches the desired files. The CA4MN SFTP user is used for this operation. If the CA4MN needs to use an SSH connection to trigger the `pcmdExport` functionality, the CA4MN user can be used for this operation. If other user is used for this operation, the user must belong to the admin user group.

21.3 Backup scheduling (Feature f14509-01)

With the *Backup scheduling* feature, operator can schedule when the system triggers the backup function automatically, for example, weekly.

The operator can create, list, modify and delete the system backup schedule using the CLI command `schedule`.

Scheduling of system backup jobs can only be done by the admin user.

Backup files are stored in the Cinder disk.

Alarm `42007 ScheduledBackupFailure` is raised when a backup job or part of it fails.

21.4 Remote copy of backup files (Feature f12003-01)

With this feature, operator can schedule a job to automatically copy the backup files from the CMM to a remote machine. It is recommended to use the remote-copy of backup files feature only when a scheduled CMM backup is in use.

To support the automatic copy of backup files from the CMM to the remote machine, SSH keys must be configured. SSH keys only need to be configured once during the lifetime of the CMM, or at the appropriate time the operator wants to re-create the SSH keys.

The schedule used for the remote-copy of backup should be aligned with the backup schedule and offset by an hour.

For example, if the backup is scheduled at 2:00 AM every day, the remote-copy of backup should be scheduled at 3:00 AM every day.

Scheduling of system remote-copy job can only be done by the admin user.

Alarm `42009 ScheduledRemoteCopyBackupFailure` is raised when a remote-copy job or part of it fails.

21.5 Cloud backup and restore improvements via NSP (Feature f14008-01)

With this feature, the CMM supports backing up and restoring CMM configuration from the Network Services Platform (NSP) NFM-P via CBAM. A new secondary IP can be set for the backup files remote copy destination. The secondary IP is used if the connection to primary IP cannot be established.

For the backup, a NetConf connection to the CMM and an HTTP (REST) connection towards CBAM are needed. The existing CMM CLI command `cmm remoteCopySetup` is used to send the backup from the CMM to the NSP. For the restore, an HTTP (REST) connection towards CBAM is needed.

21.6 CMM support for secure backup and restore of CMM instance (Feature f14008-02)

With this feature, an operator can create and manage secure backup files.

With this feature, an operator can create secure backup files, send them from the CMM to a remote machine, retrieve them from remote machine to the CMM, and restore them. If a remote machine is not configured, backup files are only stored locally.

21.7 CMM support for performance measurements (Feature f60110-11)

Collecting statistics about traffic and events makes it possible to plan network capacity, find out the reasons for unsuccessful service usage, and identify popular services.

You can measure the performance of the network services and take corrective actions with the performance management functions.

PM data is sent in from VMs to NECC which provides collection of statistical data.

The statistics API on the NECC is used to query counters from all the measurements with selected period (provisionable through the EMS or local CLI). NETCONF Notify is used to inform the EMS that new PM data file (XML format) is available for transfer. Northbound entities can retrieve the XML based performance statistics through the EMS.

21.8 PM evolution for static counters (Feature f13012-02)

This feature finalizes the PM evolution feature set introduced in f13012-03 PM evolution for component counters by moving the rest of the counters from InfluxDB to the PM architecture based on pmAggregator process in NECC.

With PM evolution features f13012-02 and f13012-03, all the counter data has been moved from InfluxDB to PM aggregation datastores in NECC. As the result of this architectural change also Grafana tool integration has been removed from CMM, as it was using counter data stored in InfluxDB as source data for visualization.

For static counters, PM aggregation datastores replace Influx DB. TCP communication channel is used. Also, the VM statistics based earlier in data provided by Telegraf, are now based on specific process IxProfile running in all VMs, and stored also in PM aggregation datastores. The following static counter groups and VM statistics counter groups are moved from Influx DB to the PM aggregator service (only affected MME/SGSN counters are listed here):

- M003 GPRS Data Measurement
- M004 GPRS User Measurement
- M007 GPRS DNS Measurement
- M008 GPRS CDR Measurement
- M011 GPRS Overload Control Measurement
- M021 GPRS PAPS User Measurement
- M022 GPRS Security Measurement
- M023 GPRS Iu Security Measurement
- M024 GPRS Iu SGSN Paging Measurement
- M026 GPRS Gb SGSN Paging Measurement
- M028 GPRS Iu OLC Measurement
- M029 GPRS SGSN Data Measurement
- M037 GPRS IPDS Interface Measurement
- M038 GPRS IPPS Data Measurement
- M041 CPI Formula
- M044 SCCP Single Meters Measurement
- M045 TCAP Performance and Utilization Measurement
- M046 GPRS GS Interface Measurement
- M101 EPS CPPS Authentication
- M103 EPS CPPS Bearer Session Management
- M105 EPS CPPS Capacity
- M107 EPS CPPS Communication

- M108 EPS CPPS Connections(108)
- M110 EPS CPPS Dedicated Bearer
- M112 EPS CPPS DNS
- M114 EPS CPPS Handover
- M115 EPS CPPS Interface
- M116 EPS CPPS Lawful Intercept
- M117 EPS CPPS Location Based Services
- M118 EPS CPPS Mobility Management
- M120 EPS CPPS Network Assisted Cell Change
- M121 EPS CPPS Overload Control
- M122 EPS CPPS Paging
- M125 EPS CPPS Roaming
- M127 EPS CPPS Session Restoration
- M131 EPS IPDS Automated Neighbor Relations
- M132 EPS IPDS Broadcast Warning Message
- M133 EPS IPDS Communication
- M134 EPS IPDS DNS
- M136 IPDS Interface
- M138 EPS IPDS Lawful Intercept
- M139 EPS IPDS Location Based Services
- M140 EPS IPDS Multimedia Broadcast Service
- M141 EPS IPDS Overload Control
- M142 EPS IPDS Paging
- M143 EPS IPDS Quality and Reliability
- M144 EPS IPDS Session Restoration
- M159 EPS DBS Session Restoration
- M161 EPS CPPS Short Message Service

VM statistic counter groups are as follows:

- M128 CPU Usage
- M129 Disk Input/Output
- M130 File System Usage
- M145 Memory Usage
- M147 Network Utilization
- M153 CPU Usage Per Core

Note:

None of the measurement groups listed above are aggregated, meaning the values are available per VM.

Static counters are moved to PM aggregator service, and as a result:

- Only 15 minutes of history is held for all the counter types (component, static, VM statistics). After that, the data is stored in the `/data-pm` files. Thus, `cmm counter` queries will only return 15 minutes. Values older than 15 minutes will be stored in the `/data-pm` files for 3 days (72 hours) or until disk quota reaches 90%.
- Support for the limit and interval parameters (`cmm counter commands`) has been removed.
- The CMM supports close to real-time counter data visualization with an optional possibility to use external Prometheus server with, for example, Grafana integrated on it. In this scenario, the CMM pushes the pre-defined real-time counter set to Prometheus Pushgateway with one minute interval, from where Prometheus server scrapes the counter data for visualizing/analyzing it, for example, with Grafana.

VM statistics based formerly on data provided by Telegraf are provided by a specific process running in every VM.

21.9 PM evolution for component counters (Feature f13012-03)

This feature evolves the performance management (PM) infrastructure to support larger amounts of component counters and much larger number of VMs by aggregating the component counters so that they are on CMM level and not reported per VM. Also, component counters are no longer stored in Influx DB. This minimizes disk usage, CPU usage, and storage and retrieval time.

For component counters (counts collected on a tracking area, routing area, and cell basis), PM aggregation datastores replace Influx DB. TCP communication channel is used.

The following component counter groups are moved from Influx DB to the PM aggregator service:

PID Group	pmJob Group	ENTITY	Group Name
-----	-----	-----	-----
-----	-----	-----	-----

m001	pMobMgmtMts	CELL	GPRS Mobility Management
m002	pSesMgmtMts	CELL	GPRS Session Management
m010	pCellDataMts	CELL	GPRS Cell Data Measurement
m013	pBpfcMts	RA	GPRS BPFC measurement
m016	pIuMmMts	SA	GPRS Iu Mobility Management
Measurement			
m017	pIuSmMts	SA	GPRS Iu Session Management
Measurement			
m020	pIuRaMts	RNC	GPRS RANAP Protocol Measurement
m025	pIuRpMts	IURA	GPRS Iu RA Paging Measurement
m027	pRaPaMts	RA	GPRS Gb RA Paging Measurement
m032	pPlmnMts	PLMNSPECIFIC	GPRS PLMN Measurement
m039	pIppsDataPlmnMts	PLMN	GPRS IPPS Data Per PLMN
m040	pIppsThClsMts	BEARERCLASS	GPRS IPPS Throughput By Class
m042	pSccpSpMts	SPC	SCCP Signaling Point Measurement
m043	pSccpSsMts	SUBSYSTEM	SCCP Subsystem Measurement
m102	cAuthHssMts	HSS	EPS CPPS Authentication Per HSS
m104	cBsmQciMts	OPERDEFQCI	EPS CPPS Bearer Session Management
Per Oper Def QCI			
m106	cCpPlmnMts	PLMNMMSELECTED	EPS CPPS Capacity Per PLMN
m109	cCnPlmnMts	PLMNMMSELECTED	EPS CPPS Connections Per PLMN
m111	cDbQciMts	OPERDEFQCI	EPS CPPS Dedicated Bearer Per Oper
Def QCI			
m113	cGwResMts	GWRESELECT	EPS CPPS Gateway Reselection
m119	cMmHssMts	HSS	EPS CPPS Mobility Management Per HSS
m123	cPagPtMts	PAGINGTYPE	EPS CPPS Paging Per Paging Type
m124	cPagPtaMts	PAGINGTAI	EPS CPPS Paging Per TAI
m126	cRpPlmnMts	PLMNMMEROAM	EPS CPPS Roaming Per PLMN
m135 /Note/	iISvcCmMts	IPDSSOCKET	EPS IPDS Inter Service Communication
m137 /Note/	iIntItMts	INTERFACE	IPDS Interface Per Interface Type
m149	cBsmTaiMts	TAI	EPS CPPS Bearer Session Management
Per TAI			
m150	cDbTaiMts	TAI	EPS CPPS Dedicated Bearer Per TAI
m151	cMmTaiMts	TAI	EPS CPPS Mobility Management Per TAI
m152	cHoTaiMts	TAI	EPS CPPS Handover Per TAI
m155	cConnTaiMts	TAI	EPS CPPS Connections Per TAI
m156	cMiscApnniMts	APNNI	EPS CPPS Miscellaneous Measurements
Per APN-NI			
m157	cMiscPlmnMts	PLMNMMSELECTED	EPS CPPS Miscellaneous Measurements

Per PLMN			
m158	cMiscUeUsageMts	UEUSAGETYPE	EPS CPPS Miscellaneous Measurements
Per UE Usage Type			
m160	dSessRestGummeiMts	GUMMEI	EPS DBS Session Restoration Per GUMMEI

 Note:

Groups m135 and m137 are not aggregated. They are still reported by entity and VM.

