

# Mobility Management Entity Overview

Cisco Mobility Management Entity (MME) is critical to the network function of the 4G mobile core network, known as the evolved packet core (EPC). The MME resides in the EPC control plane and manages session states, authentication, paging, mobility with 3GPP, 2G and 3G nodes, roaming, and other bearer management functions.

This overview provides general information about the MME.


- Product Description, on page 1
- Network Deployment and Interfaces, on page 3
- Features and Functionality - Base Software, on page 11
- Features and Functionality - Licensed Enhanced Feature Software, on page 40
- How the MME Works, on page 56
- Supported Standards, on page 64


# Product Description

This section describes the MME network function and its position in the LTE network.

The MME is the key control-node for the LTE access network. It works in relation with the evolved NodeB (eNodeB), Serving Gateway (S-GW) within the Evolved Packet Core (EPC), or LTE/SAE core network to perform the following functions:

- Involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW and for a UE at the initial attach and at the time of intra-LTE handover involving Core Network (CN) node relocation.
- Provides P-GW selection for subscriber to connect to PDN.
- Provides idle mode UE tracking and paging procedure, including retransmissions.
- Chooses the appropriate S-GW for a UE.
- Responsible for authenticating the user (by interacting with the HSS).
- Works as termination point for Non-Access Stratum (NAS) signaling.
- Responsible for generation and allocation of temporary identities to UEs.
- Checks the authorization of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE roaming restrictions.

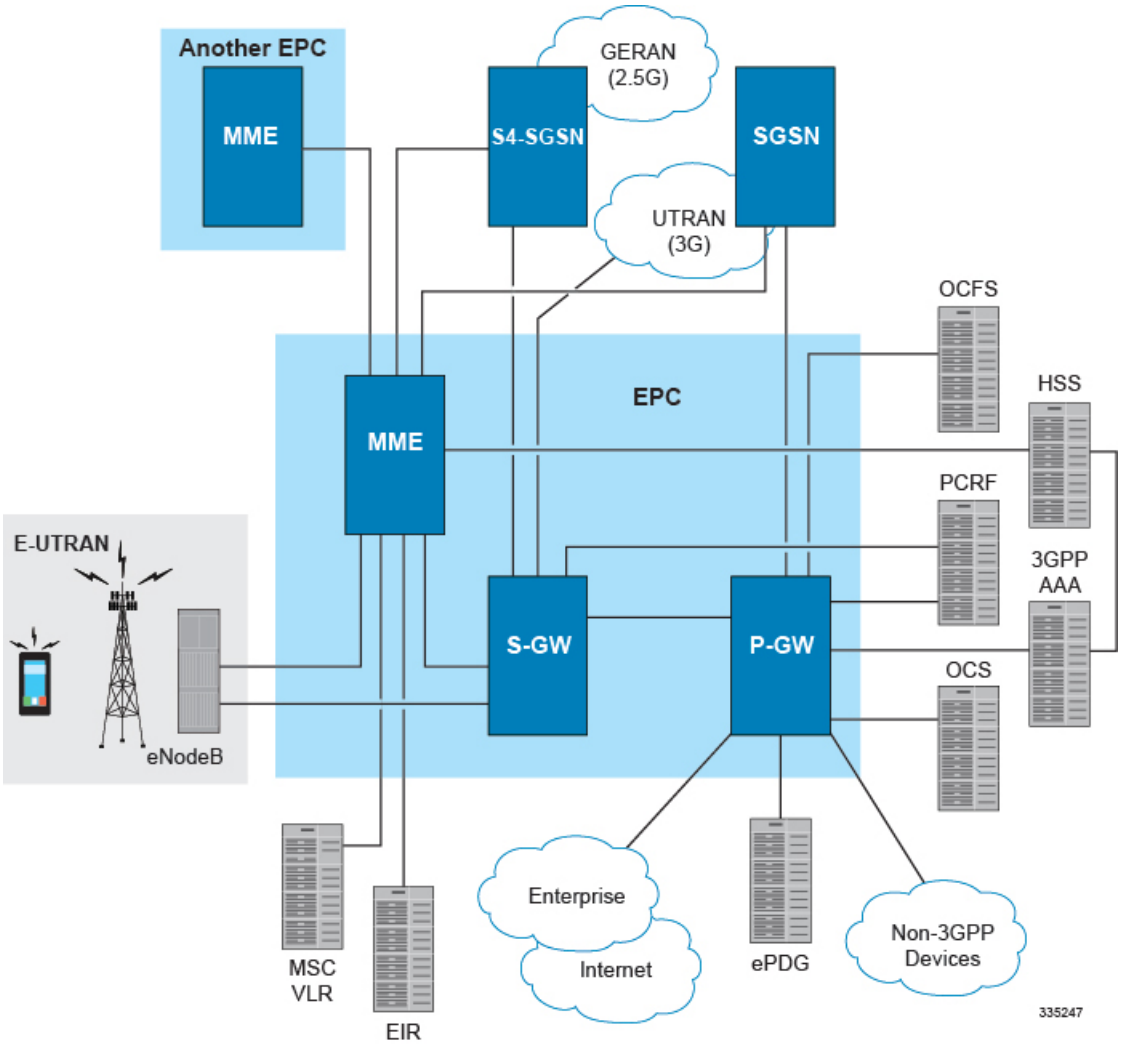
- The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management.
- Communicates with MMEs in the same PLMN or on different PLMNs. The S10 interface that is used for MME relocation and MME-to-MME information transfer or handoff.

Besides the earlier mentioned functions, the lawful interception of signaling is supported by the MME.

The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface stopping at the MME from the SGSN. In addition, the MME interfaces with SGSN for interconnecting to the legacy network.

The MME also terminates the S6a interface toward the home HSS for roaming UEs.

***Figure 1: MME in the E-UTRAN/EPC Network Topology***




In accordance with 3GPP standard, the MME provides the following functions and procedures in the LTE/SAE network:

- Non-Access Stratum (NAS) signaling

- NAS signaling security
- Inter CN node signaling for mobility between 3GPP access networks (terminating S3)
- UE Reachability in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area list management
- PDN GW and Serving GW selection
- MME selection for handover with MME change
- SGSN selection for handover to 2G or 3G 3GPP access networks
- Roaming (S6a toward home HSS)
- Authentication
- Bearer management functions including dedicated bearer establishment.
- Lawful Interception of signaling traffic
- UE Reachability procedures
- Interfaces with MSC for Voice paging
- Interfaces with SGSN for interconnecting to legacy network

## Qualified Platforms

MME is a StarOS application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

## Licenses

The MME is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

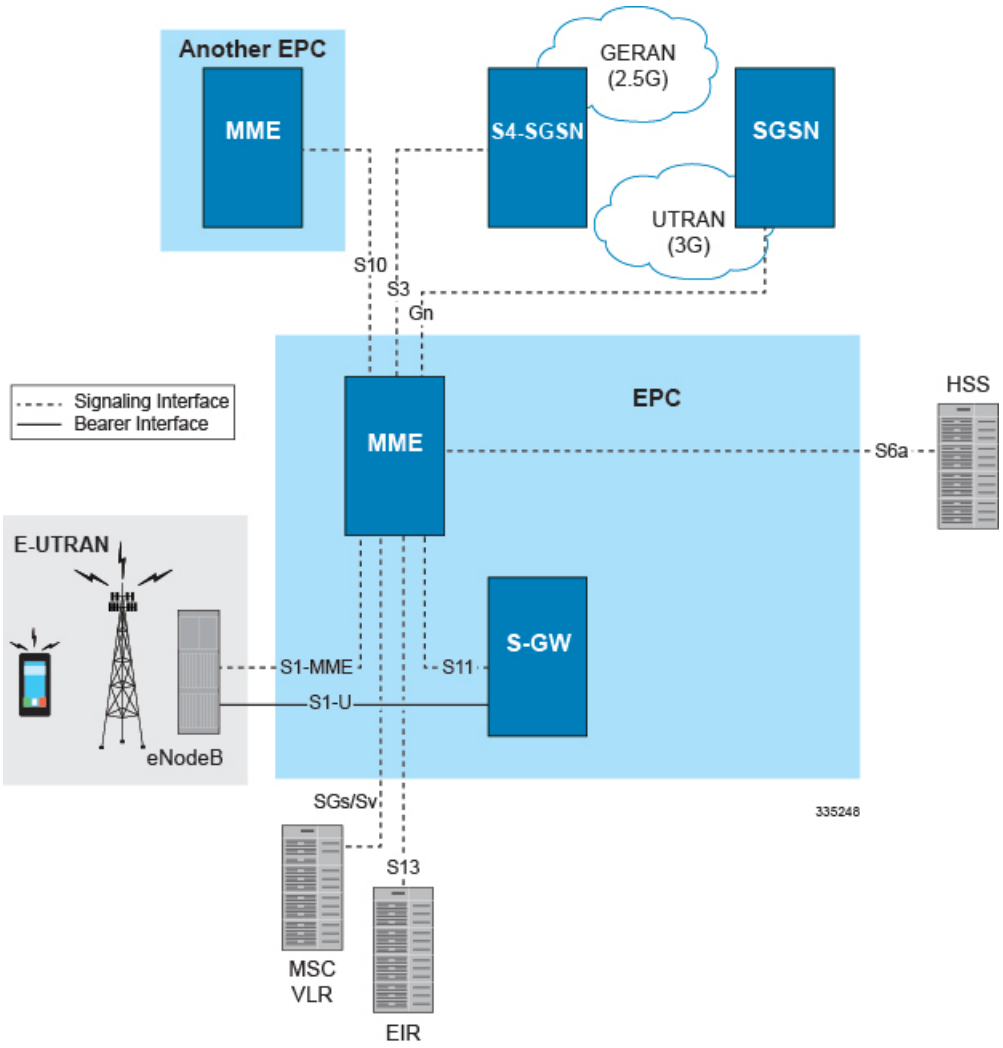
# Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of the MME in an LTE/SAE network.

## MME in the E-UTRAN/EPC Network

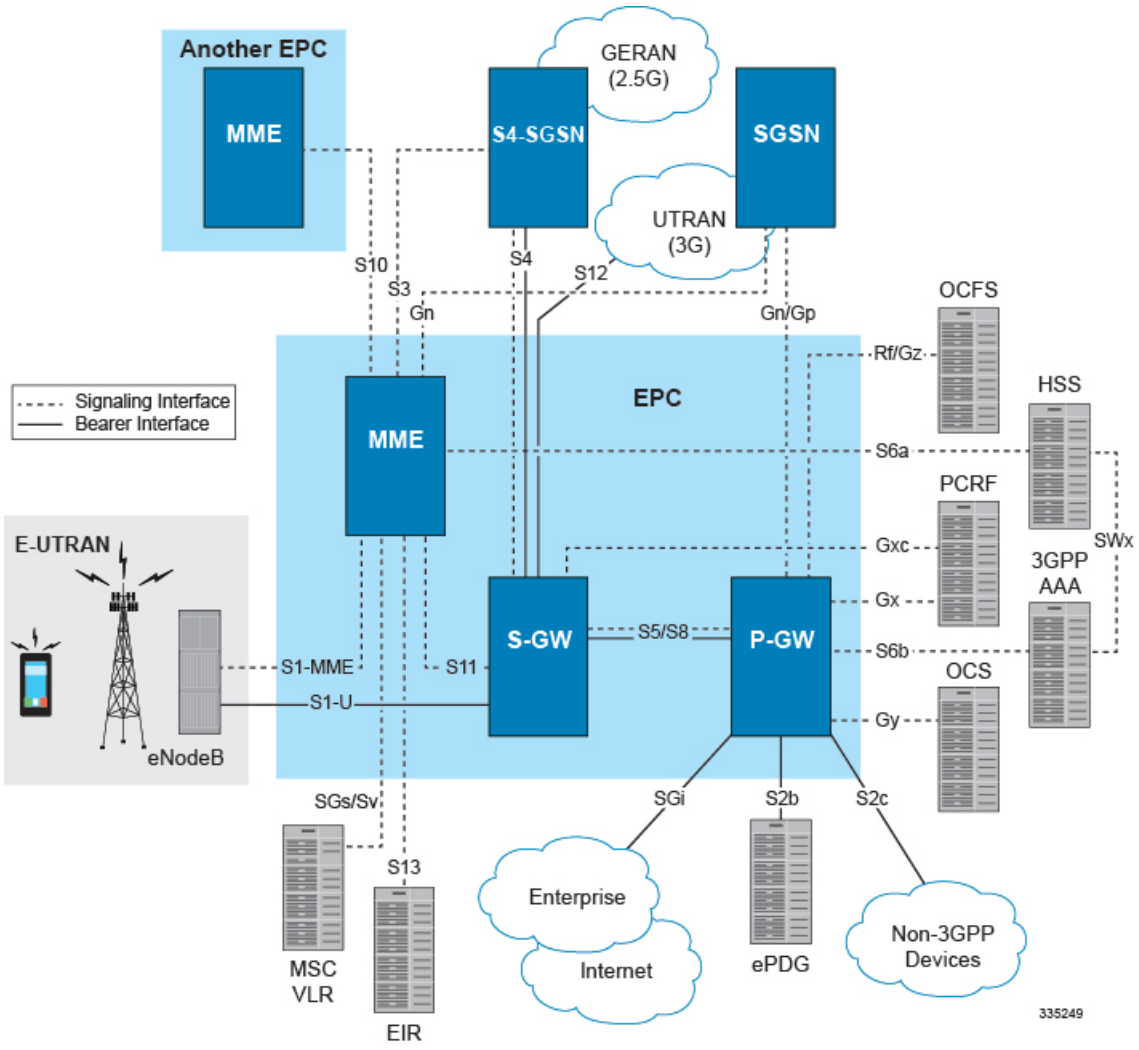
The following figure illustrates the specific network interfaces supported by the MME. Refer to the following section *Supported Logical Network Interfaces (Reference Points)* for detailed information about each interface illustrated in these figures..

*Figure 2: Supported MME Interfaces in the E-UTRAN/EPC Network*




The following figure displays a sample network deployment of an MME, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

*Figure 3: E-UTRAN/EPC Network Scenario*




## Supported Logical Network Interfaces (Reference Points)

The MME supports the following logical network interfaces/reference points:

### Gn Interface

Gn interfaces facilitate user mobility between 2G/3G 3GPP networks. The Gn interface is used for intra-PLMN handovers. The MME supports pre-Release-8 Gn interfaces to allow inter-operation between EPS networks and 2G/3G 3GPP networks.

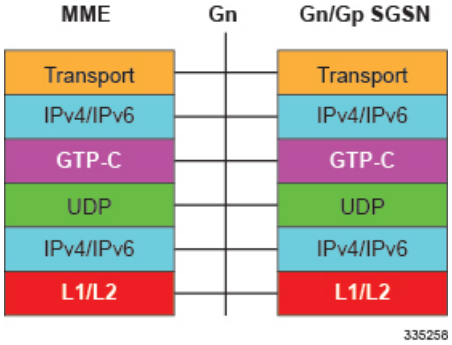
Roaming and inter access mobility between 2G and/or 3G SGSNs and an MME/S-GW are enabled by:

- Gn functionality, as specified between two SGSNs, which is provided by the MME, and
- Gp functionality, as specified between SGSN and GGSN, that is provided by the P-GW.

**Supported protocols**:

- Transport Layer: UDP, TCP

- Tunneling: IPv4 or IPv6 GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet




## S1-MME Interface

This interface is the reference point for the control plane protocol between eNodeB and MME. S1-MME uses the S1 Application Protocol (S1-AP) over the Stream Control Transmission Protocol (SCTP) as the transport layer protocol for guaranteed delivery of signaling messages between MME and eNodeB (S1).

This is the interface used by the MME to communicate with eNodeBs on the same LTE Public Land Mobile Network (PLMN). This interface serves as path for establishing and maintaining subscriber UE contexts.

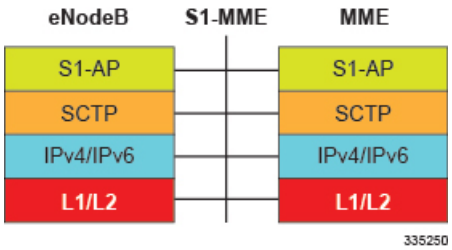
The S1-MME interface supports IPv4, IPv6, IPSec, and multi-homing.

One or more S1-MME interfaces can be configured per system context.

**Supported protocols**:

- Application Layer: S1 Application Protocol (S1-AP)
- Transport Layer: SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Note** S1-AP stack in 3GPP is R12 complaint.



## S3 Interface

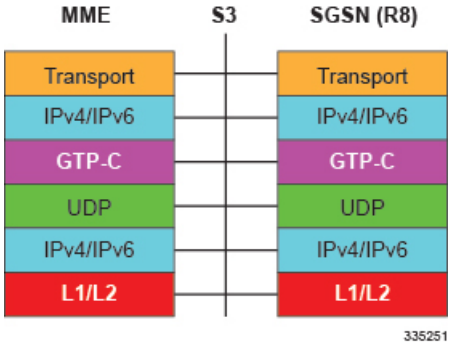
This is the interface used by the MME to communicate with S4-SGSNs on the same Public PLMN for interworking between GPRS/UMTS and LTE network access technologies. This interface serves as the signaling path for establishing and maintaining subscriber UE contexts.

The MME communicates with SGSNs on the PLMN using the GPRS Tunneling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

One or more S3 interfaces can be configured per system context.

**Supported protocols**:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTPv2-C (signaling channel)
- Signaling Layer: UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



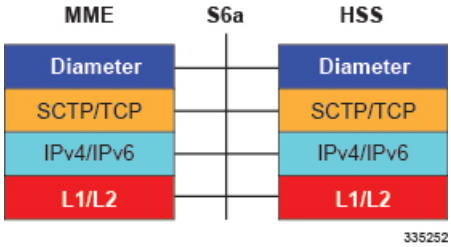

## S6a Interface

This is the interface used by the MME to communicate with the Home Subscriber Server (HSS). The HSS is responsible for transfer of subscription and authentication data for authenticating/authorizing user access and UE context authentication. The MME communicates with the HSSs on the PLMN using Diameter protocol.

One or more S6a interfaces can be configured per system context.

**Supported protocols**:

- Transport Layer: SCTP or TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



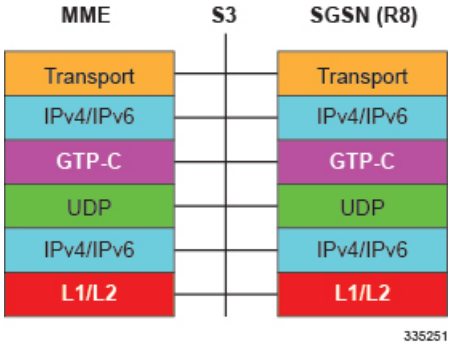
## S10 Interface

This is the interface used by the MME to communicate with an MME in the same PLMN or on different PLMNs. This interface is also used for MME relocation and MME-to-MME information transfer or handoff. This interface uses the GTPv2 protocol.

One or more S10 interfaces can be configured per system context.

**Supported protocols**:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTPv2-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



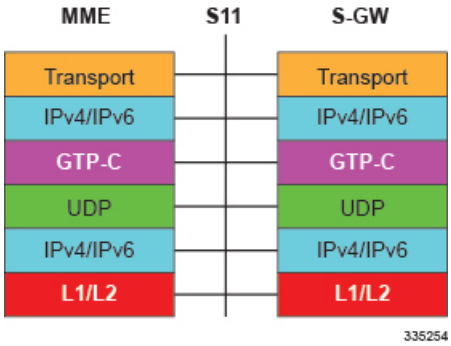

## S11 Interface

This interface provides communication between the MME and Serving Gateways (S-GW) for information transfer. This interface uses the GTPv2 protocol.

One or more S11 interfaces can be configured per system context.

**Supported protocols**:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTPv2-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



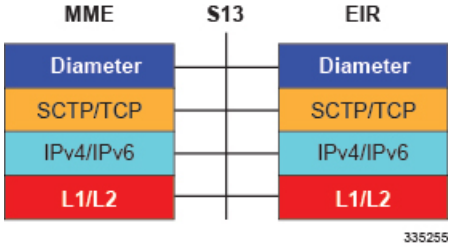
## S13 Interface

This interface provides communication between MME and Equipment Identity Register (EIR).

One or more S13 interfaces can be configured per system context.

**Supported protocols**:

- Transport Layer: SCTP or TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

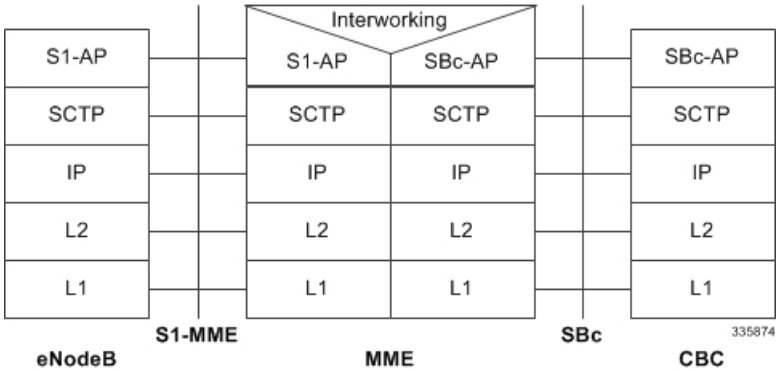



## SBc Interface

The SBc interface connects the MME to the Cell Broadcast Center (CBC) to support the Commercial Mobile Alert System (CMAS) to deliver public warning messages.

**Supported protocols**:

- Application: SBc-AP
- Transport Layer: SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



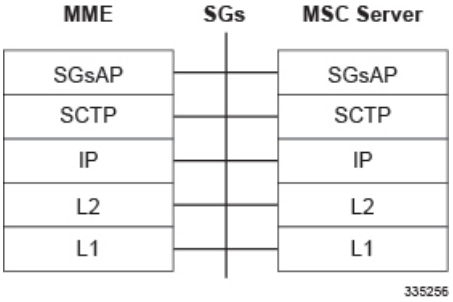

## SGs Interface

The SGs interface connects the MSC Server and the MME to support circuit switched fallback and SMS in an EPS scenario.

**Supported protocols**:

- Application: SGs-AP

- Transport Layer: SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

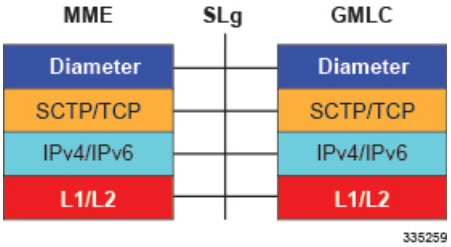



## SLg Interface

This interface is used by the MME to communicate with the Gateway Mobile Location Center (GMLC). This diameter-based interface is used for LoCation Services (LCS), which enables the system to determine and report location (geographical position) information for connected UEs in support of a variety of location services.

**Supported protocols**:

- Transport Layer: SCTP or TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

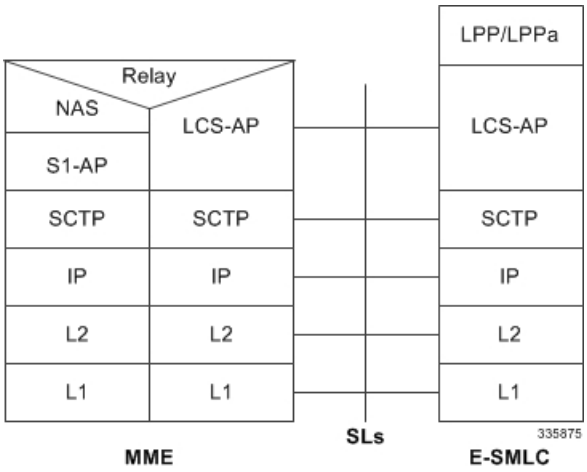



**Important** MME Software also supports additional interfaces. For more information on additional interfaces, refer to the *Features and Functionality - Licensed Enhanced Feature Software* section.

## SLs Interface

The SLs interface is used to convey LCS Application Protocol (LCS-AP) messages and parameters between the MME to the Evolved Serving Mobile Location Center (E-SMLC).

- Application: LCS-AP
- Transport Layer: SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

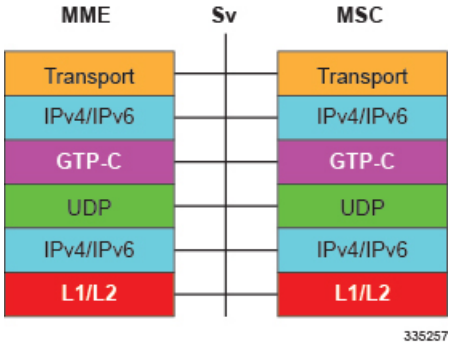



### Sv Interface

This interface connects the MME to a Mobile Switching Center to support the exchange of messages during a handover procedure for the Single Radio Voice Call Continuity (SRVCC) feature.

**Supported protocols**:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet




# Features and Functionality - Base Software

This section describes the features and functions supported by default in the base software on the MME service and do not require any additional licenses.

To configure the basic service and functionality on the system for MME service, refer to configuration examples and/or feature chapters provide in the *MME Administration Guide*.

# 3GPP R8 Identity Support

Provides the identity allocation of following type:

- EPS Bearer Identity
- Globally Unique Temporary UE Identity (GUTI)
- Tracking Area Identity (TAI)
- MME S1-AP UE Identity (MME S1-AP UE ID)

- **EPS Bearer Identity**: An EPS bearer identity uniquely identifies EPS bearers within a user session for attachment to the E-UTRAN access and EPC core networks. The EPS Bearer Identity is allocated by the MME. There is a one to one mapping between EPS Radio Bearers via the E-UTRAN radio access network and EPS Bearers via the S1-MME interface between the eNodeB and MME. There is also a one-to-one mapping between EPS Radio Bearer Identity via the S1 and X2 interfaces and the EPS Bearer Identity assigned by the MME.
- **Globally Unique Temporary UE Identity (GUTI)**: The MME allocates a Globally Unique Temporary Identity (GUTI) to the UE. A GUTI has 1) unique identity for MME which allocated the GUTI and 2) the unique identity of the UE within the MME that allocated the GUTI.

Within the MME, the mobile is identified by the M-TMSI.

The Globally Unique MME Identifier (GUMMEI) is constructed from MCC, MNC and MME Identifier (MMEI). In turn the MMEI is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

The GUTI is constructed from the GUMMEI and the M-TMSI.

For paging, the mobile is paged with the S-TMSI. The S-TMSI is constructed from the MMEC and the M-TMSI.

The operator needs to ensure that the MMEC is unique within the MME pool area and, if overlapping pool areas are in use, unique within the area of overlapping MME pools.

The GUTI is used to support subscriber identity confidentiality, and, in the shortened S-TMSI form, to enable more efficient radio signaling procedures (e.g. paging and Service Request).

- **Tracking Area Identity (TAI)**: Provides the function to assign the TAI list to the mobile access device to limit the frequency of Tracking Area Updates in the network. The TAI is the identity used to identify the tracking area or group of cells in which the idle mode access terminal will be paged when a remote host attempts to reach that user. The TAI consists of the Mobile Country Code (MCC), Mobile Network Code (MNC) and Tracking Area Code (TAC).
- **MME S1-AP UE Identity (MME S1-AP UE ID)**: This is the temporary identity used to identify a UE on the S1-MME reference point within the MME. It is unique within the MME per S1-MME reference point instance.

# ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the system and an element management system since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

# APN Restriction Support

The APN-Restriction value may be configured for each APN in the P-GW and transferred to the MME. It is used to determine, on a per-MS basis, whether it is allowed to establish EPS bearers to other APNs.

The APN-Restriction value is defined in clause 15.4 of 3GPP TS 23.060. APN-Restriction affects multiple procedures, such as Initial Attach, TAU, PDN connectivity, and inter-MME handovers. The MME saves the APN-Restriction value received in create session response for an APN and uses the maximum of the values from the currently active PDNs in the next create session request. If a PDN is disconnected, then the maximum APN-Restriction is adjusted accordingly.

# Authentication and Key Agreement (AKA)

The MME provides EPS Authentication and Key Agreement mechanism for user authentication procedure over the E-UTRAN. The Authentication and Key Agreement (AKA) mechanism performs authentication and session key distribution in networks. AKA is a challenge- response based mechanism that uses symmetric cryptography. AKA is typically run in a Services Identity Module.

AKA is the procedure that take between the user and network to authenticate themselves towards each other and to provide other security features such as integrity and confidentiality protection.

In a logical order this follows the following procedure:

1. Authentication: Performs authentication by identifying the user to the network and identifying the network to the user.
2. Key agreement: Performs key agreement by generating the cipher key and generating the integrity key.
3. Protection: When the AKA procedure is performed, it protects the integrity of messages, the confidentiality of the signaling data, and the confidentiality of the user data.

# Backup and Recovery of Key KPI Statistics

This feature allows the back up of a small set of MME key KPI counters for recovery of the counter values after a session manager (SessMgr) crash.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the MME loses the counter values as they are reset to zero. So, the KPI calculation in the

next interval will result in negative values for that interval. With this feature, it is possible to perform reliable KPI calculations even if a SessMgr crash occurs.

For details about the feature, commands, and new MME-BK schema, refer to the *Backup and Recovery of Key KPI Statistics* feature in this guide.

# Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with an element manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a partial list of supported schemas:

- **Card**: Provides card-level statistics.
- **MME-eMBMS**: Provides eMBMS service statistics.
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics.
- **HSS**: Provides HSS service statistics.
- **LCS**: Provides Location Services statistics.
- **MME**: Provides MME service statistics.
- **MME-BK**: Provides selected set of backed-up and (post-SessMgr crash) recovered MME statistics.
- **Port**: Provides port-level statistics.
- **S102**: Provides statistics for S102 interface.
- **SBc**: Provides SBc service statistics for associations to Cell Broadcast Centers.
- **SGs**: Provides statistics for SGs connections.
- **SGS-VLR**: Provides statistics for SGs connections on a per-VLR basis.
- **SLs**: Provides SLs service statistics for Location Services.
- **System**: Provides system-level statistics.
- **TAI**: Provides MME statistics at the TAI (MCC/MNC/TAC) level.

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the chassis or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, chassis host name, chassis uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When an element manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of an element manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on an element manager server.

# Cell Broadcast Center - SBc Interface

The MME provides support for Commercial Mobile Alert System (CMAS): SBc interface and underlying protocols. Warning Messages can be received from a Cell Broadcast Center (CBC) over the SBc-AP interface and relayed to all relevant eNodeBs over the S1-AP interface.

Refer to the *Cell Broadcast Center - SBc Interface* chapter in the *MME Administration Guide* for more information.

# Closed Subscriber Groups

Closed Subscriber Group identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG for a Home eNodeB.

Refer to the *Closed Subscriber Groups* chapter in the *MME Administration Guide* for more information.

# Co-Located SPGW Selection for Emergency Bearer

MME uses the canonical name of the selected S-GW (from DNS response) for the previously established Pens and compares it with the statically configured P-GW collocation string in the LTE emergency profile to select the P-GW. The static P-GW collocation string must be configured with the canonical node name of the P-GW to ensure to select collocated node for emergency call.



**Important** This behavior applies only to the PDN connectivity request for Emergency Bearer Service.

### pgw co-location

Use the following configuration to configure P-GW co-location:

```
configure
  lte-policy
    lte-emergency-profile profile_name
      [ no ] pgw co-location
      end
```

**NOTES:**

- **no** Disables the P-GW co-location configuration.
- **co-location** Configures to select the co-located S-GW/P-GW node based on static P-GW configuration and S-GW selected through DNS.

**show lte-policy lte-emergency-profile <profile_name>**

The output of this command includes "pgw co-location" to indicate if the P-GW co-location feature is enabled or disabled.

# Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  The following system resources can be monitored:

  - System CPU usage
  - System service CPU usage (Demux-Card CPU usage)
  - System Memory usage
  - License usage
  - Maximum Session per service

- **Service Congestion Policies**: Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Congestion control can be used in conjunction with the load balancing feature provided on the MME. For more information on MME load balancing, refer to the *Load Balancing and Rebalancing* section in this guide.

For more information or to configure Overload Control using the basic Congestion Control functionality, refer to the *Congestion Control* chapter in the *ASR 5500 System Administration Guide*.

For more information about the **Enhanced** Congestion Control functionality (a licensed feature), refer to the *Enhanced Congestion Control and Overload Control* chapter in this guide.

# Controlling Voice Over PS Session in S1 Mode

Configured APN is considered as IMS APN and UE is allowed to attempt IMS PDN connection only if it is subscribed to that APN. If the configured IMS APN is present in the subscription in ULA, then MME sets "IMS voice over PS session in S1 mode" in the Attach Accept/TAU Accept message.

If the configured IMS APN is not present in the subscription in ULA, then "IMS voice over PS session in S1 mode" must be unset. If there is any change in subscription due to ISDR/DSR, then the updated parameter must be sent to the UE during the next IM-Exit.

The **ims-apn** CLI command in the Call Control Profile Configuration mode is enhanced to configure the network identifier on MME.

# Define Same TAI in Multiple TAI Lists

The MME could have a tracking area in only one tracking area list (TAI List). Consequently, the tracking area list assigned to subscribers attaching from different TAIs will be same, even if the adjacency of these tracking areas is not same. This results in MME getting TAUs even as subscribers moved to the adjacent area.

The MME will allow operators to configure adjacency lists as TAI Lists, thus reducing the Tracking Area Updates (TAU) received by MME. This feature enables the MME to send configured customized TAI List in ATTACH_ACCEPT/TAU_ACCEPT when a request is received from the custom or border TAIs.

The reduced TAU results in less signaling load on the MME and better operational efficiency.

# Delay Value IE Support in MME

MME sends configured delay value as “Data Notification Delay" in DDN-ACK and "Delay Downlink Packet Notification Request" IE in Modify-Bearer-Request to SGW. When the delay value is not configured, this IE will not be included in DDN-ACK and Modify bearer request messages.