PM counter data is stored for 15 minutes at PM aggregator.

Used interval for pushing component counters from VMs to PM aggregator service in NECC is 5 minutes.

 Note:

Measurement group m135 is pushed to PM aggregator in NECC with 1 minute interval even it is containing component counters.

Impact on counter-related CLI commands

Component counters are moved to PM aggregator service, and as a result:

- For a given entity (for example, TAI, RNC, HSS), the counts are aggregated across all VMs. They will no longer be reported by entity+VM.
- The `/data-pm` file will report the count from the VMs with the lowest poolId and poolMember (CPPS-0-0, for example).
- Only 15 minutes of history is held. After that, the data is stored in the `/data-pm` files. Thus, `cmm counter` queries will only return 15 minutes. Values older than 15 minutes will be stored in the `/data-pm` files for 3 days (72 hours) or until disk quota reaches 90%.
- Component counters do not support the `limit` and `interval` parameters (`cmm counter` commands).
- The `cmm pmJob` command (which controls the generation of 5 and 15 minute `/data-pm` files) no longer supports 30 and 60 minute jobs – only 5 and 15 minute jobs are supported. All existing restrictions on the creation of 5 minute jobs have been removed.

21.10 MME support for additional component counters - part 1 (Feature f13033-01)

This feature adds PM component counters per UE HOME PLMN to enhance troubleshooting capabilities of the MME. These counters support a variety of attach (success and failure) and TAU (success and failure) scenarios.

This feature introduces counters from M164C013 to M164C113 in the M164 measurement group.

21.11 MME support for additional component counters - part 2 (Feature f13033-02)

This feature enhances the troubleshooting capabilities of the MME by adding a new set of static and component counters.

This feature introduces the following counters:

- M108: counters M108C072 and M108C073
- M164: counters from M164C114 to M164C270

21.12 MME support for additional component counters - part 3 (Feature f13033-03)

This feature enhances the troubleshooting capabilities of the MME by adding a new set of static and component counters. The component counters are reported per serving PLMN and UE home PLMN.

This feature introduces the following counters:

- M108: counters M108C076 and M108C077
- M136: counters M136C095 and M136C096
- M157: counters from M157C069 to M157C077
- M163: counter M163C061
- M164: counters from M164C271 to M164C292

21.13 MME support for additional static and component counters (Feature f13029-02)

This feature enhances the troubleshooting capabilities of the MME by adding a new set of static and component PM counters.

The feature introduces the following subsets of counters:

- static and component counters per tracking area in order to measure VolTE UE CSFB MO/MT successes
- component counters per operator-defined QCI for Create/Update/Modify/Delete Default Bearer Attempts/Failures

This feature introduces the following counters in the measurement groups:

- M104 (EPS CPPS Bearer Session Management Per Oper Def QCI): 65 component counters from M104C005 to M104C069
- M151 (EPS CPPS Mobility Management Per TAI): M151C078 and M151C079
- M163 (EPS CPPS Mobility Management 2): 4 static counters from M163C079 to M163C082

21.14 CMM support for additional PM counter for CMM system up time (Feature f13036-01)

This feature enhances the troubleshooting capabilities of the CMM by adding a new component counters.

Two counters are added:

- M155: M155C004
- M223: M223C000 (applicable only for the VNF deployment)

21.15 CMM support for enabling Prometheus direct scraping of metrics (Feature f14705-01)

This feature brings more flexibility for using Prometheus with the CMM as the close-to-real-time counter data provider. Previously, only the push mode was provided for the Prometheus Pushgateway. With this feature, the operator can configure the Prometheus server to scrape the data from the CMM. In addition, advanced labelling format where 3GPP counter names are used instead of counter PI IDs, and new label elementType are

included.

This feature supports the Prometheus server to scrape the close-to-real-time counter data from the CMM VNF or the CNF NECC using port 14300 as the front-end port. The traffic, that is, scrape requests and responses, goes through HAProxy in the NECC, supporting TLS encryption and basic authentication (both optional). In addition, rate limiting is supported. The old functionality is referred as the push mode and the basic format whereas the new functionality means the pull mode and the advanced format. With both modes, it is possible to use either the basic format or advanced format.

Here is an example of the basic format presentation (from Prometheus web GUI):

```
m128c004{instance="10.39.144.227:14300", job="esp-ate-117a", poolId="0",
poolMember="0", poolType="CPPS"}
```

Here is an example for advanced format presentation (from Prometheus web GUI):

```
peakCpuUsage{elementType="AMF/MME/SGSN", instance="10.39.144.227:14300", job="esp-
ate-117a", poolId="0", poolMember="0", poolType="CPPS"}
```

21.16 CMM support for "measInfoId" field in performance management reports (Feature f13032-01)

This feature provides an additional field in performance management (PM) reports that operators can use to group sets of PM counters similar to the capability that 3GPP provides with the MeasInfoId architecture. These PM reports are XML files in /data-pm in the NECC.

After the global parameter `measInfoIdUsage` is set to `serviceAndCategory`, the category names that are internally associated with each PM counter are added to the PM XML file.

21.17 CMM support for call trace (Feature f60110-12)

MME supports subscriber and equipment trace (3GPP TS 32.422).

Subscriber and equipment trace

The 3GPP subscriber and equipment trace allows tracing of a specific subscriber based on IMSI or MSISDN. The trace can be activated from command line (management-based call trace) or from HSS (HSS-initiated call trace). Subscriber and equipment trace can be enabled in MME peer elements or for MME's own interfaces. When the tracing is activated for MME's own interfaces, the captured messages are stored as a PCAP file.

The maximum amount of simultaneous traces is 100. The maximum duration of a call trace is 4 days.

When the lifetime limit (less than 4 days) is exceeded, the NECC (cfg_mgr) will delete the entry from the active trace table. This will cause a PCAP file creation if the user had any activity. If there was no activity, no file need to be created.

If trace is activated for the same subscriber using CLI and from HSS, the first one in is activated and the other one is rejected.

MME can be configured to allow or suspend call trace in a major or critical overload condition.

Call trace operations include creating, querying and deleting call trace jobs. Trace data can be queried and created into PCAP files.

Trace data is stored to the database in NECC for 4 days maximum.

Data stored from CLI or HSS-initiated call trace can be displayed, or it can be created into PCAP and viewed using a tool such as Wireshark. However, DNS interface message captured by CPPS will not be decoded by off-the-shelf Wireshark.