### ddn-delay

Use the following configuration to configure ddn-delay value.

```
configure
  context context_name
    mme-service mme-service_name
      ddn-delay ddn-delay_value
      no ddn-delay
      end
```

**NOTES:**

- **no**: Removes the configured downlink-data-notification delay value.
- **ddn-delay** Configures the downlink-data-notification delay value in multiples of 50 milliseconds. *ddn-delay_value* is an integer and it must be between 0 and 255.

### show mme-service all

The output of this command includes "DDN Delay Value".

# eCGI in PLA/RR Messages

To retrieve the geographical position of a UE, the MME includes the location estimate and the eCGI value in the PLA/LRR messages that is sent to the GMLC. The eCGI value is independent of the response received from the E-SMLC.

In releases prior to 21.5: During a location service request (to the MME), when the E-SMLC is configured, the MME sends the location service request to the E-SMLC. The E-SMLC processes the location service request and sends only the location estimate information back to the MME, which forwards the data in the PLA/LRR messages to the GMLC. The location estimate in the PLA/LRR messages sent to the GMLC is based on the response received from the E-SMLC.

# Emergency Call Release

Notifying the GMLC of the emergency call release event allows the GMLC to delete all information previously stored for the emergency call in accordance with regulations.

In compliance with 3GPP TS 29.172, the MME location services (LCS) feature supports sending the EMERGENCY_CALL_RELEASE event in a subscriber location report (SLR) request message to the gateway mobile location center (GMLC) when an emergency call is released or when an emergency PDN is disconnected at the MME.

With this new functionality, the MME notifies the GMLC of Emergency Call Release. The call release event enables the GMLC to clear the cache for existing calls and to correctly log the duration of an emergency call. Without call release facilitating the clearing of the cache, the location platform could send the old (erroneous) location information in response to a new location request for an E-911 call.

# Emergency Session Support

The MME supports the creation of emergency bearer services which, in turn, support IMS emergency sessions. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions).

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only
- IMSI required, authentication optional
- All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.
- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

# EPS Bearer Context Support

Provides support for subscriber default and dedicated Evolved Packet System (EPS) bearer contexts in accordance with the following standards:

- 3GPP TS 36.412 V8.6.0 (2009-12): 3rd Generation Partnership Project Technical Specification Group Radio Access Network Evolved Universal Terrestrial Access Network (E-UTRAN) S1 signaling transport (Release 8)
- 3GPP TS 36.413 V8.8.0 (2009-12): 3rd Generation Partnership Project Technical Specification Group Radio Access Network Evolved Universal Terrestrial Radio Access Network (E-UTRAN) S1 Application Protocol (S1AP) (Release 8)
- IETF RFC 4960, Stream Control Transmission Protocol, December 2007

EPS bearer context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 1024 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how UE contexts are processed such as the following:

- PDN Type: IPv4, IPv6, or IPv4v6
- EPS Bearer Context timers
- Quality of Service

A total of 11 EPS bearer per subscriber are supported. These could be all dedicated, or 1 default and 10 dedicated or any combination of default and dedicated context. Note that there must be at least one default EPS Bearer context in order for dedicated context to come up.

# EPS GTPv2 Support on S11 Interface

Support for the EPS GTPv2 on S11 interface in accordance with the following standards:

- 3GPP TS 29.274 V8.4.0 (2009-12): 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) Stage 3 (Release 8)

The system supports the use of GTPv2 for EPS signaling context processing.

When the GTPv2 protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPv2 functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the MME, and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

Whether or not the MME accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the MME always accepts the charging characteristics from the SGSN. They must always be provided by the SGSN for GTPv1 requests for primary EPS Bearer contexts. If they are not provided for secondary EPS Bearer contexts, the MME re-uses those from the primary.

If the system is configured to reject the charging characteristics from the SGSN, the MME can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level.

MME charging characteristics consist of a profile index and behavior settings. The profile indexes specify the criteria for closing accounting records based specific criteria.



**Important** For more information on GTPv2 configuration, refer to the *Creating and Configuring the eGTP Service and Interface Association* section in the *Mobility Management Entity Configuration* chapter of the *MME Service Administration Guide*.

# ERAB Setup Retry Handling

MME will start Timer (Tm) after the reception of "E-RAB Setup Response" with cause "Interaction with other procedure." Once the timer expires, MME re-transmits the "E-RAB Setup Request." MME supports the maximum retry count. This behavior is CLI controlled.

### erab-setup-rsp-fail retry-timer

Use the following configuration to configure the ERAB Setup retry handling:

```
configure
   context context_name
     mme-service service_name
        policy erab-setup-rsp-fail retry-timer retry_timer  max-retries
max_retries
        { default | no } policy erab-setup-rsp-fail retry-timer
        end
```

**NOTES:**

- **no** Disables the retry timer mechanism.
- **default** Restores the default value to existing behavior by disabling the retry timer mechanism.
- **policy** Specifies the user-defined policies like idle mode detach behavior and so on.
- **erab-setup-rsp-fail** Sets the handling for ERAB-SETUP-RESPONSE failure message.
- **retry-timer** *retry_timer* Configures the retry timer for ERAB Setup Procedure. *retry_timer* must be an integer value in the range of 1-15.
- **max-retries** *max_retries* Configures the maximum retry limit for ERAB Setup Procedure. *max_retries* must be an integer value in the range of 1-10.

# Handling the TAU and Location Update Request/Response

UE triggers TAU, results in MME sending Location Update Request/Response. MME sends TAU Accept to UE (with S1 downlink-nas to eNB). With UE sending TAU Complete, MME sends TMSI Relocation Complete to MSC and Modify Bearer Request towards S-GW.

# HSS Support Over S6a Interface

Provides a mechanism for performing Diameter-based authorization, authentication, and accounting (AAA) for subscriber bearer contexts based on the following standards:

- 3GPP TS 23.401 V8.1.0 (2008-03): 3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 8)
- 3GPP TS 29.272 V8.1.1 (2009-01): 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Evolved Packet System (EPS) Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 8)
- 3GPP TS 33.401 V8.2.1 (2008-12): 3rd Generation Partnership Project Technical Specification Group Services and System Aspects 3GPP System Architecture Evolution (SAE): Security Architecture (Release 8)
- RFC 3588, Diameter Base Protocol, December 2003

The S6a protocol is used to provide AAA functionality for subscriber EPS Bearer contexts through Home Subscriber Server (HSS).

During the initial attachment procedures the MME sends to the USIM on AT via the HSS the random challenge (RAND) and an authentication token AUTN for network authentication from the selected authentication vector. At receipt of this message, the USIM verifies that the authentication token can be accepted and if so, produces a response. The AT and HSS in turn compute the Cipher Key (CK) and Integrity Key (IK) that are bound to Serving Network ID. During the attachment procedure the MME requests a permanent user identity via the S1-MME NAS signaling interface to eNodeB and inserts the IMSI, Serving Network ID (MCC, MNC) and Serving Network ID it receives in an Authentication Data Request to the HSS. The HSS returns the Authentication Response with authentication vectors to MME. The MME uses the authentication vectors to compute the cipher keys for securing the NAS signaling traffic.

At EAP success, the MME also retrieves the subscription profile from the HSS which includes QoS information and other attributes such as default APN name and S-GW/P-GW fully qualified domain names.

Among the AAA parameters that can be configured are:

- Authentication of the subscriber with HSS
- Subscriber location update/location cancel
- Update subscriber profile from the HSS
- Priority to dictate the order in which the servers are used allowing for multiple servers to be configured in a single context
- Routing Algorithm to dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured HSS servers for new sessions. Once a session is established and an HSS server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

# IE-Extension Support for Bearers SubjectToStatusTransfer_Item

Support for Extension IEs in Bearers_SubjectToStatusTransfer_Item is added to enable MME to include the extension IEs in MME status transfer message to target eNB.

Bearers_SubjectToStatusTransfer_Item Extension IEs are sent from source eNB in eNB-Status-Transfer message.

# IMSI Manager Scaling

The support for the expanded capacities of the VPC-DI and ASR5500 platforms, the IMSIMgr Scaling feature increases the number of IMSI managers on the MME to a maximum of 4. This number is configurable.

The IMSIMgr is the demultiplexing process that selects the SessMgr instance to host a new session based on a demux algorithm logic to host a new session by handling new call requests from the MMEMgr, the EGTPC Mgr, and the (e)SGTPCMgr (New MME handoffs). The new call requests or signaling procedures include Attach, Inter-MME TAU, PS Handover, and SGs, all of which go through the IMSIMgr. The IMSIMgr process also maintains the mapping of the UE identifier (for example, IMSI/GUTI) to the SessMgr instance.



**Important** IMSIMgr scaling is only available on the ASR5500 and VPC-DI platforms.

By increasing the number of IMSIMgr instances, the new call handling capacity (primarily for Attach and SGs procedures) of the MME is increased as the calls are distributed across multiple instances. The call distribution logic across IMSIMgrs utilizes a simple hash operation on IMSI/GUTI to select the IMSIMgr instance.

It is the MMEMgr/EGTPC Mgr/SGTPC Mgr that selects an IMSIMgr instance to be contacted for session setup. Each subscriber session in a SessMgr will maintain the IMSIMgr instance number that hosts the mapping for the IMSI. The SessMgrs now remembers the IMSIMgr instance IDs per subscriber for the target IMSIMgr instance number (IMSIMgr instance ID calculated by hash on the IMSI).

All IMSIMgr instances will send the current count of sessions per MME service to the MMEMgr via existing response messaging. The MMEMgr will send the same data received from multiple IMSIMgr instances back to the IMSIMgr in existing request messaging. As a result, each IMSIMgr will know the session count per MME service for all IMSIMgr instances. Given this information, the per MME service session limits can now be enforced by each IMSIMgr instance.

This feature does not require a special license.

The following changes are observed when the number of IMSI managers set is more than 1:

- It is possible to initiate an audit request for a single, specific IMSIMgr instance.
- Increased tolerance for configurable MME per service session limits. This can be noticed when configuring commands such as **bind** in the MME Service configuration mode.
- Increased tolerance for Attach rate control as the MME Attach rate control will be independently enforced by each IMSIMgr instance.



**Important** The **task facility imsimgr max** command sets the number of IMSI managers. This is a **boot-time** configuration and must be added in the configuration file to be implemented at startup and before any MME related configuration takes effect, that is before any IMSIMgr is started. The run-time configuration of this CLI *does not* have any effect.



**Important** After you configure the **task facility imsimgr max** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

# Inter-MME Handover Support

The S10 interface facilitates user mobility between two MMEs providing for the transfer of the UE context from one to the other. It is a GTPv2 control plane interface that supports the following handover types and features:

- E-UTRAN-to-UTRAN (MME-to-MME) handover through:
  - Tracking Area Update based inter-MME relocation
  - Attach at an eNodeB connected to a different MME
  - S1 handover based inter-MME relocation
- The MME supports handing over multiple bearers and multiple PDNs over to another MME
- Trace functionality, monitor protocol, and monitor subscriber
- DNS client configuration
- IPv4 and IPv6: for peer MME selection, the preference is given to IPv6 addresses. IPv4 addresses are ignored if IPv6 addresses are present.

# Interworking Support

This section describes various interworking and handover scenarios supported by the MME, including:

- Interworking with SGSNs
- Handover Support for S4 SGSNs
- Unoptimized Non-3GPP Handover Support

## Interworking with SGSNs

This feature enables an integrated EPC core network to anchor calls from multi-mode access terminals and supports seamless mobility on call hand-offs between an LTE or GERAN/UTRAN access network. This provides a valuable function to enable LTE operators to generate incremental revenue from inbound roaming agreements with 2G/3G roaming partners.

In order to support inter-RAT hand-offs for dual-mode access terminals between LTE and 2G/3G networks with 3GPP Pre-Release 8 SGSN's, the MME will support combined hard handover and SRNS relocation procedures via the GTPv1 Gn/Gp reference interface. In preparation for the handover, the MME sends a Forward Relocation Request to the SGSN and includes subscriber identity and context information including IMSI, Mobility Management context and PDP context. The PDP context includes the GGSN address for the user plane and the uplink Tunnel Endpoint ID. These addresses are equivalent to the PDN GW address. The MME maps the EPS bearer parameters to the PDP contexts.

After sending the forward relocation signaling to the target SGSN, the MME deletes the EPS bearer resources by sending a Delete Bearer Request to the S-GW with a Cause code that instructs the S-GW not to initiate delete procedures toward the P-GW.

When a mobile subscriber roams from an EUTRAN to GERAN/UTRAN access network it must also send a Routing Area Update (RAU) to register its location with the target network. The target SGSN sends a Context Request to the MME with P-TMSI to get the Mobility Management contexts and PDP contexts for the subscriber session. The SGSN uses the Globally Unique Temporary ID (GUTI) from the MME to identify the P-TMSI/RAI.

## Handover Support for S4-SGSNs

The S3 interface facilitates user mobility between an MME and an S4-SGSN providing for the transfer of the UE context between the two. It is a GTPv2 control plane interface that supports the following handover types:

- E-UTRAN-to-UTRAN and E-UTRAN-to-GERAN (MME-to-R8 SGSN) handover through:
  - Routing Area Update (RAU) based MME-R8 SGSN relocation where the RAU could be a result of UE movement.
  - Attach at an RNC connected to a R8 SGSN
  - S1 handover/SRNS relocation based MME-R8 SGSN relocation
- UTRAN-to-E-UTRAN and GERAN-to-E-UTRAN (R8 SGSN-to-MME) handover through:
  - Tracking Area Update (TAU) based R8 SGSN-MME relocation where the TAU could be a result of UE movement.
  - Attach at an eNodeB connected to an MME.
  - SRNS relocation/S1 handover based R8 SGSN-MME relocation.

All handover types support handing over multiple bearers and multiple PDNs from the MME to a R8 SGSN and vice versa.

The S3 interface also supports the following features:

- Monitor Protocol and Monitor Subscriber
- Subscriber Session Trace
- IPv4 and IPv6: for peer SGSN selection, the preference is given to IPv6 addresses. IPv4 addresses are ignored if IPv6 addresses are present.
- Operator Policy for SGSN selection
- Session Recovery: all MME sessions established using the S3 interface are capable of being recovered in case of a session manager task failure.

## Unoptimized Non-3GPP Handover Support

The MME provides support for Non-3GPP to EUTRAN and EUTRAN to Non-3GPP un-optimized handovers. These include the LTE-eHRPD handover scenarios in sections 8.2.1.1 and 8.2.1.2, and 8.2.2 and 8.2.3 of 3GPP TS 23.402-910.

No configuration is required to enable this functionality on the MME.

Note:

- PDN Connectivity request should contain Request Type as HANDOVER.
- P-GW is selected only through HSS-provided P-GW address or FQDN (MIP6-Info), with P-GW allocation type as static always.
- In the case of multiple PDN connectivity during handover from non-3gpp access to EUTRAN, the ESM PDN connectivity message from UE is transported via S1AP Uplink NAS transport. All other such PDN connectivity requests shall be rejected.

- Handovers to other access (such as UTRAN, GERAN) are only supported after the S11 modify bearer procedures with S-GW have been completed for all PDNs.

**Performance Indicators:**

The following MME schema bulk statistics track the number of outbound and inbound non-3GPP handovers that were attempted, were successful, and which failed. Note: During an inbound relocation, both the handover statistics and relevant attach/PDN connectivity statistics will be incremented.

- out-non-3GPP-ho-attempted
- out-non-3GPP-ho-success
- out-non-3GPP-ho-failures
- in-non-3GPP-ho-attempted
- in-non-3GPP-ho-success
- in-non-3GPP-ho-failures

The **show mme-service statistics** command also displays the number of outbound and inbound non-3GPP handovers that were attempted, were successful, and which failed. Note that these counters increment on a per-PDN basis.

The system disconnect reason **disc-reason-484 - mme-reloc-to-non-3GPP** tracks the total number of session disconnects resulting from outbound non-3GPP handovers.

# IPv6 PDN Type Restriction

MME will not allow the UE to get connected to PDN Type IPv6. This means that MME will not allow the UE to include IPv6 address even if the UE has requested and subscribed for the IPv6 address.

MME will ensure that PDN will not receive any IPv6 address either by rejecting with PDN Connectivity Request or by overriding it only with IPv4 address.

The following table explains the behavior of MME when the **pdn-type-override ipv4-only** CLI command is enabled.

| UE Requested PDN Type | HSS Subscription | Behavior |
|---|---|---|
| IPv4 | IPv4v6 | PDN is assigned with IPv4 address only. |
| IPv4 | IPv4 | PDN is assigned with IPv4 address only. |
| IPv4 | IPv6 | PDN Reject with cause 32 "Service option not supported". |
| IPv6 | IPv4v6 | PDN is assigned with IPv4 address only. |
| IPv6 | IPv4 | PDN Reject with cause "Only IPv4 is supported". |
| IPv6 | IPv6 | PDN Reject with cause 32 "Service option not supported". |

| UE Requested PDN Type | HSS Subscription | Behavior |
|---|---|---|
| IPv4v6 | IPv4v6 | PDN is assigned with IPv4 address only. |
| IPv4v6 | IPv4 | PDN is assigned with IPv4 address only. |
| IPv4v6 | IPv6 | PDN Reject with cause 32 "Service option not supported". |

- In the Call Control Profile Configuration mode, the **pdn-type-override** CLI command is enhanced to enable the MME to allow only IPv4 addresses to a PDN connection. The default behavior allows PDN to have IPv6 addresses when subscription allows it.

```
configure
  call-control-profile profile_name
    [ remove ] pdn-type-override ipv4-only
    end
```

- The **PDN Type IPv6 Denied** field in the output of the **show call-control-profile full all** command displays "Configured" or "Not Configured" to indicate whether the MME is enabled to allow only IPv4 addresses to a PDN connection.

# IPv6 Support

This feature allows IPv6 subscribers to connect via the LTE/SAE infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

The MME allows an APN to be configured for IPv6 EPS Bearer contexts. Also, an APN may be configured to simultaneously allow IPv4 EPS Bearer contexts.

The MME supports IPv6 stateless dynamic auto-configuration. The mobile station may select any value for the interface identifier portion of the address. The link-local address is assigned by the MME to avoid any conflict between the mobile station link-local address and the MME address. The mobile station uses the interface identifier assigned by the MME during the stateless address auto-configuration procedure. Once this has completed, the mobile can select any interface identifier for further communication as long as it does not

conflict with the MME's interface identifier that the mobile learned through router advertisement messages from the MME.

Control and configuration of the above is specified as part of the APN configuration on the MME, e.g., IPv6 address prefix and parameters for the IPv6 router advertisements. RADIUS VSAs may be used to override the APN configuration.

Following IPv6 EPS Bearer context establishment, the MME can perform either manual or automatic 6to4 tunneling, according to RFC 3056, Connection of IPv6 Domains Via IPv4 Clouds.

## MME Interfaces Supporting IPv6 Transport

The following MME interfaces support IPv6 transport:

- S1-MME: runs S1-AP/SCTP over IPv6 and supports IPv6 addresses for S1-U endpoints.
- S3
- S6a
- S10
- S11
- S13
- SBc
- SGs
- SLg
- SLs
- Sv
- Gn

# Load Balancing

Load balancing functionality permits UEs that are entering into an MME pool area to be directed to an appropriate MME in a more efficient manner, spreading the load across a number of MMEs.

Load balancing is achieved by setting a weight factor for each MME so that the probability of the eNodeB selecting an MME is proportional to its weight factor. The weight factor is typically set according to the capacity of an MME node relative to other MME nodes. The weight factor is sent from the MME to the eNodeB via S1-AP messages.

Refer to the *Load Balancing and Rebalancing* chapter for more information about this feature.

MME load balancing can be used in conjunction with congestion control. For more information on congestion control, refer to the Congestion Control section in this chapter.

## Load Re-balancing

The MME load re-balancing functionality permits UEs that are registered on an MME (within an MME pool area) to be moved to another MME.

The rebalancing is triggered using an exec command on the mme-service from which UEs should be offloaded.

When initiated, the MME begins to offload a cross-section of its subscribers with minimal impact on the network and users. The MME avoids offloading only low activity users, and it offloads the UEs gradually (configurable from 1-1000 minutes). The load rebalancing can off-load part of or all the subscribers.

Refer to the *Load Balancing and Rebalancing* chapter in the *MME Administration Guide* for more information about this feature.

# Local Cause Code Mapping

Local cause code mapping provides the operator with the flexibility to ignore the default EPS Mobility Management (EMM) cause code and to configure a preferred EMM cause code to be sent to a UE in response to a procedural failure. For example, the operator can instruct the MME to return one of six different EMM cause codes other than the default when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

Local cause code mapping can be configured in either or both the MME-Service configuration or in the Call-Control Profile configuration. Refer to these two configuration modes in the *Command Line Interface Reference* to see the current list of **local-cause-code-mapping** commands.

# Management System Overview

The Operation and Maintenance module of the system offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces. For up-to-date details on the management options, refer to the *System Administration Guide*.

Operator-based MME configuration and monitoring functionality is enabled by default for console-based access via the command line interface. For more information on command line interface based management, refer to the *Command Line Interface Reference*.

# MME Double Counting Statistics of DECOR Rerouted Attach Accept

MME will not fetch UUT from HSS if it has already received from peer MME/SGSN and also in case of reroute scenarios.

In case of Initial attach (including local GUTI attach), when DECOR and the new CLI are configured, MME will fill the AIR-Flags to fetch UUT from HSS, irrespective of the UUT stored in MME-DB.

# MMEMgr Scaling to Support VPC-DI and USP

MME has undergone architectural changes to allow enhanced operations on Cisco's Virtual Packet Core (VPC)- Distributed Instance (DI) platform. VPC (Cisco's brand name for StarOS VM instances) is StarOS running as a virtual machine (VM). Multiple VMs act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management.

For the MME to take advantage of next generation platforms, such as the VPC-DI and USP, the MME architecture has been changed to allow:

- Linear capacity (memory) growth to support greater numbers of UEs and ENBs
- Signaling performance growth in term of CEPS
- Improved redundancy for RAN connections
- MMEMgr tasks are distributed across session PSC/DPC/SF-VM
- MMEDemux tasks are moved to demux PSC/DPC/SF-VM

- IMSIMgr scaling has increased the number of possible IMSIMgr tasks
- The maximum number of MME managers supported per SF is 4 for USP and VPC-DI platforms.
- In 21.9 and later releases: The maximum number of MMEMgrs supported per chassis is 48 for USP and VPC-DI platforms.

  In releases prior to 21.9: The number of MMEMgrs is increased to 24 on the VPC-DI platform.
- Two models of configuration, normal density and high density

For more information on the VPC platform, contact your Cisco Representative.

# MME Pooling

Provides support to configure MME pool area consisting multiple MMEs within which a UE may be served without any need to change the serving MME.

The benefits of MME pooling are:

- Enables Geographical Redundancy, as a pool can be distributed across sites.
- Increases overall capacity, as load sharing across the MMEs in a pool is possible (see the Load Balancing feature in this chapter).
- Converts inter-MME Tracking Area Updates (TAUs) to intra-MME TAUs for moves between the MMEs of the same pool. This substantially reduces signaling load as well as data transfer delays.
- Eases introduction of new nodes and replacement of old nodes as subscribers can be moved is a planned manner to the new node.
- Eliminates single point of failure between an eNodeB and MME.
- Enables service downtime free maintenance scheduling.

An MME Pool Area is defined as an area within which a UE may be served without need to change the serving MME. An MME Pool Area is served by one or more MMEs in parallel. MME Pool Areas are a collection of complete Tracking Areas. MME Pool Areas may overlap each other.

The Cisco MME supports MME Pooling functionality as defined in 3GPP TS 23.401. MME pooling allows carriers to load balance sessions among pooled MMEs.

The Cisco MME supports configuration of up to a pool size of 32 nodes.

# MME Selection

The MME selection function selects an available MME for serving a UE. This feature is needed for MME selection for handover with minimal MME changes.

MME selection chooses an available MME for serving a UE. Selection is based on network topology, i.e. the selected MME serves the UE's location and in case of overlapping MME service areas, the selection function may prefer MME's with service areas that reduce the probability of changing the MME.

# Mobile Equipment Identity Check

The Mobile Equipment Identity Check Procedure permits the operator(s) of the MME and/or the HSS and/or the PDN-GW to check the Mobile Equipment's identity with EIR.

The mobile equipment (ME) identity is checked through the MME by passing it to an Equipment Identity Register (EIR) over the S13 interface and then the MME analyzes the response from the EIR in order to determine its subsequent actions like rejecting or attaching a UE.

# Mobility Restriction

The following types of mobility restriction are supported on the MME:

- Handover Restriction
- Regional Zone Code Restriction

## Handover Restriction

Mobility Restriction comprises the functions for restrictions to mobility handling of a UE in E-UTRAN access. In ECM-CONNECTED state, the core network provides the radio network with a Handover Restriction List.

The MME performs mobility or handover restrictions through the use of handover restriction lists. Handover restriction lists are used by the MME operator policy to specify roaming, service area, and access restrictions. Mobility restrictions at the MME are defined in 3GPP TS 23.401.

## Regional Zone Code Restriction

Regional Zone Code Restriction allows an operator to control the areas in which a UE can roam in to receive service. The code representing the zone in which a UE is to be offered service by the network can be configured in the HSS or using local provisioning in the MME.

Once provisioned, the following restriction types are supported on the MME:

- HSS subscription based zone code restriction - if the subscription data in the HSS contains zone codes, the UE is allowed to camp only on those zones.

  Support for Regional Zone Code restriction based on HSS subscription data allows operators to offer zone based EPC subscriptions to home subscribers.

- Local policy based zone code restrictions - using the operator policy on the MME, certain ranges of IMSI or specific PLMN(s) could be restricted from or allowed to camp on, zones within the MME service area. This policy could apply to any PLMN.

  Local policy based zone code restriction allows operators to control access of EPC by roaming subscribers on a zone basis.

# Monitor Protocol Support for DCNR

Monitor Protocol is enhanced to display the newly introduced dcnr flag and rDCNR flag.

# Multiple PDN Support

This feature provides multiple PDN connectivity support for UE initiated service requests.

The MME supports an UE-initiated connectivity establishment to separate P-GWs or a single P-GW in order to allow parallel access to multiple PDNs. Up to 11 PDNs are supported per subscriber.

Refer to *PDN Type Control* in this chapter for information about the ability to control the PDN type (IPv4, IPv6) to which a given UE can be connected.

# NAS Protocol Support

MME provides this protocol support between the UE and the MME. The NAS protocol includes following elementary procedures for EPS Mobility Management (EMM) and EPS Session Management (ESM):

## EPS Mobility Management (EMM)

This feature used to support the mobility of user equipment, such as informing the network of its present location and providing user identity confidentiality. It also provides connection management services to the session management (SM) sublayer.

An EMM context is established in the MME when an attach procedure is successfully completed. The EMM procedures are classified as follows:

- **EMM Common Procedures**: An EMM common procedure can always be initiated when a NAS signaling connection exists.

  Following are the common EMM procedure types:

  - Globally Unique Temporary Identity (GUTI) reallocation
  - Authentication and security mode
  - Identification
  - EMM information

- **EMM Specific Procedures**: This procedure provides Subscriber Detach or de-registration procedure.
- **EMM Connection Management Procedures**: This procedure provides connection management related function like Paging procedure.

## EPS Session Management (ESM)

This feature is used to provide the subscriber session management for bearer context activation, deactivation, modification, and update procedures.

# NAS Signaling Security

The NAS Signaling Security feature provides integrity protection and encryption of NAS Signaling. The NAS security association is between the UE and the MME.

The MME uses the NAS security mode command procedure to establish a NAS security association between the UE and MME, in order to protect the further NAS Signaling messages.

See the *NAS Signaling Security* chapter for more information.

# NB-IOT EDRX Supported values in ATTACH/TAU Accept

With release 21.14, for the NBIOT devices, If the Extended DRX parameter values are 4, 6, 7 or 8, it is interpreted as 2 and sent in the Attach-Accept or in the TAU Accept.

# Network Sharing

The LTE architecture enables service providers to reduce the cost of owning and operating the network by allowing the service providers to have separate Core Network (CN) elements (MME, SGW, PDN GW) while the E-UTRAN (eNBs) is jointly shared by them. This is enabled by the S1-flex mechanism by enabling each eNodeB to be connected to multiple CN entities. When a UE attaches to the network, it is connected to the appropriate CN entities based on the identity of the service provider sent by the UE.

In such a network sharing configuration, complete radio (access) network and partial core network is shared among different operators. Each operator has its own network node for S-GW/P-GW, etc., while sharing a MME and the rest of the radio network.

To support this network sharing configuration, the MME service can be configured with multiple local PLMNs per service. This means that each mme-service will handle multiple PLMNs and will indicate this to the eNodeb during S1 SETUP procedure (as well using the S1 MME CONFIGURATION UPDATE message).

The configuration of these additional PLMNs is implemented using the **network-sharing** command within the MME service configuration mode. Refer to the *Command Line Reference* for detailed information on using this command.

When a UE attaches to the MME, the GUTI assignment will use the mme id corresponding to the PLMN configuration. The plmn-id filter in the operator policy selection criteria allows PLMN-specific configurations in an operator policy.

# Operator Policy Support

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

The operator policy configuration to be applied to a subscriber is selected on the basis of the selection criteria in the subscriber mapping at attach time. A maximum of 1,024 operator policies can be configured. If a UE was associated with a specific operator policy and that policy is deleted, the next time the UE attempts to access the policy, it will attempt to find another policy with which to be associated.

A default operator policy can be configured and applied to all subscribers that do not match any of the per-PLMN or IMSI range policies.

Changes to the operator policy take effect when the subscriber re-attaches and subsequent EPS Bearer activations.

Refer to the *Operator Policy* chapter in this guide for more information.

# Operator Policy Selection Based on IMEI-TAC

With this feature, the MME selects / re-selects an operator policy for call handling based on the user equipment's (UE's) unique international mobile equipment identity - type allocation code (IMEI-TAC) rather than the normal selection method, which is based on the UE's international mobile subscriber identity (IMSI) and PLMN-ID. The TAC (the first 8 digits of the 15 or 16-digit IMEI / IMEI-SV) serves to identify the equipment type - enabling the operator to configure how calls are handled based on the equipment type. And the operator can configure up to 25,000 IMEI-TAC in groups of individual IMEI-TAC or ranges.

For more information on configuring this functionality, refer to *Operator Policy Selection Based on IMEI-TAC* chapter of the *MME Administration Guide*.

# Overload Control

Using the Congestion Control functionality or the Enhanced Congestion Control functionality, the MME can signal to the eNodeBs to which it is connected to redirect traffic to other MMEs in the MME pool. This is accomplished using the S1 interface Overload Procedure (3GPP TS 36.300 and 3GPP TS 36.413).

When overload control is configured and a congestion threshold is reached, the MME can be configured to send an S1AP Overload Start message to a percentage of the eNodeBs to which the MME is connected. To reflect the amount of load that the MME wishes to reduce, this percentage configurable. In the Overload Response IE sent to the eNodeBs, the MME can request the eNodeB to reject or permit specific types of sessions, including:

- reject non-emergency sessions
- reject new sessions
- permit emergency sessions
- permit high-priority sessions and mobile-terminated services
- reject delay-tolerant access.

For more information or to configure Overload Control using the basic Congestion Control functionality, refer to the *Congestion Control* chapter in the *System Administration Guide*.

For more information or to configure Overload Control using the **Enhanced** Congestion Control functionality, refer to the *Enhanced Congestion Control and Overload Control* chapter in this guide.

# PDN Type Control

PDN Type Control enables the MME to override the requested Packet Data Network (PDN) type based on the inbound roamer PLMN, and assign the UE to an IPv4 only or IPv6 only PDN.

If a UE requests an IPv4v6 PDN, it can be downgraded to an IPv4- or IPv6-only address. The MME signals the appropriate cause to the UE to account for the PDN type change.

This functionality enables operators to control resource usage for roaming and home subscribers differently, and ensures that IP network continuity works for inbound roamers.

PDN Type Control is configured in a call control profile that is applied via an operator policy. Refer to the *Call Control Profile Configuration Mode* chapter of the *Command Line Reference* for more information.

# Packet Data Network Gateway (P-GW) Selection

Provides a straightforward method based on a default APN provided during user attachment and authentication to assign the P-GW address in the VPLMN or HPLMN. The MME also has the capacity to use a DNS transaction to resolve an APN name provided by a UE to retrieve the PDN GW address.

P-GW selection allocates a P-GW that provides the PDN connectivity for the 3GPP access. The function uses subscriber information provided by the HSS and possibly additional criteria. For each of the subscribed PDNs, the HSS provides:

- an IP address of a P-GW and an APN, or
- an APN and an indication for this APN whether the allocation of a P-GW from the visited PLMN is allowed or whether a P-GW from the home PLMN shall be allocated.

The HSS also indicates the default APN for the UE. To establish connectivity with a PDN when the UE is already connected to one or more PDNs, the UE provides the requested APN for the PDN GW selection function.

If the HSS provides an APN of a PDN and the subscription allows for allocation of a PDN GW from the visited PLMN for this APN, the PDN GW selection function derives a PDN GW address from the visited PLMN. If a visited PDN GW address cannot be derived, or if the subscription does not allow for allocation of a PDN GW from the visited PLMN, then the APN is used to derive a PDN GW address from the HPLMN.

# Radio Resource Management Functions

Radio resource management functions are concerned with the allocation and maintenance of radio communication paths, and are performed by the radio access network.

To support radio resource management in E-UTRAN, the MME provides the RAT/Frequency Selection Priority (RFSP) parameter to an eNodeB across S1. The RFSP is a "per UE" parameter that is used by the E-UTRAN to derive UE specific cell reselection priorities to control idle mode camping. The RFSP can also be used by the E-UTRAN to decide on redirecting active mode UEs to different frequency layers or RATs.

The MME receives the RFSP from the HSS during the attach procedure. For non-roaming subscribers, the MME transparently forwards the RFSP to the eNodeB across S1. For roaming subscribers, the MME may alternatively send an RFSP value to the eNodeB across S1 that is based on the visited network policy, such as an RFSP pre-configured per Home-PLMN or a single RFSP's values to be used for all roamers independent of the Home-PLMN.