HSS-initiated call trace

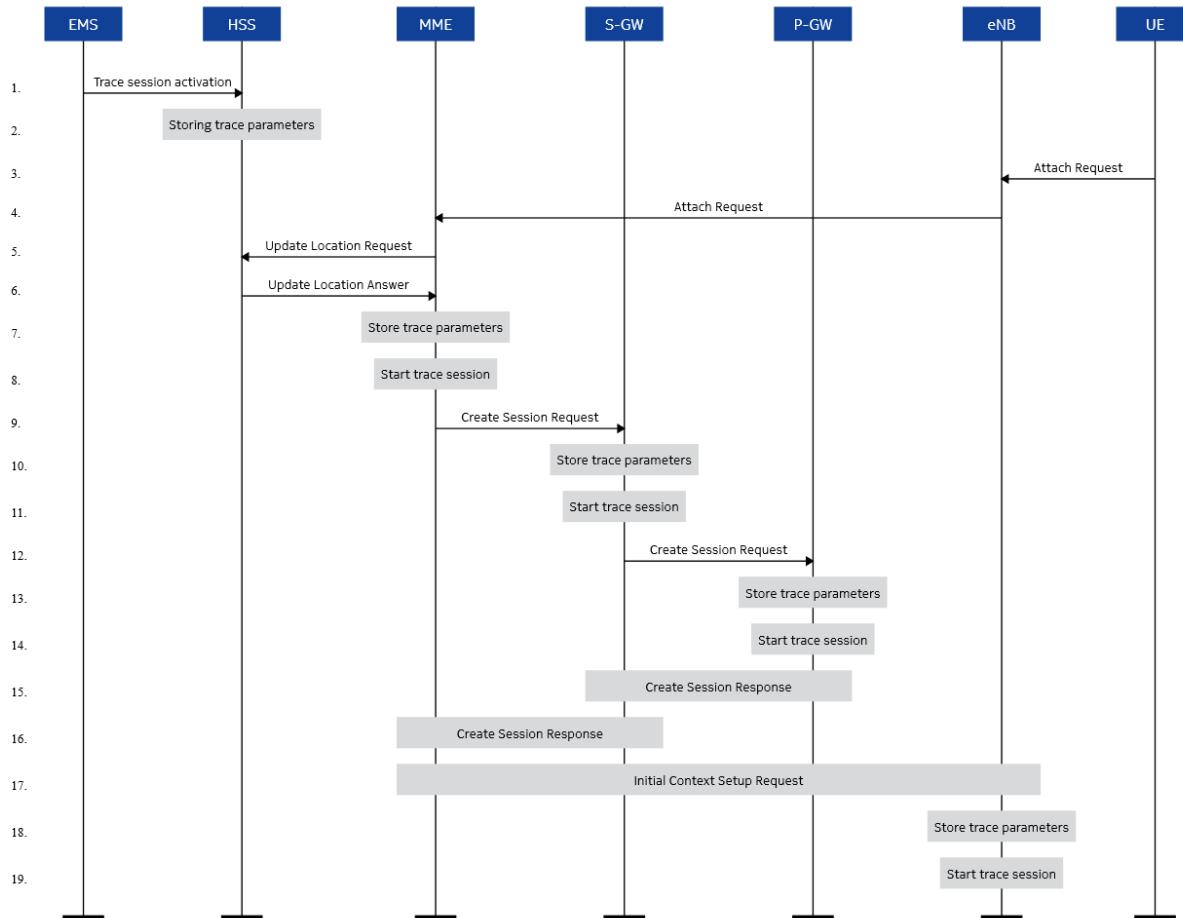
With HSS-initiated call trace, the HSS messaging contains information that indicates to the MME that a call trace for a given UE must be initiated or terminated. In contrast to management activation of call trace, HSS-initiated call trace parameters are configured in the HSS and propagated from the MME to the S-GW (over S11) and to the eNB (over S1-mme) and between MMEs (over S10). HSS-initiated call trace provides the capability of network-wide tracing with UE mobility. Support for HSS-initiated call trace complies with 3GPP TS 32.422.

HSS needs to initiate the trace by sending a Diameter TRACEDATA AVP. HSS-initiated call trace parameters are configured in the HSS, passed to the MME in Update Location Answer and Insert Subscriber Data messages, and propagated from the MME to the S-GW (over S11) and to the eNB (over S1-mme) and between MMEs (over S10):

```
{TRACEREFERENCE %tracerefERENCE}
{TRACEDEPTH %tracedepth}
{TRACENETYPELIST %tracenetypelist}
{TRACEINTERFACELIST %traceinterfacelist}
{TRACEEVENTLIST %traceeventlist}
{OMCID %omcid}
{TRACECOLLECTIONENTITY %tracecollectionidentity} }}
```

HSS-initiated call trace can be enabled in MME using a global parameter.

Figure 178: HSS-initiated call trace



21.18 CMM support for source and destination IP and port preservation in call trace - Phase 1 (f13402-01)

This feature enhances call trace on the MME by preserving the local and remote endpoints of the supported external interface's traced message packets.

By preserving the local and remote endpoint information for traced external or internal message packets, the MME allows for a more accurate analysis of where the message packet travels and aids in troubleshooting call procedure issues. For multi-homed (MH) SCTP interfaces, the IP addresses of the primary paths of the local and remote endpoints are always added, regardless of which path was used.

On the DNS, NAS, and NR10 CMM-supported proprietary interfaces, call traced messages are representative of the actual messaging. These interfaces do not show the actual message sent or received on the external interfaces, but can be used to understand the message flow. In some cases, the actual information is encrypted in the external network; in others, there may or may not be an actual external message sent or received. The DNS and NAS proprietary interfaces do not have a defined external interface or corresponding link.

- The MME call Trace (CT) supports a proprietary DNS “interface” in CPPS to aid in the understanding of call processing DNS activities. As it is not possible for the CPPS CT to know the entire route and IP information of a DNS query or response, the CPPS host IP addresses are provided for both the local and remote endpoints for the CPPS CT-captured DNS packet.
- The MME CT supports a proprietary NAS “interface” in CPPS to aid in the understanding of CPPS S1AP NAS PDU encoding and decoding. This is especially useful if the UE’s S1AP NAS PDU is integrity protected and ciphered. As NAS is not a real external interface and link, the dummy local and remote IP addresses (10.0.0.0 and 20.0.0.0) and ports are used for the CT-captured NAS packet.

For a configuration with multiple IPDS, an interface proxy in the CPPS does not know which IPDS link will be used until the first call procedure is completed. For example, first the session request is created, then a response is received from the S11 interface.

21.19 MME support for UE counts per eNB (Feature f14117-01)

With this feature, the MME supports two commands: `enbUeQuery` **and** `enbUeQuerySum`.

With the `enbUeQuery` command, the MME can retrieve the information of the number of UEs per connected eNBs. The command is used to retrieve the relevant information from all

connected eNBs. The relevant output can be shown on screen with up to 20 lines of data. This command can also be used to create a file with all output.

With the `enbUeQuerySum` command, the MME can provide the overview information about the total number of eNBs, total number of S1 connections, and total number of disconnected eNBs.

21.20 Management activation for area-based minimization of drive test (Feature f10918-01)

This feature introduces minimization of drive test (MDT) functions.

The minimization of drive test (MDT) feature is a mechanism used to control and configure trace. For the area-based MDT, the MDT data is collected from UEs in a specified area. The area is defined as a list of cells (UTRAN or E-UTRAN) or as a list of tracking/routing/location areas. Area-based MDT can be either a logged MDT (collection of UE measurements in idle mode) or immediate MDT (collection of UE measurements in connected mode).

When the minimization of drive test feature is enabled and a UE attaches to the network, the MME stores the user consent information forwarded by the HSS.

The MME checks the roaming status of the UE. If the UE is in the home PLMN and the user consent information is included in the subscriber data record (SDR), the MME sends the management-based MDT Allowed IE to the eNB during the UE context setup procedure. The MME also forwards the already-stored user consent information to the corresponding eNB with the management-based MDT Allowed IE.

Management-based MDT Allowed IE is included in:

- Handover Request message when the MME is the target for an inter-system handover.
- Forward Relocation Request message when the MME is the source for an inter-system handover procedure.
- Initial Context Setup Request message when the MME is the target for an idle mode TAU procedure.
- Context Response message when the MME is the source for an idle mode TAU procedure.

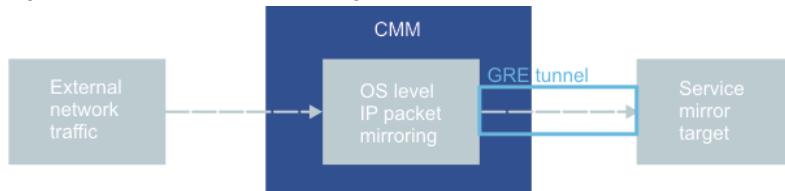
21.21 Service mirroring (Feature f13401-01)

This feature provides service mirroring capability for the IPDS and the PAPS on the CMM.

The service *mirroring* feature allows the external IP traffic to be replicated in real time,

encapsulated within the GRE tunneling protocol and sent to an external target IP address.

Figure 179: Service mirroring



Service mirror is created per IPDS or PAPS. Only one service mirror is supported per IPDS or PAPS. By default, all external traffic is mirrored. A service mirror session is operationally disabled when resources reach an overload condition. The session is operationally enabled once the overload condition has abated.

A separate network is recommended for sending service mirror traffic. A GRE tunnel is defined to carry the service mirroring traffic. The GRE tunnel can be either IPv4 or IPv6.

Service mirroring sessions are automatically locked after one hour or upon excessive operational state transitions. In such cases, unlock the service mirroring session in order to re-enable traffic replication.

21.22 Service mirroring enhancements (Feature f13401-02)

This feature enhances the duration of service mirroring. An operator can now control the duration of the port mirroring.

Originally, service mirroring had a one-hour limit for any mirroring session. Service mirroring sessions are automatically locked after one hour or upon excessive operational state transitions. In such cases, the service mirroring session must be unlocked in order to re-enable traffic replication.

With this feature, an operator can modify the duration of service mirroring session with command `cmm serviceMirror --timeLimit`.

21.23 OAM enhancements (Feature f13204-01)

The `cmm_monitor` command is modified to provide more useful data for the VM size checks. There are new checks for the minimum requirements of the vCPUs, memory and root disk size. Also CMM configuration type is detected. The `cmm_monitor` command verifies that the deployment meets the minimum requirements of the detected CMM

configuration.

21.24 Syslog collection and streaming to remote server (Feature f13207-02)

With this feature, the CMM supports the sending of message logs from NECCs to a remote logging server.

If configured, the CMM streams syslog data from all NECCs.

Transport layer security (TLS) certificates are created before client configuration. The `syslogAdmin` command is used to specify the remote IP address, port, and name for the remote syslog server and to set the protocol used. The message logs are from the `/var/log/messages` and `/var/log/secure` files.

For information about how to configure syslog collection and streaming, see the *Security* document.

21.25 Event logging of PDN connectivity failures (Feature f10170-01)

With this feature, the MME supports recording event logs to capture logging of PDN connectivity failure with ESM cause code #27 for IMS APN only. IMSI, MSISDN and IMEI are captured as part of the log.

When this feature is enabled, attach or standalone PDN connectivity procedures with IMS APN are rejected with cause #27 if the subscription does not have an IMS APN specifically subscribed. This means the procedure is rejected even if the subscription has wild card APN with QCI 5. A log is written to master log with the user's IMSI, IMEI and MSISDN (if available).

The feature is disabled by default (IMS APNs are accepted with only wild card in the subscription) and can be enabled through the global parameter `attachRejForUnsubImsApnWithLogging`.