# RAN Information Management

The MME supports RAN Information Management (RIM) procedures as defined in 3GPP TS 23.401 on the S1-MME, S3, Gn, and S10 interfaces.

RIM procedures allow the MME to exchange information between applications belonging to the RAN nodes. The MME provides addressing, routing and relaying support for the RAN information exchange.

# Reachability Management

It provides a mechanism to track a UE which is in idle state for EPS connection management.

To reach a UE in idle state the MME initiates paging to all eNodeBs in all tracking areas in the TA list assigned to the UE. The EPS session manager have knowledge about all the eNodeB associations to the MME and generates a list of eNodeBs that needs to be paged to reach a particular UE.

The location of a UE in ECM-IDLE state is known by the network on a Tracking Area List granularity. A UE in ECM-IDLE state is paged in all cells of the Tracking Areas in which it is currently registered. The UE may be registered in multiple Tracking Areas. A UE performs periodic Tracking Area Updates to ensure its reachability from the network.

# SCTP Multi-homing Support

This sections describes multi-homing support for specific interfaces on the MME.

- **S1-MME** support for up to two SCTP bind end point IPv4 or IPv6 addresses.
- **S6a** support for up to four SCTP bind end point IPv4 or IPv6 addresses.
- **SBc** support for up to two SCTP bind end point IPv4 or IPv6 addresses.
- **SGs** support for up to two SCTP bind end point IPv4 or IPv6 addresses.
- **SLs** support for up to two SCTP bind end point IPv4 or IPv6 addresses.

# Serving Gateway Pooling Support

The S-GW supports independent service areas from MME pooling areas. Each cell is associated to a pool of MMEs and a pool of Serving Gateways. Once a cell selects an MME, that MME is able to select an S-GW which is in an S-GW pool supported by the cell.

Static S-GW pools can be configurable on the MME. Each pool is organized as a set of S-GWs and the Tracking Area Identities (TAIs) supported by them, known as a service area (SA). The incoming TAI is used to select an SA. Then, based on protocol and statistical weight factors, an S-GW is selected from the pool serving that SA. The same list of S-GWs may serve multiple TAIs. Static S-GW pools are used if there is no DNS configured or as a fallback if DNS discovery fails.

For additional Information on TAI lists, refer to the *Tracking Area List Management* section in this overview.

# Serving Gateway Selection

The Serving Gateway (S-GW) selection function selects an available S-GW to serve a UE. This feature reduces the probability of changing the S-GW and a load balancing between S-GWs. The MME uses DNS procedures for S-GW selection.

The selection is based on network topology the selected S-GW serves the UE's location, and in the case of overlapping S-GW service areas, the selection may prefer S-GWs with service areas that reduce the probability of changing the S-GW. If a subscriber of a GTP-only network roams into a PMIP network, the PDN GWs (P-GWs) selected for local breakout supports the PMIP protocol, while P-GWs for home routed traffic use GTP. This means the S-GW selected for such subscribers may need to support both GTP and PMIP, so that it is possible to set up both local breakout and home routed sessions for these subscribers.

# Session and Quality of Service Management

This support provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

The MME Operator Policy configuration allows the specification of QoS for each traffic class that can either be used as a default or as an over ride to the HSS settings.

In LTE-EPC 4G architectures, QoS management is network controlled via dynamic policy interactions between the PCRF and PDN GW. EPS bearer management is used to establish, modify or remove dedicated EPC bearers in order to provide service treatments tied to the needs of specific applications/service data flows. The service priority is provisioned based on QoS Class Identifiers (QCI) in the Gx policy signaling. PCRF signaling interaction may also be used to establish or modify the APN-AMBR attribute assigned to the default EPS bearer.

When it is necessary to set-up a dedicated bearer, the PDN GW initiates the Create Dedicated Bearer Request which includes the IMSI (permanent identity of mobile access terminal), Traffic Flow Template (TFT - 5-tuple packet filters) and S5 Tunnel Endpoint ID (TEID) information that is propagated downstream via the S-GW over the S11 interface to the MME. The Dedicated Bearer signaling includes requested QoS information such as QCI, Allocation and Retention Priority (ARP), Guaranteed Bit Rate (GBR - guaranteed minimum sending rate) and Maximum Bit Rate (MBR- maximum burst size).

The MME allocates a unique EPS bearer identity for every dedicated bearer and encodes this information in a Session Management Request that includes Protocol Transaction ID (PTI), TFT's and EPS bearer QoS parameters. The MME signals the Bearer Setup Request in the S1-MME message toward the neighboring eNodeB.

# Session Tracing

The subscriber-level Session Tracing provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an LTE environment. In general, the Session Tracing capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

For more information about this functionality, see the *Session Tracing* chapter in this guide.

# State-Location Information Retrieval Flag

In compliance with 3GPP TS 29.272 v11.9.0, the MME sends the "State/Location-Information-Retrieval" flag set in the Feature-List AVP of the Update Location Request (ULR) message over the S6a interface to the HSS at the time the UE attaches. With the "State/Location-Information-Retrieval" flag set, the HSS knows to set the "EPS User State Request", "EPS Location Information Request" and "Current Location Request" bits in the IDR-Flags AVP in IDR messages towards the MME. This subscriber data provides the UE's current location information needed in multiple service scenarios, such as VoLTE services on the IMS side.

For more information about this functionality, see the *State-Location Information-Retrieval Flag* feature chapter in this guide.

# Target Access Restricted for the Subscriber Cause Code

This enhancement is a 3GPP TS (29.274 and 29.060) release compliance enhancement. As per 3GPP TS 29.274 and TS 29.060,the source-serving node (MME/SGSN) is allowed to reject SGSN Context Request (GTPv1) and Context Request (GTPv2) mobility management messages with "Target Access Restricted for the subscriber" cause if target access is restricted for the subscriber based on the Access-Restriction-Data in the subscription profile. The target node (MME/SGSN) is allowed to reject RAU/TAU with anyone one of the following NAS Causes:

- 15 "No suitable cells in tracking area", or
- 13 "Roaming not allowed in this tracking area", or
- 12 "Tracking area not allowed"

New statistics have been introduced under "show egtpc statistics verbose" and "show sgtpc statistics verbose" to reflect the context response sent and received with the new reject cause "Target Access Restricted for the subscriber".

Rejecting RAU/TAU much early in call cycle results in reduced signaling.



**Important** No new CLI is provided for GTP cause code mapping to EMM/NAS cause. RAU Reject will always be sent with NAS cause "No suitable cells in location area" and TAU Reject will always be sent with EMM cause "No suitable cells in Tracking Area".



**Important** The MME and SGSN revert to the old behavior as per earlier releases if the peer node is not capable of sending the RAT-TYPE IE in CONTEXT-REQ message.

*For more information refer to the 3GPP TS 29.274 (section 7.3.6), TS 29.060 (section 7.5.4), TS 29.060 Annex B (Table B.5: Mapping from Gn/Gp to NAS Cause values Rejection indication from SGSN) and TS 29.274 Annex C ( Table C.5: Mapping from S3/S16 to NAS Cause values Rejection indication from MME/S4-SGSN)*

# Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, number of sessions etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management functionality of an element manager.

The Alarm System is used only in conjunction with the Alarm model.



**Important** For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

# Tracking Area List Management

Provides the functions to allocate and reallocate a Tracking Area Identity (TAI) list to the UE to minimize Tracking Area Updates (TAUs).

The MME assigns the TAI list to a UE so as to minimize the TAUs that are sent by the UE. The TAI list should be kept to a minimum in order to maintain a lower paging load.

The MME allows up to 16 tracking areas configured locally to be included and sent to the mobile station in Tracking Area List IE as part of Attach/TAU Accept message.

# UMTS to LTE ID Mapping

The MME allows seamless inter-RAT interworking when the operator's networks are configured with LACs allocated from the reserved space of 32K to 64K. 3GPP Specifications have reserved this space for LTE MME Group IDs. The MME and SGSN can distinguish between UMTS IDs (P-TMSI/RAI) and LTE IDs (GUTI) by configuring an MME group ID to PLMN ID mapping.

**Use Case 1:** When a UE moves from 3G to LTE, the UE maps the P-TMSI and RAI to GUTI and uses this mapped GUTI in the TAU Attach Request that it sends to the MME. At the MME, this mapped GUTI gets reverse mapped to P-TMSI and RAI, which are used to fetch the UE's Context from the old SGSN.

**Use Case 1:** When a UE moves from LTE to 3G, the UE maps the GUTI to P-TMSI and RAI, and performs a RAU Attach to the SGSN. A Pre-Rel8 SGSN would attempt to fetch the UE's context over the Gn/Gp

interface using the mapped P-TMSI and RAI. At the MME, the P-TMSI and RAI are reverse mapped to GUTI to fetch the locally stored UE's context. An S3-SGSN also behaves similar to Pre-Rel8 SGSN except for the way it discovers the source MME. S3-SGSN identifies the P-TMSI & RAI received in RAU Request as a mapped one and performs LTE specific DNS query using MME ID, to discover the source MME.

For the two use cases above, the MME/S3-SGSN would need to identify whether a given UMTS or LTE ID is a native one or a mapped one. MME GroupID or LAC is used to make this distinction. If the Most Significant Bit(MSB) in LAC is set then the UMTS ID is mapped from LTE. Similarly, if the MSB of MME Group ID is zero then the LTE ID is mapped from UMTS. If the standard defined ranges are not complied, the target MME/S3-SGSN may incorrectly conclude the source node as S3-SGSN/MME. This misinterpretation would lead to unsuccessful attempt to resolve the source node since the DNS query is formulated with the assumption that the source node is either MME or S3-SGSN.

In order to address networks where the 1/0 MSB logic does not apply, the MME and SGSN can rely on a global database of MME Group IDs (configured via CLI) instead of the standards specified MSB, to distinguish between mapped and native UMTS and LTE IDs.

The MME consults this database of MME Group IDs when the below two conditions apply:

1. The MME is not aware of the received GUTI Type, such as when either the UE or the network are not Release 10 compliant.

2. MME-Service is associated with the MME Group ID database.

Refer to *Configuring UMTS to LTE ID Mapping* in Chapter 2 of this document for steps to create and configure this database and to associate the MME service to this database.

# VoLTE Offloading

Offloading of a certain percentage of users can be configured using the **mme offload** command. The MME sends S1 Release (with cause "load balancing TAU required" for offload) to the configured percentage of UEs attached to the MME. The MME does not distinguish between VoLTE and Non-VoLTE subscribers. Some subscribers with voice bearers are also offloaded as a result calls are dropped. This feature enhancement is targeted to preserve VoLTE voice bearers during MME offloading. A new CLI keyword is added to the **mme offload** command to preserve VoLTE subscribers (QCI = 1) from offloading until voice calls are terminated.



**Note** This feature enhancement is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

# VoLTE Support based on UEs SRVCC Capability

MME sends "Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions" to HSS only for SRVCC capable UEs. Once MME is configured with the **network-feature-support-ie ims-voice-over-ps supported srvcc-ue** CLI command, only "SRVCC capable" and "SRVCC subscribed" UEs are allowed to make VoLTE calls. SRVCC non-capable UEs have to do CSFB to get the voice services. This ensures that the UEs not capable of SRVCC will not experience any call disconnects if they move between 4G and 3G networks.

In releases prior to 21.5, MME used to allow all subscribed users to make VoLTE call irrespective of whether SRVCC was supported by the UE or not when **network-feature-support-ie ims-voice-over-ps support** CLI command was configured.

# Features and Functionality - Licensed Enhanced Feature Software

This section describes the optional enhanced features and functions for MME service.

**Important** The following features require the purchase of an additional feature license to implement the functionality with the MME service.

## Feature Description

### 128K eNodeB Connection Support

The MME now supports 128K eNodeB connections for VPC-DI and ASR5500-DPC2 platforms; it has been enhanced from 64K eNodeB connections. A MME manager instance supports 4K eNodeBs, a minimum of 32 MME managers are required to support 128K eNodeB's. If the network has more than 32 MME managers, 128k eNodeB connections limit is not enforced. The support for 128K eNodeB connections is per chassis and not per MME service.

The maximum number of MME managers that can be configured per chassis for the VPC-DI platform has been enhanced from "24" to "48".

### Distribution of Multiple SCTP Association - VLR

The SCTP associations of a VLR are now distributed across MME managers. Distribution of VLR SCTP associations across MME managers helps in achieving better load distribution at the MME managers.

There is no change for load balancing of SGs messages sent by MME across multiple SCTP associations of a VLR.

### S1-SCTP Rate Limiting

The operator can now configure a rate limit for incoming S1 SCTP connections from the eNodeB. This prevents an overload at the MME in case there is a surge of S1 SCTP connections from the eNodeBs. New command keywords **s1-sctp rate limit** are introduced in the **task facility mmedemux** command, they can be used to specify the rate limit value of connections per second for the chassis. New MME Demux subsystem statistics are introduced to display the number of packets that are dropped due to the configured rate limit.

## Attach Rate Throttling

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature enables operators to limit the rate at which the MME processes new connections (attaches, TAU requests, and forward relocation requests) which in turn reduces the signaling on the external nodes.

See the **network-overload-protection mme-new-connections-per-second** command in the *Global Configuration Mode Commands* chapter of the *Command Line Reference* for more information.

# Cell Traffic Trace

The Cell Traffic Trace feature provides a 3GPP standard-based cell trace function for tracing all calls in a single cell or multiple cells. Cell Tracing provides the capability to log on to data on any interface at a call level for a specific user or mobile type or a service initiated by a user. In addition, Cell Tracing provides instantaneous values for a specific event.

The Cell Traffic Trace feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

For more information on Cell Traffic Trace refer to the *Cell Traffic Trace* feature chapter.

# CSFB and SMS over SGs Interface

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Circuit Switched Fallback (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switch over to the circuit switched (CS) domain or other CS-domain services (e.g., Location Services (LCS) or supplementary services). Additionally, SMS delivery via the CS core network is realized without CSFB. Since LTE EPC networks were not meant to directly anchor CS connections, when any CS voice services are initiated, any PS based data activities on the E-UTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

For additional information, refer to the *CSFB and SMS over SGs Interface* section in this guide.

# CSFB and SRVCC for CDMA

This functionality requires valid license keys be installed. Contact your Cisco Account or Support Representative for information required licenses.

The MME already supports circuit switched fallback (CSFB) and single radio voice call continuity (SRVCC) for E-UTRAN. The MME has expanded support to normal and enhanced CSFB and SRVCC for CDMA 1xRTT (single-carrier radio transmission technology) networks.

The primary purpose of either CSFB or SRVCC for CDMA is to enable a UE from an LTE network to move seamlessly to a CDMA network and ensure that CDMA2000 messages are received from the UE and then relayed to the MSC (or vice-versa) through S1-APP and S102 interfaces. The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWF/MSC.

For details on these functions and their configuration, refer to the *CSFB for 1xRTT* and *SRVCC for 1xRTT* feature chapters in this administration guide.

# Customized Inter-MME SGW S1-Handover and TAU Procedure for PS-LTE Support

In the Public Safety LTE (PS-LTE) network, every MME is co-located with an S-GW and at least one P-GW, and the MME must always use the co-located S-GW and a co-located P-GW for all calls that it handles. This requires configuring the IP addresses of the S11 interface of the S-GW as part of the MME service configuration, and the S5/S8 interface of the P-GW as part of an APN profile configuration. An MME configured for PS-LTE network operation will not send any DNS queries for S-GW or P-GW lookup, it will only use the S-GW

configured for PS-LTE operation and the P-GW configured in the matching APN profile regardless of any other configuration present.

All intra-MME S1 and X2 handovers and all TAU Requests with a local GUTI will be serviced by the same S-GW that is configured for PS-LTE network operation with the P-GW(s) used at the time of the initial Attach or relocation to the MME. S-GW relocation is neither necessary nor supported for intra-MME handovers or intra-MME TAU Requests

This feature allows the co-location of the MME, P-GW and S-GW nodes for Public Safety deployments.

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

# DDN Throttling

The DDN Throttling feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

In this feature, MME is provisioned to reject non-priority (traffic based on ARP and LAPI) Downlink Data Notification (DDN) requests when the UE is in idle mode. Additionally, MME dynamically requests S-GW to reduce the number of DDN requests based on a throttling factor and a throttling delay specified in the DDN Ack message.

For more information on configuring this functionality, refer to *DDN Throttling* chapter of the *MME Administration Guide*.

# Enhanced Congestion Control and Overload Control

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature builds on the functionality provided by the Congestion Control and Overload Control features described in the *Features and Functionality - Base Software* section.

To allow greater control during overload conditions, the MME supports the configuration of three separate levels (critical, major, minor) of congestion thresholds for the following system resources:

- System CPU usage
- System service CPU usage (Demux-Card CPU usage)
- System Memory usage
- License usage
- Maximum Session per service

The MME can, in turn, be configured to take specific actions when any of these thresholds are crossed, such as:

- Drop or reject the following S1-AP/NAS messages: S1 Setup, Handover events, TAU request, Service request, PS-Attach request, Combined-attach request, Additional PDN request, or UE initiated bearer resource allocation.
- Allow voice or emergency calls/events.
- Initiate S1AP overload start to a percentage of eNodeBs with options to signal any of the following in the Overload Response IE:
  - reject non-emergency sessions
  - reject new sessions

- permit emergency sessions
- permit high-priority sessions and mobile-terminated services
- reject delay-tolerant access.