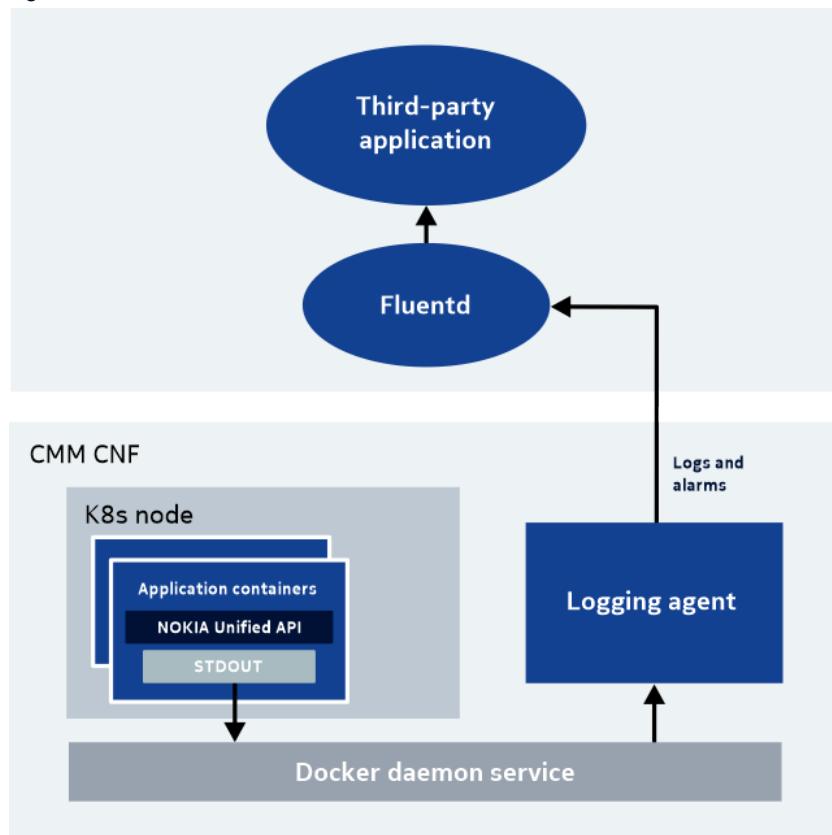
21.26 CMM support for sending log and alarm information to stdout in addition to current destinations (Feature f14402-01)

Cloud native applications typically use the infrastructure to forward information to NB

clients. With this feature, the CNF CMM configuration supports sending selected logs and alarms to stdout in addition to all legacy handling.

This feature adds support for using the stdout mechanism to capture logs and make them accessible to Fluentd only for the CNF configuration of the CMM. Fluentd is an open source data collector for building unified logging layer. Once installed on a Kubernetes server, it runs in the background to collect, parse, transform and store various types of data, as shown in Figure *Stdout and Fluentd on a CNF CMM*.

Figure 180: Stdout and Fluentd on a CNF CMM



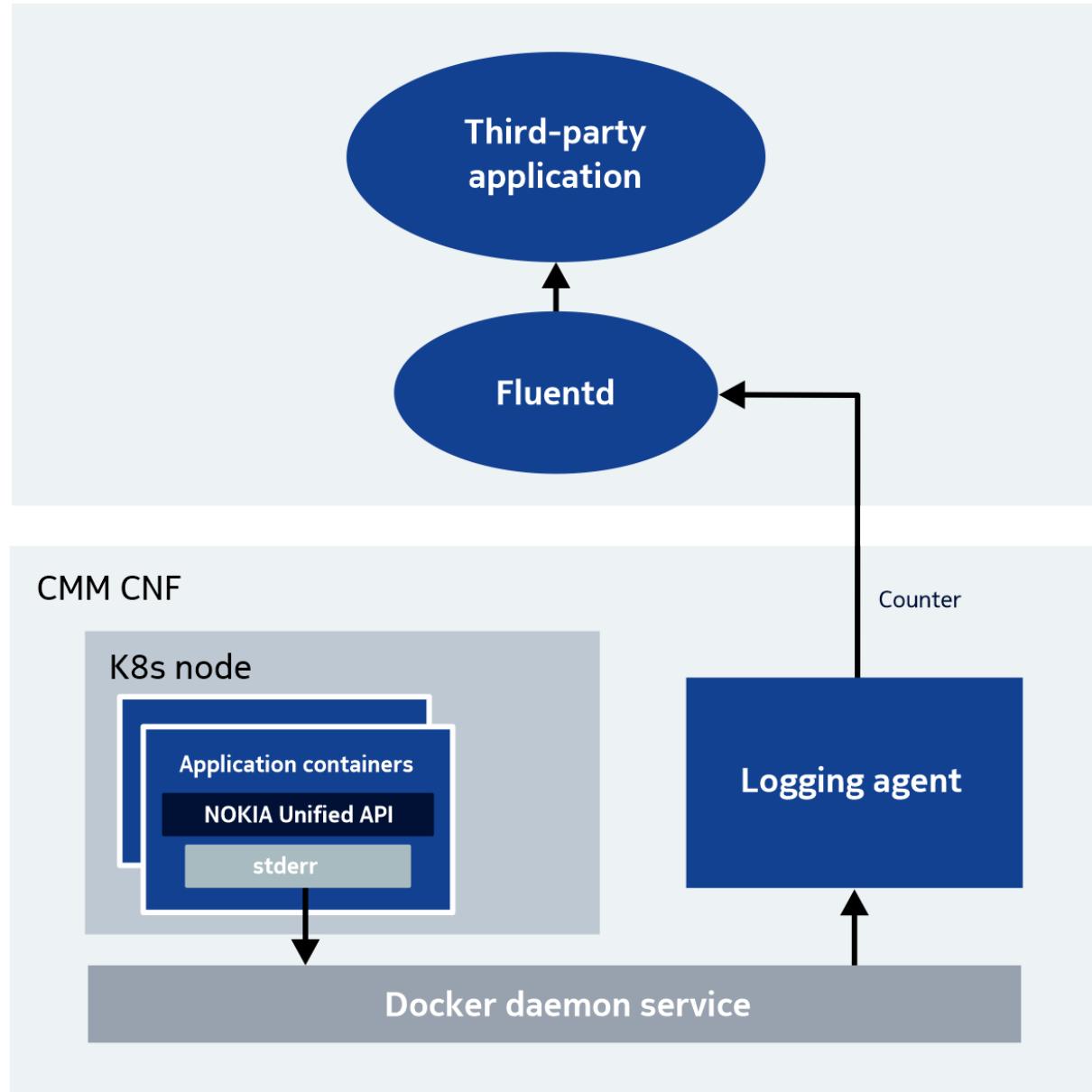
Selected CMM logs are sent to the host side via stdout. Normally the host side writes logs to the `/var/log/containers/` directory. The CMM logs are sent in JSON format, but the host side ultimately decides how they are handled. Refer to the *MME User Guide* for detailed information about fields used for alarms and logs.

21.27 CMM support for streaming PM XML file to Fluentd (Feature f14402-03)

This feature supports using the standard error (stderr) mechanism to capture counters and make them accessible to the Fluentd only for the CNF CMM.

The Fluentd is an open-source data collector for building the unified logging layer. Once installed on a Kubernetes server, it runs in the background to collect, parse, transform, and store various data types.

Figure 181: Fluentd on a CNF CMM with stderr



The data produced by this feature is based on the PM XML file that is generated every 15 minutes. This feature ignores the PM XML file that is generated in 5-minute interval. Counters are pushed to the host side from NECC-0 and NECC-1 only. Each NECC handles only its own set of counters. The time used to push counters can take close to 15 minutes to ensure that system does not get overloaded. To reduce the number of generated counters, most counters with zero value are ignored. Exception are counters that calculate averages, maximum or minimum values or counters with meaningful zero values.

The CMM produces counters with the JSON format. Each counter is pushed to stderr as an independent JSON line. The host side captures this output and can write them as logs under `/var/log/containers/` per container. The host side configuration determinates how logs are handled and what output is. The Fluentd can track the generated log file and handle counters as needed. The JSON format includes the pod details, the counter name, and the value, in addition to the potential component level information.

Table 84: Additional component type fields included in JSON

Measurement group	Additional component type fields included in JSON
M001	PLMN, LAC, RAC, CELLID
M002	PLMN, LAC, RAC, CELLID
M010	PLMN, LAC, RAC, CELLID
M013	PLMN, LAC, RAC
M016	IUSAPLMN, IUSALAC, SAC, IURAPLMN, IULAC, IURARAC, IURARNC
M017	IUSAPLMN, IUSALAC, SAC, IURAPLMN, IULAC, IURARAC, IURARNC
M020	PLMN, RNCID
M025	IURAPLMN, IULAC, IURARAC, IURARNC
M027	PLMN, LAC, RAC
M032	PLMN, ACTC, PLTC
M039	PLMN
M040	BEARERCLASS
M042	SNET, SPC
M043	SNET, SSNUMBER, SSNAME
M102	HSS
M104	OperDefQCI
M106	PLMN
M109	PLMN
M111	OperDefQCI

Measurement group	Additional component type fields included in JSON
M113	Reselection
M119	HSS
M123	PagingType
M124	PLMN, TAC
M126	PLMN
M130	FileSystem
M135	partner
M137	InterfaceType
M147	Interface
M149	PLMN, TAC
M150	PLMN, TAC
M151	PLMN, TAC
M152	PLMN, TAC
M153	Core
M155	PLMN, TAC
M156	APNNI
M157	PLMN
M158	UeUsageType
M160	PLMN, MMEGI, MMECI
M162	PLMN, PagingType
M164	PLMN
M189	PagingType
M194	5GPLMN, TAC
M195	5GPLMN, TAC

Measurement group	Additional component type fields included in JSON
M200	Proxy
M202	Proxy
M203	5GPLMN, TAC
M204	SST, SD
M208	UE5GPLMN
M209	SERVING5GPLMN
M210	UE5GPLMN
M213	Proxy
M214	APPERROR
M215	SERVING5GPLMN
M217	OLDSERVING5GPLMN
M218	UE5GPLMN
M219	NFType, NFEntity, HttpStatusCode
M220	NFType, NFEntity, HttpStatusCode
M221	NFType, NFEntity, HttpStatusCode

21.28 CMM support for inactive session timeout configurable in CMM CLI (Feature f13213-02)

This feature provides the ability to configure an inactivity time-out period for OAM users' interactive sessions.

This feature allows an OAM user interactive session to be terminated automatically after a specified period of inactivity. It is possible to configure an inactivity time-out period with command `oamSession`. Allowed values are from 30 seconds to eight hours and the default value is one hour.

Special users, for example, sam5620, cgw, orchest, rsp, ca4mn, dcae-dfc and cmm_fallback -

users, which need to be always connected are excluded from the functionality.

21.29 CMM support for authentication of NTP server (Feature f13213-05)

The network time protocol (NTP) is a networking protocol for clock synchronization between the computer systems over packet-switched and variable-latency data networks. The authentication support allows the NTP client to verify that the NTP server is trusted.

The NTP client authenticates the packets of NTP server with symmetric keys.

The network time security (NTS) for the NTP is a new authentication mechanism specified by the IETF for the NTP. It allows the clients to verify that the packets they received from the server are not modified while transiting.

The NTS includes a key establishment (NTS-KE) protocol that automatically creates the encryption keys used between the server and its clients. The NTS uses the TLS on TCP port 4460 to establish the keys. The NTS provides the clients with cookies, which are encrypted and contain the keys needed to authenticate the NTP packets. The NTP packets are authenticated with authenticated encryption with associated data (AEAD).

21.30 CMM support for OAM alignment (Feature f14516-01)

This feature provides OAM alignment across MME, SGSN, and AMF configurations.

This feature eliminates the ELK SW stack (Elasticsearch, Logstash, and Kibana). As a result,

- call trace data is moved to RedisDB
- applications that previously used Elasticsearch have been updated
- 'web' user group, previously used for accessing Kibana, has been removed
- CLI commands `logData`, `logDataStatus`, `logLiData`, `logLiDataStatus`, and `healthMon` are removed
- software upgrade does not back up Elasticsearch logs

Additionally:

- CLI command `cmm help` has an enhanced output, organized by application (common, AMF, MME, SGSN or any combination).
- CLI commands `counter`, `counterdefinition`, and `counterGroupDefintion` also

display AMF counters.

21.31 Trap notification enhancements (Feature f14618-01)

With this feature, you can create and provision an SNMP trap destination for both default and non-default CMM SNMPv3 users. You can create and provision a custom noAuthNoPriv SNMPv3 non-default user, instead of being limited to use of pre-defined SNMPv3 default users. Previously, SNMP trap notifications were allowed and forwarded only to pre-defined SNMPv3 default users. With this feature, SNMP trap notifications also work for non-default SNMPv3 users.

Use the existing `emsTrapNotification` command to create a custom SNMP user. When you specify an SNMP user name that does not match any of the SNMP default user names, the new user is created with noAuthNoPriv access. For related information, see *Configuring SNMP* in the *SGSN User Guide* for your deployment scenario.

21.32 CMM support for network trace/trace all for MME/SGSN CNF (Feature f23401-02)

This feature allows the CMM to perform network tapping of all MME/SGSN signaling messages.

When this feature is enabled with a global parameter, a custom-sized IPDS is used to provide the messaging streaming towards a capture server (an external packet collector). This feature applies to the CNF only.

The CMM connects to the capture server over HTTP2 and is TLS1.2 encrypted.

If the feature is activated, then all active IPDS pods attempt to connect to the capture server. If the connections are not possible, a retry is made every 5 seconds indefinitely. If the connection to the capture server is lost after a successful connection, then the IPDS pods attempt to re-connect. If a connection is not possible, a retry is made every 5 seconds, indefinitely. During the connection loss to the capture server, the captured messages that do not fit into IPDS buffers are dropped.

If the IPDS overloads, then tapping is stopped and the following message is displayed: "Stopping network trace due to critical overload". When the overload is cleared, tapping is resumed and the following message is displayed: "Resuming network trace after critical overload".

This feature introduces a new interface for the IPDS. The NETWORK_TRACE NI type should be used when the service IP is created.

Note:

The connection between the IPDS and the external packet collector should be over a high throughput IP link.

21.33 CMM support for show command to display 20 representative IMSIs for an input PLMN (Feature f13406-01)

This feature introduces a new show command on the CMM that displays 20 (default value) representative IMSIs for an input PLMN. The input parameters include the PLMN and the radio access type. The output of the command is the PLMN, the RAT and the IMSIs. This feature is supported for the 2G/3G/4G/5G network.

The new CLI command is created to query the lead IPDS map table to display at most 100 matching IMSIs per PLMN (considering the UE's MCC and MNC) entered. By default, 20 representative IMSIs are displayed. The command examines coherently the lead IPDS UE context map. The output displays the list of the IMSIs belonging to the PLMN. The user can clear the created IMSI list with the `taskOp clear` parameter of the `subsImsiDisplayAdmin` command.

21.34 CMM support for CMPv2 protocol (Feature f13216-01)

This feature enables the CMM to support the CMPv2 protocol. The certificate management protocol (CMP) is an internet protocol standardized by the IETF used for obtaining X.509 digital certificates in a public key infrastructure (PKI).

In a public key infrastructure (PKI), the end entities (EEs) act as the CMP client, and request the certificate for themselves from a certificate authority (CA). The CA issues the TLS certificates and acts as a CMP server (for example, the PKI server). The CMM is always the CMP client.

The CMP client can utilize the CMP to obtain the TLS certificates from a CA, request TLS certificate updates, and get the TLS certificates revoked. The use of the CMP replaces the

`scp` and `sftp` commands used to copy the TLS certificate files and certificate revocation list files to the NECC disk.

The following CMPv2 operations are supported:

Initial registration (IR) The CMM obtains a certificate from a certain CA for the first time.

Certificate update (CR) The CMM obtains additional certificates from the CA.

Key pair update (KUR) The CMM updates an existing TLS certificate for any reason, such as a key or certificate refresh before the key or certificate expires.

Certificate revocation list (CRL) The CMM obtains a certificate revocation list (CRL) from the CA.

Polling In some cases, the CA may not immediately return the certificate. The CMM supports polling requests and responds. Polling is used for the IR, CR, and KUR operations. The CMM raises a critical alarm when a CMPv2 operation fails due to a polling failure. The alarm is deleted when the next CMPv2 operation with the CA succeeds.

The CMM only requests one certificate in each IR, CR, and KUR message.

The CMP provides inbuilt integrity protection and authentication.

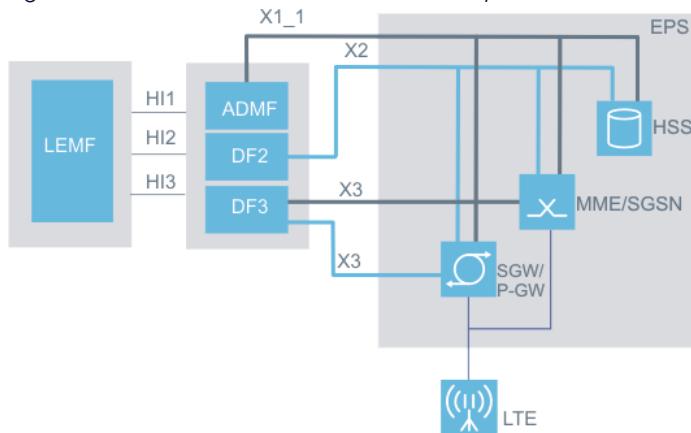
22. MME/SGSN support for lawful interception

In the evolved packet system, MME-only and MME/SGSN deployments of CMM support IP layer interception of content of communication (CC) data. The LI solution for EPS generates intercept related information (IRI) records from control plane messages.

The networking architecture for lawful interception is shown in the figure with the MME/SGSN's administrative interface to the administration function (ADMF) over X1_1, and to the delivery function 2 (DF2) distribution function over X2.

The DF3 network element handles the content of communication (CC) messages over X3. The X3 interface is supported only for LIPv2 specification for SGSN.

Figure 182: MME/SGSN lawful interception architecture



The following table summarizes the LI functions and their corresponding VM/link usage.

Table 85: LI functions and VM/link usage

LI function	VM entity	Link used
Administration	ADMF/LIC	X1_1
Event reports	DF2/LIB	X2
Content of communication	DF3/LIB	X3

Handover interfaces

Communication between the network operator and the LEA is performed using the

handover interface (HI). The HI interface is implemented as part of the regional mediation function and is provided by the administration function (ADMF) and delivery function (DF). The lawful interception standards provide for HI1, HI2, and HI3 handover interfaces.

- HI1 interface represents the interface between the law enforcement monitoring facility (LEMF) and the lawful interception administration function (ADMF) in the service provider's network.
- HI2 interface represents the interface between the lawful interception agency (LEA) and the delivery function responsible for distributing the intercept related information (IRI) to the relevant LEA.
- HI3 interface represents the interface between the LEA and the delivery function responsible for distributing the content of communication (CC) to the relevant LEA.