For more information on configuring this functionality, refer to *Enhanced Congestion Control and Overload Control* chapter of the *MME Administration Guide*.

# Feature Description

This feature is developed to provide MME support for eMPS (Enhanced Multimedia Priority Service) in PS (Packet Switched) and CS (Circuit Switched) domains. If UEs subscription information contains MPS-Priority AVP and the MPS-EPS-Priority bit set, the MME classifies such UEs for Enhanced Multimedia Priority Service (eMPS) in PS domain. The MME includes paging priority IE in S1 AP Paging message if it receives events like DDN/CBR/UBR for users having MPS EPS subscription. The MME also supports priority SRVCC handovers by providing ARP information to the MSC in SRVCC PS to CS Request message.



**Important** This feature is license controlled. Please consult your Cisco Account Representative for information about the specific license.

# HSS-based P-CSCF Restoration

The HSS-based P-CSCF Restoration feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

PCSCF Restoration aids in successful establishment of MT VoLTE calls when the serving P-CSCF has failed or unreachable.

The HSS-based P-CSCF Restoration mechanism is executed when a terminating request cannot be serviced due to a P-CSCF failure. The execution is possible if there are no other registration flows available for the terminating UE using an available P-CSCF.

The HSS-based P-CSCF restoration consists of a basic mechanism that makes usage of a path through HSS and MME/SGSN to request the release of the IMS PDN connection to the corresponding UE and an optional extension that avoids the IMS PDN deactivation and re-activation.

The HSS-based P-CSCF Restoration complies with the following standard: 3gpp TS 23.380 section 5.4 HSS-based P-CSCF Restoration.

For more information on configuring this functionality, refer to *HSS-based P-CSCF Restoration* chapter of the *MME Administration Guide*.

# Idle-mode Signaling Reduction

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Idle-mode Signaling Reduction (ISR) allows a UE to be registered on (and roam between) E-UTRAN and UTRAN/GERAN networks while reducing the frequency of TAU and RAU procedures and overall signaling.

Refer to the *Idle-mode Signaling Reduction* chapter in the *MME Administration Guide* for more information.

# IP Security (IPSec)

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways.

IPSec can be implemented on the system for the following applications:

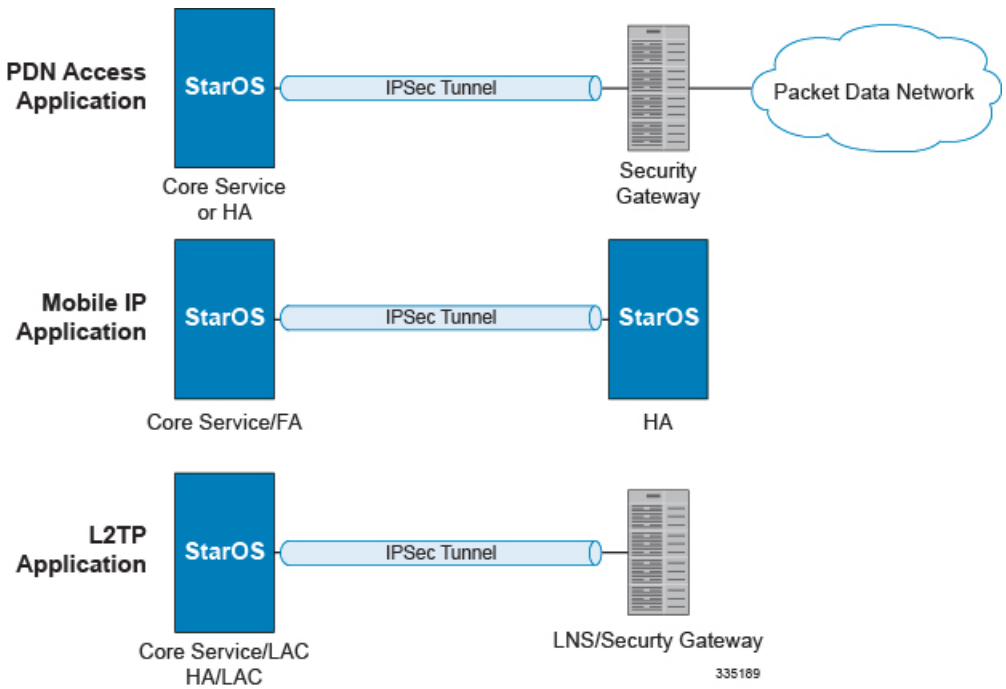
- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.

**Important** Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

- **L2TP**: L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

The following figure shows IPSec configurations.

***Figure 4: IPSec Applications***



**Important** For more information on IPSec support, refer to the *Cisco StarOS IP Security (IPSec) Reference*.

# IPNE Service Support

The MME supports the IP Network Enabler (IPNE), a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers.

**Important** This feature, with its CLI commands, counters, and statistics, are all under development for future use and are not yet fully qualified.

The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services.

Implementation of this feature requires configuration of an IPNE Service that is then associated with the MME Service refer to the *IPNE Service Configuration Mode Commands* and *MME Service Configuration Mode Commands* in the *Command Line Interface Reference* manual. This feature and its configuration are described in greater detail in the *IPNE Service* chapter in this guide.

IPNE and MINE clients are each licensed Cisco features. Contact your Cisco account representative for information on licensing requirements. For additional information about this feature and how to configure it, refer to the section on *IPNE Service* in this guide.

# Lawful Intercept

The Lawful Intercept feature-use license is included in the MME session-use license.

The Cisco Lawful Intercept feature is supported on the MME. Lawful Intercept is a license-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

# Location Services

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

LoCation Services (LCS) on the MME and SGSN is a 3GPP standards-compliant feature that enables the system (MME or SGSN) to collect and use or share location (geographical position) information for connected UEs in support of a variety of location services.

The SLs interface is used to convey LCS Application Protocol (LCS-AP) messages and parameters between the MME to the Evolved Serving Mobile Location Center (E-SMLC). It is also used for tunnelling LTE Positioning Protocols (LPP between the E-SMLC and the target UE, LPPa between the E-SMLC and the eNodeB), which are transparent to the MME.

Refer to the *Location Services* chapter in the *MME Administration Guide* for more information.

# MBMS for MME (eMBMS)

The MME provides full 3GPP TS 23.246 support for the LTE version of multimedia broadcast / multicast service (MBMS) -- eMBMS. Running the Cisco MME-eMBMS service on the MME, the MME communicates with the MBMS GW and the MCE using Sm and M3 interfaces. MME-eMBMS facilitates sessions scheduled by the BM-SC, identifies service areas to be served by a particular MBMS session, and handles session start, update, and stop as well as setup and configuration requests from the MCEs.

The Sm and M3 interfaces for MME-eMBMS require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

For more information on configuring this functionality, refer to *MBMS for MME (eMBMS)* chapter of the *MME Administration Guide*.

# MME Handling of PGW Restart

This feature requires that a valid MME Resiliency license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

P-GW Restart Notification Procedure is a standards-based procedure supported on the S-GW to notify detection of P-GW failure to the MME/S4-SGSN. P-GW failure detection is performed by the S-GW when it detects that the P-GW has restarted (based on restart counter received from the restarted P-GW) or when it detects that P-GW has failed but not restarted (based on path failure detection). When an S-GW detects that a peer P-GW has restarted, it deletes all PDN connection table data and bearer contexts associated with the failed P-GW and notifies the MME via P-GW Restart Notification. The S-GW indicates in the echo request/response on S11/S4 interface that the P-GW Restart Notification procedure is supported.

P-GW Restart Notification Procedure is an optional procedure and is invoked only if both the peers, MME/S4-SGSN and S-GW, support it.

In the absence of this procedure, the S-GW will initiate the Delete procedure to clear all the PDNs anchored at that failed P-GW, which can lead to flooding of GTP messages on S11/S4 interface if there are multiple PDNs using that S-GW and P-GW.

The MME adds support for the P-GW restart handling procedures as specified in 3GPP TS 23.007 v11.6.0. An S-GW will send the "PGW Restart Notification" message only to the SGSNs / MMEs that indicated their support of this feature through the Echo Request -> Node Features IE -> PRN bit.

This feature reduces the S11 signaling load between the S-GW and MME in case of a P-GW restart.

### PDN Deactivation Behavior

If a PDN is impacted and needs to be restored:

- If all PDNs of a UE are impacted, a UE in ECM-Connected state will be explicitly detached with cause "reattach required" and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be explicitly detached with cause "reattach required". Otherwise, the UE will be implicitly detached.
- If some PDNs of a UE are impacted, a UE in ECM-Connected will be sent NAS Deactivate Bearer Request with cause "reactivation requested" and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be sent a NAS Deactivate Bearer Request with cause "reactivation requested". Otherwise, the PDN will be locally deactivated.

If a PDN is impacted but does **not** need to be restored:

- If all PDNs of a UE are impacted, a UE in ECM-Connected state will be explicitly detached with cause "reattach required" and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be explicitly detached with cause "reattach required". Otherwise, the UE will be implicitly detached.
- If some PDNs of a UE are impacted, a UE in ECM-Connected will be sent NAS Deactivate Bearer Request with cause "regular deactivation", and a UE in ECM-IDLE will **not** be paged and will be locally deactivated in a paced manner.

#### PDN Deactivation Rate

By default, the MME will perform deactivations at the rate of 100 PDNs ( 50 Idle + 50 Connected) per session manager per second. This rate will be applied to MME specific pacing queues ( Idle & Connected).

This default pacing rate can be altered using the **MME Messaging Rate Control** feature.

Refer to the *MME Administration Guide* and to the **network-overload-protection mme-tx-msg-rate** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for more information about this feature.

**Note:** Configuration of this deactivation rate should be based on appropriate dimensioning exercise to arrive at the appropriate rate.

#### PDN Reactivation Behavior

After the affected subscribers have been deactivated, the MME will prioritize the re-activation of impacted PDN connections based on subscribed APN restoration priority, if received from the HSS. If an APN restoration priority is not received from the HSS, then this locally configured value is used. If there is no local configuration then by default such PDNs will be assigned the lowest restoration priority.

#### Limitations

Currently, the MME does not deactivate a PDN connection upon receiving P-GW Restart Notification when the P-GW serving the PDN is dual IP stack.

The PGW Restart Notification is received with cause PGW-NOT-RESPONDING, however the MME is not able to find the matching P-GW entry as the MME stores either IPv4 or IPv6 PGW address.

This occurs when the PGW Restart Notification does not contain the P-GW IP address stored by MME.

# MME Message Rate Control

This feature requires that a valid MME Resiliency license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature provides controls to mitigate the undesirable effects of congestion due to excessive S1 Paging load or upon failure of an EGTPC path.

See the **network-overload-protection mme-tx-msg-rate-control** command in the *Global Configuration Mode Commands* chapter of the *Command Line Reference* for more information.

## S1 Paging Rate Limit

The MME provides a configuration to limit the rate of S1 paging requests sent per eNodeB. S1 Paging requests exceeding the configured rate threshold are dropped. All S1 Paging requests are treated uniformly without any special considerations for the type of paging request (CS/PS).

## Pacing UE Deactivation

During an EGTPC (S11/S10/S3) path failure, the MME detects the failure and begins the process of deactivating all UE sessions affected. The MME supports two separate configurable internal pacing queues for deactivating UEs: one for active UEs and a second for idle mode UEs. This enables the path failure processing and deactivation pacing rate to be different for each of these queues.

Upon detecting an EGTPC path failure, the impacted EGTPC tunnels are added to separate queues based on ECM-State and deactivations are scheduled based on the respective configured rates.

# MME Restoration - Standards Extension

The feature implements the Network Triggered Service Restoration (NTSR) procedures defined in 3GPP TS 23.007 Release 11 (DDN with IMSI) on the MME.

By implementing the extensions to the standard MME restoration, the robustness of the network is greatly enhanced and potential issues due to the MME downtime are mitigated.

The solution to recover from MME node failures proposed in the 3GPP standards rely on the deployment of MME pools where each pool services a coverage area. Following a MME failure, the S-GW and MSC/VLR nodes may select the same MME that used to service a UE, if it has restarted, or an alternate MME in the same pool to process Network-initiated signaling that it received in accordance with the NTSR procedures defined in 3GPP TS 23.007 Release 11.

Upon receipt of a DDN without any TAI list or other previously sent information from the S-GW after a MME failure or restart, the MME shall proceed with regular IMSI-based paging.

The MME can be configured to throttle IMSI-based DDN requests as needed to maintain adequate service performance for normal procedure processing. Refer to the **network-overload-protection mme-new-connections-per-second** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

## MME/VLR Restoration Procedure via Alternate MME

The MME now supports the Mobile Terminated CS service delivery via an alternate MME in MME pool feature described in 3GPP TS 23.007 Section 14.1.3 & 26 and 29.118 Release 11.

Upon receipt of a SGs Paging request from a VLR with CS restoration bit set, the MME will perform a regular IMSI-based paging procedure, in the absence of any additional context information. If the CS Restoration Indicator is set, the MME shall page the UE regardless of the value of MME-Reset indicator. The location information shall be set in accordance with the existing procedures for unknown UE with the MME-Reset indicator set to TRUE.

No special configuration is needed to enable this functionality.

## ULA for Periodic TAU when VLR Inaccessible

When processing a periodic TAU request from a UE, if the MME detects that the VLR serving the UE is inaccessible, the MME now selects an alternative VLR that is in service for the UE and performs a location update for non-EPS services procedure towards the selected VLR.

The MME previously supported this functionality in case of non-periodic TAU.

# MTC Features

The MTC feature set allows the operator to handle the signaling storm MTC devices can bring to the network thus ensuring a more robust network and more efficient resource utilization The MME supports several of the 3GPP TS23.401 R10 machine type communications (MTC) overload control mechanisms to be used in the handling of signaling bursts from machine-to-machine (M2M) devices.

Some of the features in the set include:

- Configurable congestion control for LAPI subscribers.
- Configurable congestion control based on specific APN.
- Support for reject causes with MM and SM back off timers: EMM T3346 timer, ESM T3346 timer, and ESM T3396 timer
- Support for subscribed periodic TAU timer - extended-t3412 timer

The MTC feature set requires that a valid license key be installed.This license will be enforced for usage of related commands. Contact your Cisco Account or Support representative for information on how to obtain a license.

# Network Provided Location Info for IMS

Network provided Location Info (NPLI) enables the MME to send user location information (ULI) to the P-GW/S-GW (and consequently PCRF) in a number of Session Management messages. This information is required for Lawful Intercept (LI), VoLTE, aids in charging in the IMS domain.

The MME supports the PCC-EPC based framework is defined in 3GPP TR 23.842 section 6.4, which allows the P-CSCF to request the user location through PCRF when it needs it (for example at voice call establishment).

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

No special configuration is required to enable this functionality.

The MME can now report the Location of a UE through the GTPv2 messages using the NPLI IEs (ULI Info, ULI-Timestamp and the UE-Timezone). The ULI Info is now included in the following GTPv2 messages:

- Create Session Request
- Create Bearer Response
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response
- Delete Bearer Command

This feature also includes:

- Support for Retrieve Location Indication in the Update Bearer Request message. For this feature, the MME does not retrieve specific location information of UE but instead uses the last stored location information.
- Support for ULI timestamp in Delete Bearer Response, Delete Session Request and Delete Bearer Command messages. (Added newly in 3GPP TS 29.274 V11.8.0)
- Support for UE Time Zone in Delete Bearer Command messages.

**Note:** NPLI related IEs in CSReq and DSReq messages will be sent only in case of PDN establishment, but not in case of SGW relocation.

# Optimized Paging Support

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Also known as heuristic or idle-mode paging, this feature reduces network operations cost through more efficient utilization of paging resources and reduced paging load in the EUTRAN access network.

Idle mode paging over EUTRAN access networks is an expensive operation that causes volumes of signaling traffic between the S-GW and MME/SGSN. This problem is acute in the radio access network, where paging is a shared resource with finite capacity. When a request for an idle mode access terminal is received by the S-GW, the MME floods the paging notification message to all eNodeBs in the Tracking Area List (TAI). To appreciate the magnitude of the problem, consider a network with three million subscribers and a total of 800 eNodeBs in the TAI. If each subscriber was to receive one page during the busy hour, the total number of paging messages would exceed one million messages per second.

To limit the volume of unnecessary paging related signaling, the Cisco MME provides intelligent paging heuristics. Each MME maintains a list of "n" last heard from eNodeBs inside the TAI for the UE. The intent is to keep track of the eNodeBs that the AT commonly attaches to such as the cells located near a person's residence and place of work. During the average day, the typical worker spends the most time attaching to one of these two locations. When an incoming page arrives for the idle mode user, the MME attempts to page the user at the last heard from eNodeB. The MME uses Tracking Area Updates to build this local table. If no response is received within a configurable period, the MME attempts to page the user at the last "n" heard from eNodeBs. If the MME has still not received acknowledgment from the idle mode UE, only then does it flood the paging messages to all eNodeBs in the TAI.