Lawful interception administration function

The lawful interception administration function varies among service providers and is used for activation, deactivation, and interrogation of lawful interception. The ADMF:

- Interfaces with all the LEAs that require interception in the intercepting network.
- Keeps the intercept activities of individual LEAs separate.
- Interfaces to the intercepting network.

When the LIPv2 interface specification is used, this ADMF is commonly referred to as the lawful interception controller (LIC).

Lawful interception delivery function

The delivery function (DF) is the portion of the LIG responsible for the collection of messages from the lawful interception extension (LIE) network elements and the delivery of this content to the LEAs. A DF2 network element handles the delivery of IRI messages and a DF3 network element handles the delivery of content of communication (CC) messages.

When the LIPv2 interface specification is used, this DF is commonly referred to as the lawful interception browser (LIB).

Encryption

- LI surveillance target records are automatically encrypted on the lawful interception handling service (LIHS).
- The LIPsec encryption mechanism is supported for use with the LIPv2 interface specification.



Note:

CMM supports LIPsec only on the X1_1 interface.

- IPsec is supported on the LIHS, PAPS, and IPPS to protect the X1_1, X2, X3_2G, and X3_3G interfaces.
- Libreswan 3.25 is used to support IPsec on the X1_1, X2, X3_2G, and X3_3G interfaces.

The following IPsec attributes are supported:

- Internet key exchange (IKE) key exchange version 1 and version 2.
- Encryption methods aes, aes128, aes256, 3des.
- Hash functions sha1, sha2_256, sha2_384, sha2_512 and md5.
- Perfect forward secrecy (PFS) groups modp1024, modp1536, and modp2048.

Capacity

With LIPv2, the maximum number of connections is:

- 5 connections to LIC per node, thus maximum 5 X1_1 connections in the SGSN/MME.
- 10 LIBs/LIC, thus maximum 50 LIBs with 5 LICs per node.

With ASN.1, the maximum number of connections is:

- Up to 5 X1_1 transmission control protocol (TCP) connections to an ADMF for administering target identities. If an X1_1 link between the MME/ADMF goes down, an alarm is raised.
- Up to 6 primary X2 TCP connections to an LIG (DF2) for processing IRI messages. If an X2 link between the MME/LIG goes down, an alarm is raised.

General LI capacity:

- Total stored targets are 150 000 (AMF/MME/SGSN or AMF/MME or AMF or MME).
- Up to 1000 UEs with LI surveillance active is supported per CPPS.

With X2 interface, for 2G/3G subscribers, up to 8 PDP contexts are included in IRI event reports.

Related descriptions

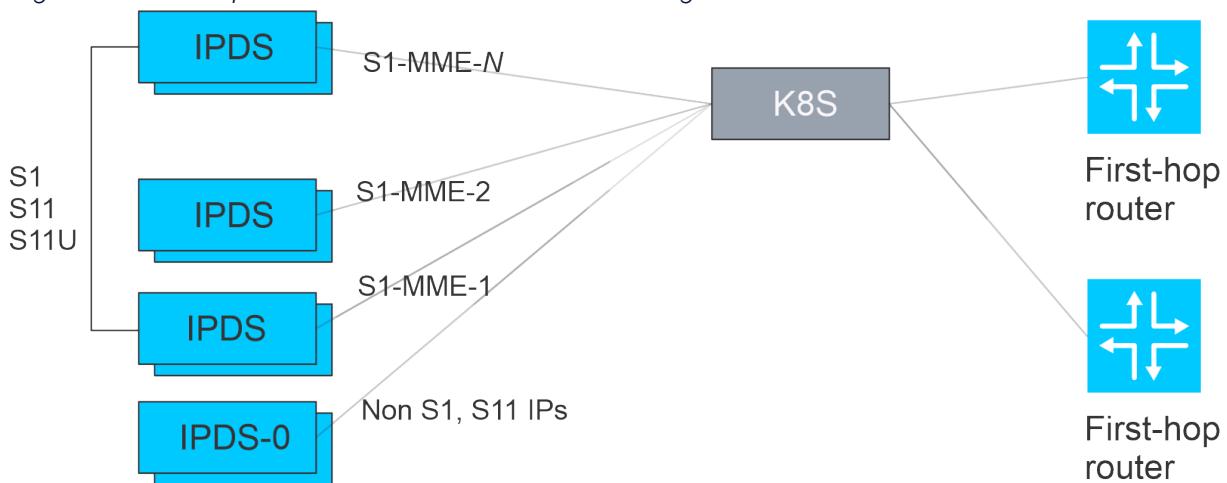
- [Configuring MME/SGSN LI](#)

23. Multi-IPDS deployments on CNFs

The CMM supports M-IPDS on quad access CNF deployments.

The feature *CMM support for Quad Access - Delivery (Feature f20060-05)* introduced support for M-IPDS on the CNF for quad access deployments. Separate IP addresses are provisioned for each IPDS pair, for each interface.

Figure 183: Example of a CNF MME multi-IPDS configuration



The MME M-IPDS implementation on the CNF differs from the implementation on the VNF; VSR is not supported on CNF, so there is no L3NS steering function. Instead, the high throughput interfaces (M3, S1, S11, and S11U) can be spread manually via provisioning.

The following restrictions apply:

- S1, M3, S11, and S11U are high throughput interfaces. High throughput interfaces cannot be configured on pool 0 of an M-IPDS configuration.
- Non-high throughput MME and SGSN interfaces must be configured on IPDS pool 0.

23.1 CMM support for MME and AMF using flow distribution - delivery (Feature f72002-43)

For MME-only and AMF-only configurations, the CNF CMM supports a flow distributor using multiple IPDS instances with the Linux stack. The flow distributor distributes S1, S11, S11-U, and N2 traffic.

Flow distributor pods act as forwarding devices and take packets from the external network and distribute them to the IPDS pools based on their source IP address.

The flow distributor pods use SR-IOV on their external-facing networking interfaces and SR-IOV on their IPDS-facing networking interfaces to act as the front end for S1, N2, S11, and S11U traffic. The flow distributor pods are as follows:

- The SCTP flow distributor service (SFDS) handles S1-MME (SCTP single-homing) and AMF (N2 single-homing) traffic.
The SCTP acts as a single-entry point for signaling by steering the traffic among the multiple IPDS instances. S1-MME and N2 traffic are load balanced among the various IPDS instances, while the non-S1MME and non-N2 signaling traffic are routed directly to the specified IPDSs. The SCTP also acts as a layer 3 forwarding device between the next hop routers and the IPDS services for S1-MME and N2 signaling.
- UDP flow distributor service (UFDS) handles S11 and S11U (UDP) traffic.
UFDS acts as a single-entry point for signaling by steering the traffic among the multiple IPDS instances; S11 and S11-U traffic are load balanced among the various IPDS instances, while the non-S11 and non S11-U signaling traffic are routed directly to the specified IPDS pairs.

The flow distributor pods are based on vector packet processing (VPP). The flow distributor pods use SR-IOV on their external-facing networking interfaces and SR-IOV on their IPDS-facing networking interfaces. The flow distributor pods use SR-IOV CNI for external Multus interfaces when deployed on bare metal (CN-B) and host-dev CNI when deployed on top of a VM (CN-A).

The SFDS and UFDS follow the 1+1 redundancy model (active-standby). For the SFDS and UFDS pods, duplex EIPM_ARPNDP monitoring handles the redundancy between the Ethernet interfaces towards external routers. Only one of the Ethernet interfaces is active. The active interface handles ARP messaging and neighbor discovery protocol (NDP) to the gateway address. When three or more ARP or NDP messages are lost, duplex EIPM_ARPND switches to the standby Ethernet interface. Duplex EIPM_ARPNDP also handles the redundancy between the interfaces on the flow distributor pods that are connected to the IPDS pairs that they serve. The IPDS being served by a flow distributor pod uses IP VLAN; the VLAN interfaces are bonded. Only one of the VLAN interfaces is active.

For related information, see the following documents:

- *IP Connectivity*
- *Integrating CMM or Integrating AMF*
- *Container Lifecycle Management and Software Upgrade*
- *Product Description*

23.2 CMM support for flow distributor with multi-home and dynamic flow control (Feature f72002-48)

This feature provides a CNF front-end distribution service for S1, N2, S11, and S11-U signaling traffic. This service reduces the number of externally visible IP addresses in the configuration when multiple IPDS are required.

The flow distribution functionality (introduced with feature f72002-43) is expanded to support the following:

- IPv6 and dual-stack connectivity
- multi-homing for the SCTP S1/N2 links
- dynamic distribution flow based on the overload control direction
- AMF-MME-SGSN and AMF-MME configurations in addition to the MME-only and AMF-only configurations

24. Software architecture

This section describes architecture features for CMM deployments with MME.

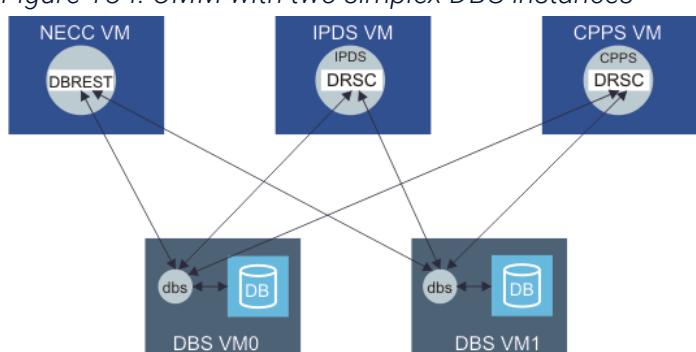
24.1 MME support for simplex DBS (Feature f14111-06)

This feature supports the deployment of an MME-only CMM in simplex DBS VM configuration.

In simplex DBS configuration, all **N** DBS instances actively store user context data, in addition to CPPS cache. There is no DBS active-standby redundancy; if the active DBS instance fails, no switchover or failover occurs. This configuration helps the customer reduce the VM footprint, but at the cost of additional redundancy. Duplex DBS VM configuration continues to be supported.

The overall architecture of the CMM is the same for simplex and duplex DBS configuration, except that in simplex configuration, each DBS pool has only one DBS in the active state. Each DBS continues to have the fixed IP address, as well as a floating IP address. The applications running in NECC, IPDS, and CPPS open TCP channels to the DBS instances using floating IP addresses for both simplex and duplex configurations. In the MME, UE context is stored in CPPS VLR cache, then check-pointed to the active DBS, which is then check-pointed to the standby DBS. In simplex configuration, there is no active to standby check-pointing.

Figure 184: CMM with two simplex DBS instances



Simplex DBS configuration is applicable to MME-only and MME/SGSN (provided by *f14111-07 - SGSN support for simplex DBS*) configuration on OpenStack and VMware deployments; it is not applicable to appliance deployments. Two DBS VMs are required for simplex deployment.

During CMM deployment, to specify simplex DBS configuration, the parameters section of configuration file should be set with `dbs_duplex: false`.

With simplex configuration, you can deploy odd number of DBS VMs (in contrast to duplex growth, where DBS is grown in pairs).

24.2 CMM support for flexible size CPPS/DBS for MME/TA/AMF on OpenStack - Delivery (Feature f80005-10)

This feature delivers support for flexible-sized CPPS and DBS on OpenStack deployments. The features, *MME support for flexible size CPPS (Feature f80005-03)* and *CMM support for flexible size DBS (f80005-15)*, deliver the functions. This feature allows a service provider to better optimize use of available cores and memory of the cloud host based on their network requirements.

Options for CPPS and DBS VM sizes are shown below.

Table 86: CPPS and DBS VM size options

VM	vCPU per VM	VRAM [GB]
DBS	8	16
	8	20
	8	24
	8	28
	8	32
CPPS	10	28
	12	32

Flexible CPPS and DBS sizing is available on OpenStack MME-only, MME/SGSN, and AMF deployments. Flexible sizing is not supported on other VMs; for information about supported VM sizes, see *Resource requirements* in the *Product Description* or lifecycle management documents.

CPPS and DBS VM size is specified during CMM instantiation. For instructions, see the lifecycle management document for your deployment scenario. Within a CMM, all DBS VMs

must be of the same size. Similarly, all CPPS VMs must also be of the same size.

When selecting a CPPS VM size, consider also the DBS VM size. For example, a CMM AMF deployment for a maximum of 1M UEs can be supported with a minimum of 5 CPPS VMs of size 28GB/8vCPUs and 3 simplex DBS VMs of size 24GB/8vCPUs.

Related descriptions

- [Overload control](#)

24.2.1 MME support for flexible size CPPS (Feature f80005-03)

This feature supports two CPPS size options: 10 vCPUs with 28 GB of RAM and 12 vCPUs with 32 GB of RAM.

This feature provides the following CPPS size options:

Table 87: CPPS VM size options

CPPS size option	Number of CPPS vCPUs	CPPS RAM (GB)	Maximum number of UEs served by CPPS	Suggested when the priority is...
1	10	28	350,000	efficient memory utilization of the cloud host
2	12	32	500,000	maximizing call processing capacity (that is, the processing messages handled per second)

24.2.2 CMM support for flexible size DBS (Feature f80005-15)

The flexible size DBS is applicable to OpenStack MME, MME/SGSN, and AMF deployments and can be used on both duplex and simplex DBS configurations. DBS VM size is specified at the time of CMM instantiation and therefore all DBS VMs are sized equally. While the 8

vCPU size is fixed for all configurations, memory size of 16GB & 20GB are more practical for smaller deployments, while 24GB, 28GB, and 32GB size are recommended for deployments according to the underlying hardware capacity and needs.

Following are the DBS size options for commercial OpenStack deployments:

Table 88: DBS VM size options

vRAM [GB]	vCPU per VM
16	8
20	8
24	8
28	8
32	8

Note:

Within a CMM, all DBS VMs must be of the same size.

24.3 Support for quad access (Feature f20060-05)

With this feature, the CMM supports quad access application types for combined instantiations.

The CMM supports the following additional RAT type combinations:

5G-4G AMF-MME, with both personalities of CPPS

5G-4G-2G/3G AMF-MME-SGSN, with both personalities of CPPS and PAPS

For details, see the *Supported deployment scenarios* in the *Product Description*.

This feature provides the following changes:

- CPPS personalities support 4G vs 5G decisions to be made in CPPS software:

EMMS allocates only resources needed by 4G call processing code

AMMS allocates only resources needed by 5G call processing code

CPPS personality is specified during instantiation and persists in the DBS.

The following commands display CPPS personality information for quad access deployments:

- ❑ `cmm serviceState list --personality <list-item>`
- ❑ `cmm serviceStatus list --personality <list-item>`

For quad access deployments, the `cmm restorationEndPtList list` command displays the type of restoration end point for the pool.

- This feature provides a more efficient way of memory use in the IPDS software to allow a VM or pod to support quad access configuration. The hash tables that store mapping of identifiers (MTMSI, TEID, 5G-TMSI, and PTMSI) are allocated and reallocated dynamically, instead of being allocated during initialization.
 - This feature enhances the CPPS selection mechanism to select the correct personality. The CMM distributes 4G traffic in EMMS CPPSs and 5G traffic in AMMS CPPSs. The CMM automatically load balances 4G UEs among EMMS CPPSs and 5G UEs among AMMS CPPSs.
 - The DBS stores 4G and 5G data separately and procedure handling for QA call processing. UE contexts are stored in DBS where 4G subscriber data are kept separately from 5G subscriber data. Thus, when a CPPS personality attempts to fetch or update the subscriber data, the DBS acts only on the subscriber data that is relevant to the CPPS personality.
 - Intra CMM mobility between the MME and AMF loops the N26 messages internally for the N26 interface. During intra CMM (intra node) mobility procedures between the MME and AMF, IPs for the MME and AMF are different, but on the same IPDS. Messages over the N26 interface are routed over the IPDS, not through network router.
 - Preference for local node MME or AMF in mobility between 4G and 5G
For handover scenarios between MME and AMF, the preferred node that serves the handover is the local node, the CMM.
 - To enable intra-CMM mobility when UEs performing inter-RAT mobility, QA CMMs indicate in Setup and Configuration Update procedures both the native and mapped GUMMEI and GUAMI, respectively
- This functionality is part of feature described in 3GPP as pooling, which enables radio nodes to connect to several core network elements and choose these elements for the UE if the UE stays within the pool area.
- The following parameters control this capability:
- ❑ `cmm gParms sendMappedGuami`

- `cmm amfGparms sendMappedGummei`

For details, see the *CMM CLI Reference Guide*.

- For LTE, during RRC connection setup, the eNB chooses the MME based on the UE-indicated GUMMEI. When the RRC is made as part of an IRAT change from 5G to LTE, the UE indicates to the eNB GUMMEI that has been mapped from the 5G identifiers. The GUMMEI provided can be mapped from the 5G-GUTI and indicates it as a native GUMMEI and also indicates it as "Mapped from 5G-GUTI".
- For 5G, during EPS to 5GS mobility registration or initial registration procedure, if the UE holds a native 5G-GUTI for this PLMN, the UE also includes the GUAMI part of the native 5G-GUTI in the RRC to enable the NG-RAN to route the registration request to the same AMF, if available. Otherwise, in RRC signaling, the UE provides a GUAMI mapped from the EPS GUTI and indicates it as "Mapped from EPS" if the UE was previously registered to EPC.
- QA CMMs provide a list of unavailable GUAMI in the AMF STATUS INDICATION message. This list, which is communicated to gNBs, includes the single supported GUAMI with mapped GUAMI so that when native GUAMI is indicated as unavailable, the associated GUAMI must also be indicated as unavailable.

24.4 CMM support for Quad Access on VMware (Feature f70006-13)

With this feature, the CMM supports combinations of 2G, 3G, 4G, and 5G technologies, or quad access on VMware deployments.

Quad access support

This feature combines existing functionality from previous releases that support TA or MME deployment with additional integrated AMF deployment for VMware.

Support for quad access includes the following characteristics:

- CPPS AMMS and EMMS personalities are scaled independently.
- DBS simplex deployment is recommended.
- An additional network (NSX-T) must be created for AMF external traffic in addition to previous external networks for IPDS and PAPS traffic.
- A single IPDS pair is supported as in previous VMware deployments.

For more information about VMware deployments, see the *Lifecycle Management and Software Upgrade for VMware - VMware or CBAM VNFM*.

Sample configuration capacity

The following example is for configuration for 8 VMware compute hosts. Suppose the deployment has 3 NECC, 2 IPDS, 5 DBS simplex, 7 CPPS (EMMS), 2 AMMS, 4 PAPS, and 2 IPPS. The maximum message rate at IPDS suggested in lab test is 380k mps with the following distribution:

19% 2G

8% 3G

11% 3G DT

34% 4G

8% 4G IOT

11% 5G NSA

9% 5G SA

Total: 2.5M UEs

24.5 Support for CPPS VM auto-balancing AMMS and EMMS for quad access (Feature f20060-07)

This feature supports auto-balancing of the AMMS and EMMS personalities across the CPPS VMs based on load.

This feature allows the CMM in a quad access deployment to automatically change the personality of a CPPS from the 4G domain (EMMS) to the 5G domain (AMMS) or the reverse (from the AMMS to the EMMS), based on the amount of 4G and 5G traffic carried by the CMM.