In the majority of instances with this procedure, the UE will be paged in a small set of eNodeBs where it is most likely to be attached.

# Overcharging Protection

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Overcharging Protection helps in avoiding charging subscribers for dropped downlink packets while the UE is in idle mode. This feature helps ensure subscribers are not overcharged while the subscriber is in idle mode.

Refer to the *Overcharging Protection* chapter in the *MME Administration Guide* for more information.

# Operator Specific QCI

In Release 20.0, MME has been enhanced to support new standardized QCIs 65, 66, 69 and 70. Also, MME also supports operator specific (non-standard) QCIs from 128 to 254. The non-standard QCIs provides Operator Specific QoS for M2M and other mission critical communications.

The **operator-defined-qci** command under the QoS profile configuration is provisioned to enable or disable Operator Specific QCI. When enabled, MME accepts Operator Specific QCI values (128-254) both from HSS and PGW. If not enabled, MME will reject the procedure on receiving any Operator Specific QCI value.

Additionally, this chapter describes the mapping of operator specific QCIs to Pre-Release8 QoS parameters during a handover to UTRAN/GERAN.

The Operator Specific and Non-Standard QCI Support feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

For a complete description of this feature and its configuration requirements, refer to the *Operator Specific QCI* chapter in *MME Administration Guide*.

# Separate Configuration for GTPC Echo and GTPC Non-Echo Messages

GTP echo and GTP message retry timer can be configured separately. The maximum retry number can also be configured separately, in a similar fashion as the timer configuration.

In egtp-service, the **echo-max-retransmissions** keyword is added to allow the separate configuration of GTPC echo retransmission.

**Previous Behavior:** The maximum number of retransmission for Echo Requests was configured by **max-retransmissions** configuration option.

**New Behavior: echo-max-retransmissions** is introduced explicitly for the configuration of echo max retransmission in the eGTPC Service Configuration Mode.

# Session Recovery Support

The feature use license for Session Recovery on the MME is included in the MME session use license.

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.



**Important** For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Administration Guide*.

# SGSN-MME Combo Optimization

The SGSN-MME Combo Optimization feature enables the co-located SGSN and MME to co-operate with each other in order to achieve lower memory utilization, lower CPU utilization, and reduced signaling towards other nodes in the network.

The SGSN and MME can be enabled simultaneously in the same chassis and, though co-located, they each behave as independent nodes. When functioning as mutually-aware co-located nodes, the SGSN and MME can share UE Subscription data.

This SGSN-MME Combo Optimization feature is enabled with a new CLI command:

- If the operator intends the MME to use DNS to dynamically discover the Target SGSN, then the DNS Server must be configured with an entry for the co-located SGSN.
- If the operator intends the MME to use location configuration to select the Target SGSN, then the MME Service configuration is required to have a **peer-sgsn** entry for the co-located SGSN.

For detailed Combo Optimization feature and implementation description see the *SGSN-MME Combo Optimization* section in the *MME Administration Guide, StarOS Release 18*.

Combo Optimization functionality for both the SGSN and the MME is a licensed Cisco feature. Contact your Cisco account representative for information on acquiring this separate feature license or for any other licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section in the *System Administration Guide.*

# Single Radio Voice Call Continuity Support

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Voice over IP (VoIP) subscribers anchored in the IP Multimedia Subsystem (IMS) network can move out of an LTE coverage area and continue the call over the circuit-switched (CS) network through the use of the Single Radio Voice Call Continuity (SRVCC) feature. The smooth handover of the VoIP call does not require dual-mode radio.

For more information about SRVCC, refer to the *Single Radio Voice Call Continuity* chapter in this document.

## MSC Fallback on Sv Interface

MME maintains the reachability status of MSCs on the Sv interface. Only reachable MSCs are selected for PS to CS handovers (SRVCC procedures). The MSC Fallback feature is currently applicable only when MSC IP address is statically configured in StarOS, and not when MME determines MSC IP using DNS resolution.

When the MSC Fallback feature is enabled, MME acquires the status information independent of any ongoing SRVCC procedures, from the EGTPMGR. The status of an MSC will be unknown until MME acquires its status by sending ECHO requests to the MSCs. If a response is received from the MSC, the status of the MSC is moved to UP state. If no response is received, the MSC is considered to be in the DOWN state (unreachable).

If the status of an MSC is DOWN, ECHO Requests will be sent to the MSCs based on a configured reconnect-interval value. If an MSC responds to the request within this interval, the status of the MSC is changed to UP state. For more information related to reconnect-interval configuration, please refer to the Configuring MSC Fallback section.

For PS to CS handovers, MME only selects the MSCs in the UP state. The status information of the MSC provided by the EGTPMGR helps to select only reachable MSCs. This process reduces latency during fallback to reachable MSCs.

The MSC Fallback feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

For a complete description of this feature and its configuration requirements, refer to the *Single Radio Voice Call Continuity* chapter in the *MME Administration Guide*.

# Subscribed Periodic TAU Timer

This feature helps the MME to reduce network load from periodic TAU signaling and to increase the time until the UE detects a potential need for changing the RAT or PLMN.

The feature enables the Operator to configure longer values for the periodic TAU timer and Mobile Reachable timer using new commands on the MME.

A new configuration is supported under the MME Service to define an EMM extended-3412 timer value. Refer to the *Command Changes* section below for more information.

The UE must include the "MS network feature support" IE in the Attach Request/TAU Request. This IE indicates to the MME that the UE supports the extended periodic timer T3412, in which case the MME sends the extended-3412 IE in the attach/TAU response. The MME will not forward the extended-T3412 timer value to any UE which has not indicated that it supports this extended-t3412 timer.

The MME supports storing the Subscribed-Periodic-RAU-TAU-Timer value if received as part of subscription data, and deleting this stored value if the corresponding withdrawal flag is received in the DSR command.

For homers, the MME will send the extended-3412 IE value as received in Subscribed-Periodic-RAU-TAU-Timer IE in subscription data.

For roamers, the MME takes the presence of Subscribed-Periodic-RAU-TAU-Timer IE in subscription data as an indication and shall send the extended-3412 IE with the value from the local configuration.

The MME adjusts the configured mobile reachability timer value if the subscribed extended-3412 timer value received from HSS is greater than the sum of the mobile reachability timer + implicit detach timer such that the extended-3412 timer value becomes 10 less than the mobile reachability timer + implicit detach timer.

Refer to 3GPP TS 23.401 Section 4.3.17.3 (Version 10.4.0) & 29.272 for more details.

# Support for Reject Causes with MM and SM Back Off Timers

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Under congestion, the MME can now assign EMM or ESM back-off timer to the UEs and request the UEs not to access the network for a given period of time.

Refer to 3GPP TS 23.401 Section 4.3.7.4.2.4 (Version 10.4.0) for more details.

### EMM T3346 Timer

The MME now allows configuration of the T3346 back-off timer value. EMM timer value. The default value of this timer will be set to 25 minutes.

With this feature, when any EMM request rejected by MME because of congestion, the reject will have EMM cause of "congestion" (22) and will include the back-off timer (T3346) IE. This back-off timer is chosen randomly and will be 10 below or above the configured T3346 timer value.

While storing the back-off timer expiry time, MME shall adjust the mobile reachability timer and/or implicit detach timer. This is to make sure that the sum of the mobile reachability timer + implicit detach timer is greater than the back-off timer duration.

The MME will store the DB for at least the EMM back-off timer duration even if the attach is rejected because of congestion. The MME will not start any timer for EMM back-off. Instead, back-off timer expiry time will be stored in the DB as the DB is stored for at least back-off timer duration.

If an EMM call is rejected due to congestion control for EMM, the DB created during ULA will not be cleared and the purge timer will be started for a time period 10 greater than the back-off timer duration. This is done to make sure that DB is available during back-off timer duration to reject any requests during this period and also to avoid the HSS signaling again if the UE comes back immediately after the back-off timer duration.

The MME will not reject any TAU received in EMM-CONNECTED state.

The MME will not reject any requests related to handovers as part of this feature even if EMM back-off timer is running.

The MME will drop attach requests received during congestion while EMM back-off timer is running based on configuration in congestion-action-profile. For example, if configuration is enabled to reject new call only when low priority indication is set and the UE comes without low priority indication while back off timer is running, the MME will accept the new call attempt from the UE.

The MME will not reject/drop attach requests received even if EMM back-off timer is running if the congestion gets cleared.

The MME will forward SGS paging requests received from MSC for a UE attached in MME even if back-off timer is running.

### ESM T3396 Timer

The MME allows configuration of the T3396 back-off timer value. When any ESM request is rejected because of congestion, the reject will have ESM cause "Insufficient resources" and will include a back-off timer IE (T3396). This back-off timer is chosen randomly and will be 10 below or above the configured T3396 timer value.

The MME will not start any timer for SM back-off and store the SM back-off timer expiry time. If an SM request is received and if congestion exists, the request will be rejected and a new random value will be sent as the ESM back-off timer value. The MME will reject any subsequent requests from the UE targeting the same APN based on the presence of congestion at that time and not based on the SM back-off time previously sent to the UE.

The T3396 timeout is configurable only for the ESM cause values - 26 'insufficient resources' or 27 'missing or unknown APN'. If the ESM cause value is 26 "insufficient resources" or 27 "missing or unknown APN", the MME will include a value for timer T3396 in the reject message. If the ESM cause value is 26 "insufficient resources" and the request message was sent by a UE accessing the network with access class 11 - 15 or if the request type in the PDN CONNECTIVITY REQUEST message was set to "emergency", the MME will not include a value for timer T3396.

In 21.3 and later releases, the T3396 timer can be configured at APN Profile and Call Control Profile to control the UE behavior depending on the APN and subscriber type. This is compliant with 3GPP TS 24.301 (section 6.5.1.4) and specifically intended for VoLTE signaling control for subscribers that have no IMS subscription. This enhancement can also limit the number of Attach attempts for such subscribers and reduce the signaling impact on EPC nodes.

The T3396 timeout configuration will be applied from APN Profile, Call Control Profile and MME service in decreasing order of precedence. In releases prior to 21.3, the T3396 timeout could only be configured at the MME service level and the cause value could not be specified. If the ESM message is rejected with either of the cause values, the network will include a value for T3396 timer in ESM reject message. UE will not retry the ESM request message until the T3396 timer expires.

# User Location Information Reporting

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

User Location Information (ULI) Reporting allows the eNodeB to report the location of a UE to the MME, when requested by a P-GW.

The following procedures are used over the S1-MME interface to initiate and stop location reporting between the MME and eNodeB:

- **Location Reporting Control**: The purpose of Location Reporting Control procedure is to allow the MME to request that the eNodeB report where the UE is currently located. This procedure uses UE-associated signaling.
- **Location Report Failure Indication**: The Location Report Failure Indication procedure is initiated by an eNodeB in order to inform the MME that a Location Reporting Control procedure has failed. This procedure uses UE-associated signaling.

- **Location Report**: The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signaling.

The start/stop trigger for location reporting for a UE is reported to the MME by the S-GW over the S11 interface. The Change Reporting Action (CRA) Information Element (IE) is used for this purpose. The MME updates the location to the S-GW using the User Location Information (ULI) IE.

The following S11 messages are used to transfer CRA and ULI information between the MME and S-GW:

- **Create Session Request**: The ULI IE is included for E-UTRAN Initial Attach and UE-requested PDN Connectivity procedures. It includes ECGI and TAI. The MME includes the ULI IE for TAU/ X2-Handover procedure if the P-GW has requested location information change reporting and the MME support location information change reporting. The S-GW includes the ULI IE on S5/S8 exchanges if it receives the ULI from the MME. If the MME supports change reporting, it sets the corresponding indication flag in the Create Session Request message.
- **Create Session Response**: The CRA IE in the Create Session Response message can be populated by the S-GW to indicate the type of reporting required.
- **Create Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Modify Bearer Request**: The MME includes the ULI IE for TAU/Handover procedures and UE-initiated Service Request procedures if the P-GW has requested location information change reporting and the MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Modify Bearer Response**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Delete Session Request**: The MME includes the ULI IE for the Detach procedure if the P-GW has requested location information change reporting and MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Update Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Change Notification Request**: If no existing procedure is running for a UE, a Change Notification Request is sent upon receipt of an S1-AP location report message. If an existing procedure is running, one of the following messages reports the ULI:
  - Create Session Request
  - Create Bearer Response
  - Modify Bearer Request
  - Update Bearer Response
  - Delete Bearer Response
  - Delete Session Request

  If an existing Change Notification Request is pending, it is aborted and a new one is sent.

**Important** Information on configuring User Location Information Reporting support is located in the *Configuring Optional Features on the MME* section of the *Mobility Management Entity Configuration* chapter in this guide.

## VLR Management

These features require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

The following features provide for additional resiliency of the Circuit Switched Fallback (CSFB) service.

- **Passive VLR Offloading and Active VLR Offloading:** The MME supports the capability to passively offload UEs for a specific VLR. This capability enables operators to preemptively move subscribers away from an SGs interface associated with a VLR which is planned for maintenance mode.

  Active VLR Offloading provides all of the functionality of Passive VLR Offloading, but also actively detaches UEs associated with the VLR during an operator-specified time period. This expedites the process of offloading UEs prior to a planned VLR maintenance event.

  Both passive and active offload functionality is available only for VLRs within a LAC pool area.

- **UE Detach on VLR Failure:** The MME supports the ability to perform a controlled release of UEs when a VLR connection becomes unavailable.

- **UE Detach on VLR Recovery:** The MME also has the ability to perform a controlled release of CSFB (SMS-only) UEs when a failed VLR becomes responsive again (thereby returning the UE to a combined attached state on a different VLR).

Refer to the **VLR Management** chapter in the *MME Administration Guide* for more information about these features.

# How the MME Works

This section provides information on the function and procedures of the MME in an EPC network and presents message flows for different stages of session setup.

## EPS Bearer Context Processing

EPS Bearer context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the P-GW system.

Each APN template consists of parameters pertaining to how EPS Bearer contexts are processed such as the following:

- **PDN Type:** The system supports IPv4, IPv6, or IPv4v6.

- **Timeout:** Absolute and idle session timeout values specify the amount of time that an MS can remain connected.

- **Quality of Service:** Parameters pertaining to QoS feature support such as for Traffic Policing and traffic class.

A total of 11 EPS bearer contexts are supported per subscriber. These could be all dedicated, or 1 default and 10 dedicated or any combination of default and dedicated context. Note that there must be at least one default EPS bearer context in order for dedicated context to come up.

# Purge Procedure

The purge procedure is employed by the Cisco MME to inform the concerned node that the MME has removed the EPS bearer contexts of a detached UE. This is usually invoked when the number of records exceeds the maximum capacity of the system.

# Paging Procedure

Paging is initiated when there is data to be sent to an idle UE to trigger a service request from the UE. Once the UE reaches connected state, the data is forwarded to it.

Paging retransmission can be controlled by configuring a paging-timer and retransmission attempts on system.

# Subscriber-initiated Initial Attach Procedure

The following figure and the text that follows describe the message flow for a successful user-initiated subscriber attach procedure.