When fewer AMMSs are available than the number required to carry the offered 5G load and a number of EMMSs have excess capacity, then the CMM automatically drains traffic and changes the personality of the required number of EMMSs to become AMMSs. The reverse personality change from an AMMS to an EMMS is also supported.

For a personality change to take place, following conditions must be met:

- The feature is enabled via the `supportCppsAutoPersonalityChange` global parameter.
- The VNF-based CMM is deployed as quad access.

- If all AMMSs carrying 5G traffic are roughly 70% loaded and the 4G domain has extra capacity of more than one EMMS, then the CMM automatically drains one EMMS at the end and changes its personality to AMMS.
- If all EMMSs carrying 4G traffic are roughly 70% loaded and the 5G domain has extra capacity of more than one AMMS, then the CMM automatically drains one AMMS at the end and changes its personality to EMMS.

After a CPPS's personality is changed by the CMM software, the CPPS is restarted to bring it up with appropriate resources for the new domain that the CPPS supports.

Note:

After the `supportCppsAutoPersonalityChange` global parameter is enabled and after personalities have automatically changed, the only way to revert the personalities to the static personalities that were originally deployed is to re-deploy the CMM and restore it from a backup taken prior to the feature being enabled.

The `cmm serviceStatus list` CLI command can be executed on the NECC to show the list of CPPSs in the 4G domain and in the 5G domain.

The personality change is preserved across CMM software upgrades.

This feature is applicable only to VNF-based large OpenStack. This feature does not apply to CNF-based CMMs or VNF-based small CMMs. This feature is controlled by a global parameter, `supportCppsAutoPersonalityChange`, which is disabled by default.

24.6 CMM support for providing container and multi-service VM infrastructure (Feature f72011-03)

This feature provides the pod infrastructure for splitting functionality into containers including logging, alarms, and PMs. This feature also provides the multi-service infrastructure for splitting functionality in multiple services in VMs.

The following features implement the capabilities provided by this feature:

- AMF support for event exposure pod (f72006-06)
- CMM support for call trace/alarm pod containers (f72006-04)

A pod has one service while a VM can have more than one service. The following combinations of services are available with this feature:

- For VNFs, service combinations include EEMS+ IPDS in the IPDS VM and in the NECC VM,

NECC service+CTCS +ALMS.

- For CNFs, the EEMS, ALMS, and CTCS have their own pods. The IPDS service remains its own pod, while the NECC service (that is, all other NECC processes) is in the NECC pod.

For CNF deployments, the functionality provided by this feature is specified by the `multi_container` parameter in the `values.yaml` file. By default, the feature is enabled.

This feature introduces the pod/container aspect of container dimensioning. A pod can be composed of multiple containers, and the container size must be considered in container dimensioning. For related information, see *CNF Dimensioning* in the *Capacity or Container Lifecycle Management and Software Upgrade* documents.

For related information, see the following documents:

- *Troubleshooting CMM*
- *Container Lifecycle Management and Software Upgrade*
- *CMM Counters* - counts that were reported in the IPDS under PID group m197 are now reported in the EEMS under the new PID group m198.

24.7 AMF support for event exposure pod (Feature f72006-06)

With this feature, the event exposure management service (EEMS) runs as a separate process on a VNF CMM and as a pod on a CNF CMM.

EEMS service

On VNF and CNF deployments, the EEMS performs the event exposure service by handling requests from subscribing NF consumers, triggering notifications associated with active subscriptions and keeping in local cache all active event exposure subscription data. The EEMS receives call processing triggers from the CPPS and produces the event exposure notifications as implemented by the feature *AMF support for Event Exposure for Location report and Presence including LADN* (f20053-01).

VNF

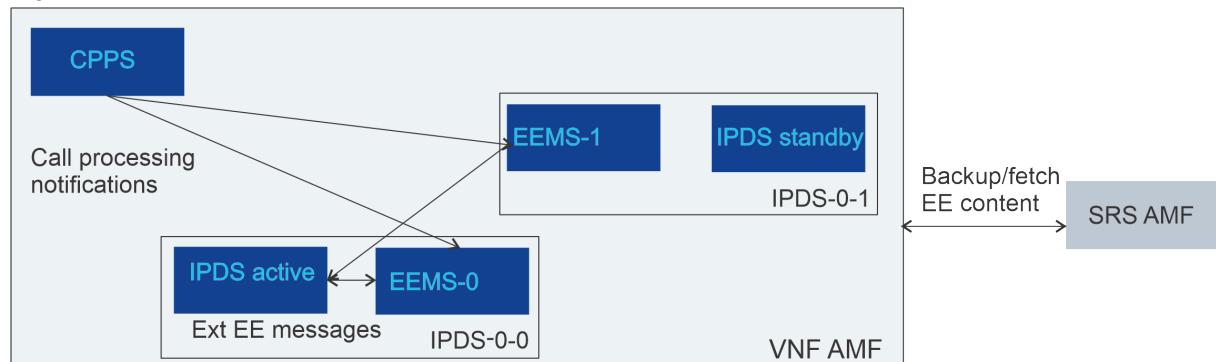
EEMS runs as a separate process within the IPDS VM. Two EEMS instances, both active, run on IPDS pair 0:

- One EEMS runs on the active IPDS instance of pair 0, IPDS-0-0.

- One EEMS runs on the standby IPDS of pair 0, IPDS-0-1.

The external SBI interface Namf EE remains on the active IPDS.

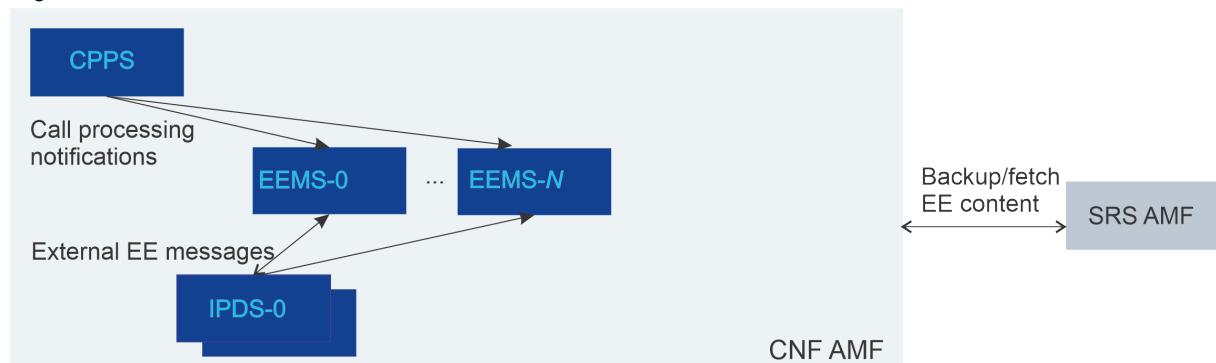
Figure 185: EEMS in VNF CMM



CNF

EEMS runs as a separate pod on a CNF. The CNF requires two EEMS pods and can scale out to 6 instances, all active. The external SBI interface Namf EE remains on the active IPDS.

Figure 186: EEMS in CNF CMM



24.8 CMM support for call trace/alarm pod (Feature f72006-04)

This feature moves the call trace collection functionality into a call trace process or pod and the alarm functionality into an alarm process or pod.

The CMM call trace functionality, call trace collection service (CTCS), runs as a separate service on the NECC of a VNF CMM and as a CTCS pod on a CNF CMM. For more information about call trace, see the *MME User Guide*.

The CMM alarm functionality, alarm management service (ALMS), run as a separate service on the NECC of a VNF CMM and an ALMS pod on a CNF CMM.

This feature requires the *CMM support for providing container and multi-service VM infrastructure (f72011-03)* feature.

For related information, see the following documents:

- *Product Description*
- *Container Lifecycle and Management and Software Upgrade*
- *Troubleshooting CMM*
- *Integrating CMM*

24.9 MME support for 24K UE radio capability information using RCIS for VNF (Feature f10937-01)

This feature enhances the MME's capability to store the UE radio capability information up to 24 kB in a new standalone optional radio capability information service (RCIS) VM.

This feature supports the following functionalities when enabled by setting the global parameter `maxMmeUeRadioCapLength` to 24576:

- An optional VM type RCIS is supported.
- The RCIS acts as a Layer 3 database or storage function.
- If a UE has a radio capability size greater than 8 kB and up to 24 kB for 4G, then the information is stored in the RCIS and the CPPS only keeps an indication along with an RCIS identifier which is available in the RCIS but not in the CPPS.

Note:

If a UE has a radio capability size up to 8 kB for 4G, then the information is stored in the CPPS.

- If a UE originally sent a radio capability of 8 kB, stored in the CPPS and later sends a radio capability which is greater than 8 kB and no greater than 24 kB. Then, the data is removed from the CPPS and the new information is stored in the RCIS.
- The RCIS stores each radio capability information separately per UE. Optimization of the RCIS storage is not in the scope of this feature.
- When the radio capability information that is stored in the RCIS is needed by call processing, then the CPPS queries the information from the RCIS.
- When a UE's data is purged from the CPPS, the radio capability information is also cleared if stored in the RCIS.

- Measurements on the radio capabilities are stored in each CPPS and RCIS.
- The number of RCIS VMs is scalable between 0 to 10 in increment of 1. The RCIS runs in a simplex configuration, therefore, Nokia recommends deploying 2 RCIS VMs to provide availability.

This feature is only applicable for OpenStack-based MME deployments on the VNF.

This feature introduces two timers:

Timer name	Value range	Default value	Description
<code>rcisPurgeTimer</code>	1 - 720 hours	120 hours	Max allowed storage time after which a UE radio capability data stored in the RCIS is purged if it has not been updated
<code>rcisRemHeartbeat</code>	200 - 20,000 millisec	200 millisec	REM heartbeat interval for RCIS service