*Figure 5: Subscriber-initiated Attach (initial) Call Flow*

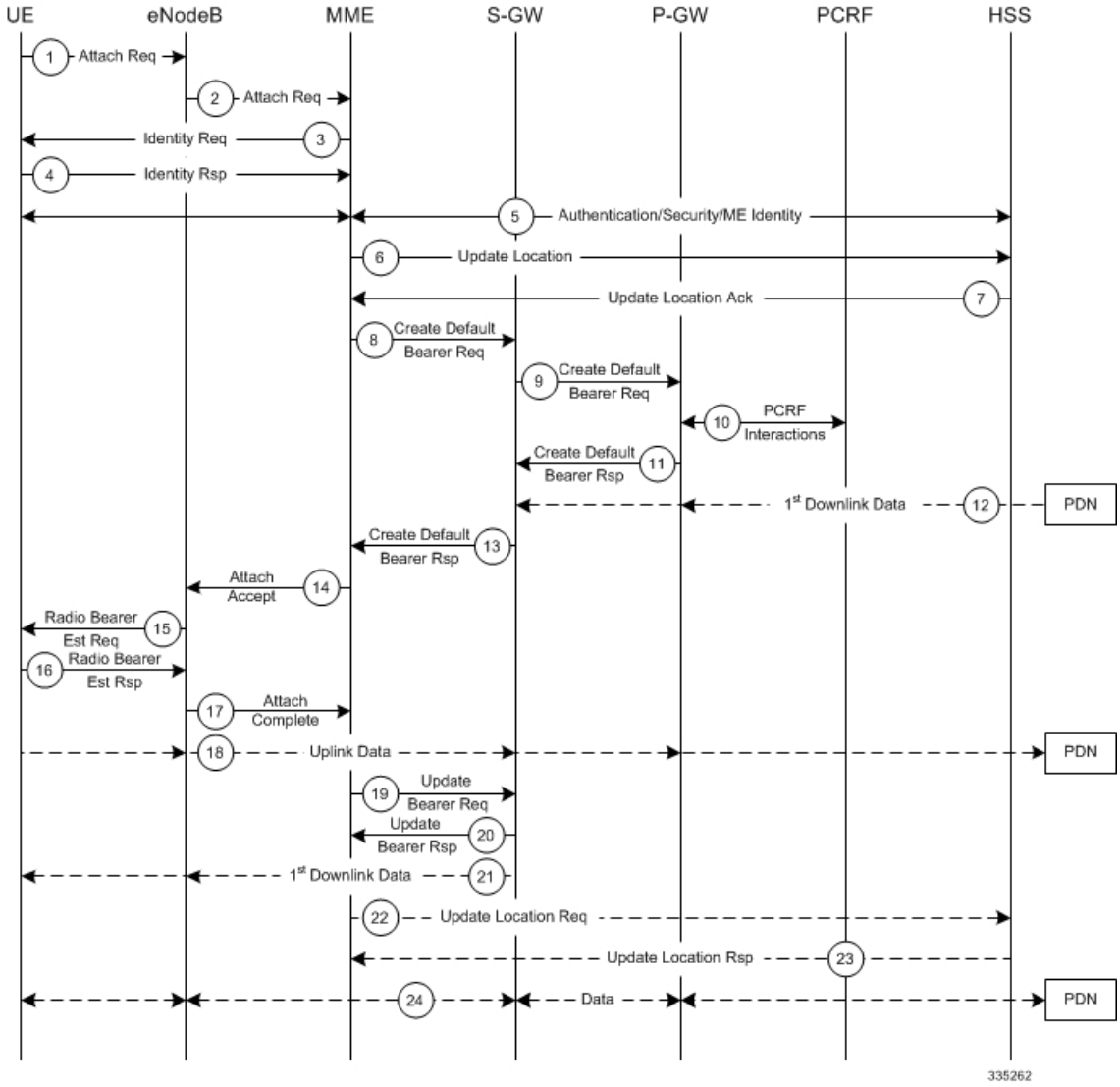



*Table 1: Subscriber-initiated Attach (initial) Call Flow Description*

| Step | Description |
|---|---|
| 1 | The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included. |
| 2 | The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an "MME selection function". The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME. |

| Step | Description |
|---|---|
| 3 | If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI. |
| 4 | The UE responds with Identity Response (IMSI). |
| 5 | If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages. |
| 6 | The MME sends an Update Location Request (MME Identity, IMSI, ME Identity) to the HSS. |
| 7 | The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause. |
| 8 | The MME selects an S-GW using "Serving GW selection function" and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause "PDN GW selection function". Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW. |
| 9 | The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW. |
| 10 | If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message. |
| 11 | The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response. |
| 12 | The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data. |
| 13 | The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW. |
| 14 | The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB. |
| 15 | The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE. |

| Step | Description |
|---|---|
| 16 | The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included. |
| 17 | The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME. |
| 18 | The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW. |
| 19 | The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW. |
| 20 | The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME. |
| 21 | The S-GW sends its buffered downlink packets. |
| 22 | After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses. |
| 23 | The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME. |
| 24 | Bidirectional data is passed between the UE and PDN. |

# Subscriber-initiated Detach Procedure

The following figure and the text that follows describe the message flow for a user-initiated subscriber de-registration procedure.

***Table 2: Subscriber-initiated Detach Call Flow Description***

| Step | Description |
|---|---|
| 1 | The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not. |
| 2 | The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW. |
| 3 | The S-GW sends a Delete Bearer Request (TEID) message to the P-GW. |
| 4 | The P-GW acknowledges with a Delete Bearer Response (TEID) message. |
| 5 | The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network. |
| 6 | The S-GW acknowledges with a Delete Bearer Response (TEID) message. |
| 7 | If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE. |
| 8 | The MME releases the S1-MME signaling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach. |

# Service Request Procedures

Service Request procedures are used to establish a secure connection to the MME as well as request resource reservation for active contexts. The MME allows configuration of the following service request procedures:

- UE-initiated Service Request Procedure
- Network-initiated Service Request Procedure

For call flow details for these procedures, refer to the following sections.

## UE-initiated Service Request Procedure

The call flow in this section describes the process for re-connecting an idle UE.

The following figure and the text that follows describe the message flow for a successful UE-initiated service request procedure.

***Figure 7: UE-initiated Service Request Message Flow***

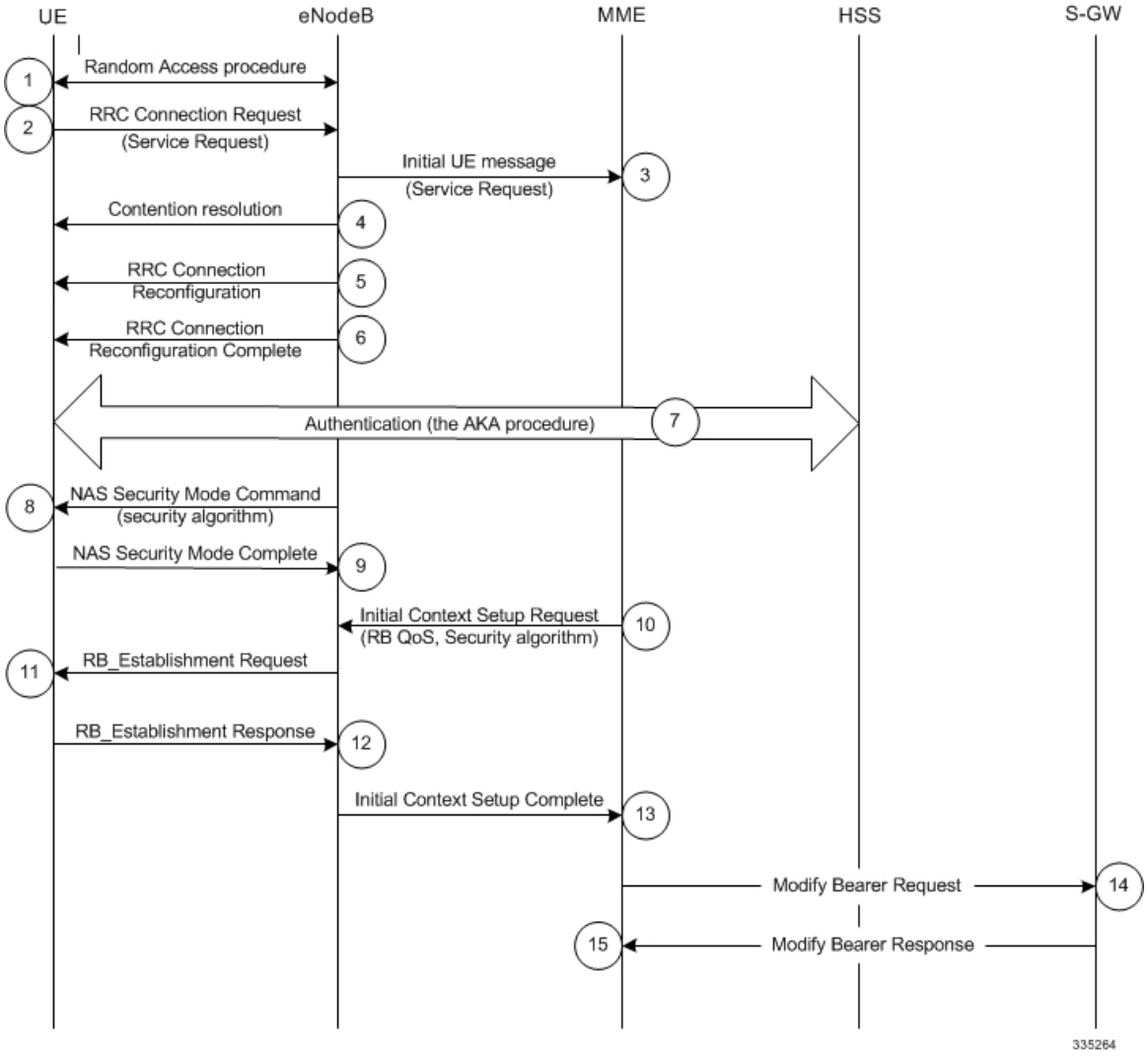


*Table 3: UE-initiated Service Request Message Flow Description*

| Step | Description |
|---|---|
| 1 | (NAS) The UE sends a Network Access Signaling (NAS) message Service Request (S-TMSI) towards the MME encapsulated in an RRC message to the eNodeB. |
| 2 | The eNodeB forwards NAS message to the MME. The NAS message is encapsulated in an S1-AP: Initial UE message (NAS message, TAI+ECGI of the serving cell). |
| 3 | NAS authentication procedures may be performed. |
| 4 | The MME sends an S1-AP Initial Context Setup Request (S-GW address, S1-TEID(s) (UL), EPS Bearer QoS(s), Security Context, MME Signaling Connection Id, Handover Restriction List) message to the eNodeB. This step activates the radio and S1 bearers for all the active EPS Bearers. The eNodeB stores the Security Context, MME Signaling Connection Id, EPS Bearer QoS(s) and S1-TEID(s) in the UE RAN context. |
| 5 | The eNodeB performs the radio bearer establishment procedure. |
| 6 | The uplink data from the UE can now be forwarded by eNodeB to the S-GW. The eNodeB sends the uplink data to the S-GW address and TEID provided in step 4. |
| 7 | The eNodeB sends an S1-AP message Initial Context Setup Complete message (eNodeB address, List of accepted EPS bearers, List of rejected EPS bearers, S1 TEID(s) (DL)) to the MME. |
| 8 | The MME sends a Modify Bearer Request message (eNodeB address, S1 TEID(s) (DL) for the accepted EPS bearers, RAT Type) to the S-GW. The S-GW is now able to transmit downlink data towards the UE. |
| 9 | The S-GW sends a Modify Bearer Response message to the MME. |

## Network-initiated Service Request Procedure

The call flow in this section describes the process for re-connecting an idle UE when a downlink data packet is received from the PDN.

The following figure and the text that follows describe the message flow for a successful network-initiated service request procedure:

*Figure 8: Network-initiated Service Request Message Flow*

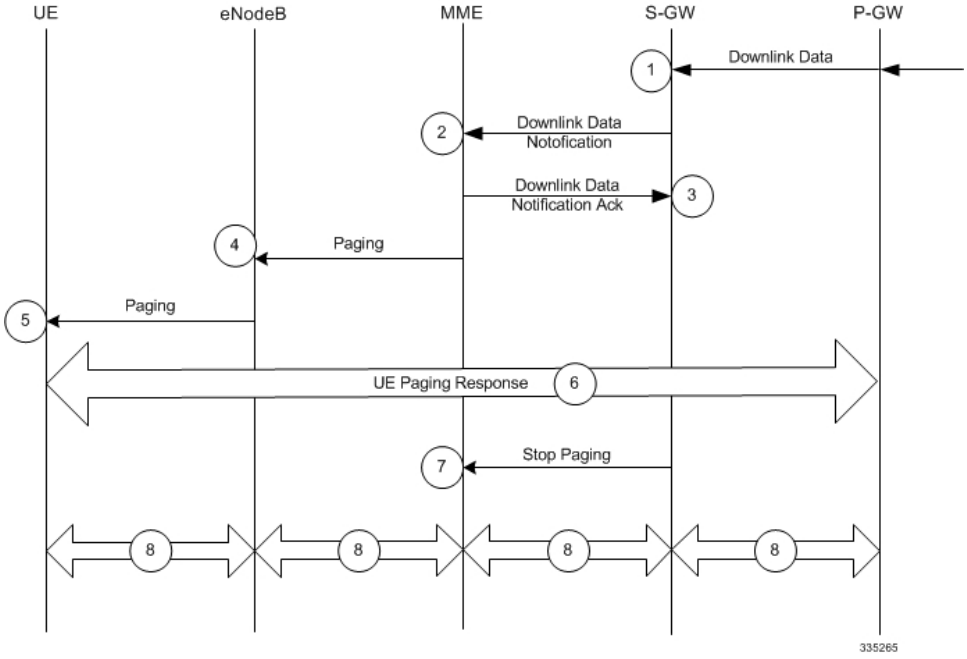



*Table 4: Network-initiated Service Request Message Flow Description*

| Step | Description |
|---|---|
| 1 | A downlink data packet is received on the S-GW from PDN for the targeted UE. The S-GW checks to see if the UE is user-plane connected (the S-GW context data indicates that there is no downlink user plane (TEID)). The downlink data is buffered and the S-GW identifies which MME is serving the intended UE. |
| 2 | The S-GW sends a Downlink Data Notification message to the MME for the targeted UE. |
| 3 | The MME responds with a Downlink Data Notification Acknowledgment message to the S-GW. |
| 4 | The MME send a Paging Request to the eNodeB for the targeted UE. The Paging Request contains the NAS ID for paging, TAI(s), the UE identity based DRX index, and the Paging DRX length. The Paging Request is sent to each eNodeB belonging to the tracking area(s) where the UE is registered. |
| 5 | The eNodeB broadcasts the Paging Request in its coverage area for the UE.<br>**Note**<br>Steps 4 and 5 are skipped if the MME has a signaling connection over the S1-MME towards the UE. |
| 6 | Upon receipt of the Paging indication in the E-UTRAN access network, the UE initiates the UE-triggered Service Request procedure and the eNodeB starts messaging through the UE Paging Response.<br>The MME supervises the paging procedure with a timer. If the MME receives no Paging Response from the UE, it retransmits the Paging Request. If the MME receives no response from the UE after the retransmission, it uses the Downlink Data Notification Reject message to notify the S-GW about the paging failure. |

| Step | Description |
|---|---|
| 7 | The S-GW sends a Stop Paging message to MME. |
| 8 | The buffered downlink data is sent to the identified UE. |

# Supported Standards

The MME complies with the following standards for 3GPP LTE/EPS wireless networks.

## 3GPP References

- 3GPP TS 23.007 V13.3.0:Technical Specification Group Core Network and Terminals Restoration procedures
- 3GPP TS 23.041 V10.6.0: Technical realization of Cell Broadcast Service (CBS)
- 3GPP TS 23.216 V12.2.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Single Radio Voice Call Continuity (SRVCC) Stage 2
- 3GPP TS 23.251 V12.1.0: Network Sharing; Architecture and Functional Description
- 3GPP TS 23.271, v10.4.0 (2013-03): Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE. Functional stage 2 description of Location Services (LCS)
- 3GPP TS 23.272 V12.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Circuit Switched (CS) fallback in Evolved Packet System (EPS) Stage 2
- 3GPP TS 23.401 V13.11.0: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.682 V13.9.0: Architecture enhancements to facilitate communications with packet data networks and applications
- 3GPP TS 23.842 V11.0.0:3rd Generation Partnership Project Technical Specification Group Services and System Aspects Study on Network Provided Location Information to the IMS
- 3GPP TS 24.008 V13.0.0 (2016-06): Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
- 3GPP TS 24.008 V13.6.0 (2016-06): Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
- 3GPP TS 24.080, V12.8.0: Mobile radio interface layer 3 supplementary services specification Formats and coding
- 3GPP TS 24.301 V12.8.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) Stage 3
- 3GPP TS 24.301 V13.10.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) Stage 3

- 3GPP TS 29.118 V10.9.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Mobility Management Entity (MME) - Visitor Location Register (VLR) SGs interface specification
- 3GPP TS 29.168 V12.8.0: Cell Broadcast Centre Interfaces with the Evolved Packet Core
- 3GPP TS 29.171 V12.1.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Location Services (LCS) LCS Application Protocol (LCS-AP) between the Mobile Management Entity (MME) and Evolved Serving Mobile Location Centre (E-SMLC) SLs interface
- 3GPP TS 29.172 V12.5.0 : 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Location Services (LCS) Evolved Packet Core (EPC) LCS Protocol (ELP) between the Gateway Mobile Location Centre (GMLC) and the Mobile Management Entity (MME) SLg interface
- 3GPP TS 29.272 V12.7.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals 3GPP Evolved Packet System (EPS) Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.274 V12.8.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C) Stage 3
- 3GPP TS 29.277 V12.0.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals Optimised Handover Procedures and Protocol between EUTRAN access and non-3GPP accesses (S102) Stage 3
- 3GPP TS 29.280 V10.4.0 (2012-06): 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals 3GPP Evolved Packet System (EPS) 3GPP Sv interface (MME to MSC, and SGSN to MSC) for SRVCC
- 3GPP TS 29.305 V12.4.0: 3rd Generation Partnership Project Technical Specification Group Core Network and Terminals InterWorking Function (IWF) between MAP based and Diameter based interfaces
- 3GPP TS 32.422 V12.4.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace Trace control and configuration management
- 3GPP TS 32.423 V12.1.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace: Trace data definition and management
- 3GPP TS 36.413 V13.6.0: 3rd Generation Partnership Project Technical Specification Group Radio Access Network Evolved Universal Terrestrial Radio Access Network (E-UTRAN) S1 Application Protocol (S1AP)

# IETF References

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984

- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996

- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC 2131, Dynamic Host Configuration Protocol
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol "L2TP", August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999

- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- Draft, Route Optimization in Mobile IP
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

# Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group